Lab Name	Lab Description	Lab Series	NSA CAF KU's	Platform	Expected Duration	Maximum Duration	Average Duration	Average Startup Duration
Lab Name	Active Directory's are an important part of many organizations' IT structure. Thus, Active	Lab Jeries		riacionii	Expected Duration	Waximum Duration	Average Duration	Average startup buration
Active Directory Security Checkup Capstone	Directory security is just as important and there are several best practices to follow. This capstone tests a student's ability to manage an Active Directory while implementing those best practices.	CYBRScore Capstones	Windows System Administration (WSA), Topics: 13 Cybersecurity Principles (CSP), Topics: j: Operating System Concepts (OSC), Topics: 1, 9	Hyper-V	1 Hour, 30 Minutes	1 Hour, 30 Minutes	28 minutes, 44 seconds	1 minute, 41 seconds
Additional Scanning Options	Students will leverage Nmap, a network discovery and mapping tool, to identify the systems on a network of responsibility. Students will utilize non-traditional scans to attempt avoiding an Intrusion Detection System (IDS).	CYBRScore Scored Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10	Hyper-V	45 Minutes	45 Minutes	22 minutes, 36 seconds	1 minute, 40 seconds
Additional Scanning Options	Students will leverage Nmap, a network discovery and mapping tool, to identify the systems on a network of responsibility. Students will utilize non-traditional scans to attempt avoiding an intrusion Detection System (IDS).	CYBRScore Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10	Hyper-V	45 Minutes	45 Minutes	37 minutes, 46 seconds	34 seconds
Additional Scanning Options	Students will leverage Nmap, a network discovery and mapping tool, to identify the systems on a network of responsibility. Students will utilize non-traditional scans to attempt avoiding an intrusion Detection System (IDS).	CYBRScore Network Forensics	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10	Hyper-V	45 Minutes	45 Minutes	19 minutes, 14 seconds	44 seconds
Advanced Malware Analysis Labs	MALEOD exposes students to the theoretical knowledge and hands-on techniques to reverse engineer malware that was designed to thwart the most common reverse engineering techniques. The students learn how to identify and analyze the presence of advanced packers, polymorphic malware, encryptied malware, and malkicous gain a high-level understanding of complex malware enalysis techniques. Students gain a high-level understanding of complex malware analysis techniques and spend a significant amount of time solving hands-on challenges throughout the course. This course is for malware analysis, on appring analysis, who have already taken CritiScores' MALAGO (Fundamentals of Malware Ravlaysis) and MALEOD (Reverse Engineering Malware) courses. Those who have encounteer danware analysis as part of incident response, research, or secure development and want to improve upon their knowledge and skills may also find this course beneficial. Students should have intermediate malware analysis skills, the ability to read and understand moderately complex finally-level language code constructs in assembly, familiarity with Windroos APA, networking, and scripting, and finally, experience with IDA Pro, Olly, Immunity, or another similar application.	CYBRScore Labs	Software Security Analysis (SSA); Topics: 1, 2, 3, 4, 5	vSphere	40 Hours	41 Hours, 40 Minutes	6 minutes, 59 seconds	12 seconds
Advanced Techniques for Malware Recovery	Students will use the SysInternals Suite of utilities to analyze processes, DLLs, registry edits and other auto start functions to locate and remove malicious software from an infected Windows 7 victim machine.	CYBRScore Scored Labs	Software Security Analysis (SSA); Topics: 1, 2, 3, 4, 5	Hyper-V	1 Hour, 5 Minutes	2 Hours	44 minutes, 11 seconds	1 minute, 21 seconds
Advanced Techniques for Malware Recovery	infected Windows 7 victim machine.	CYBRScore Labs	Software Security Analysis (SSA); Topics: 1, 2, 3, 4, 5	Hyper-V	1 Hour, 5 Minutes	2 Hours	23 minutes, 23 seconds	35 seconds
Analysis and Recommendation Report	Students will do a Vulnerability Assessment on a network. Students will then analyze the results and place them in a Recommendation Report.		Operating Systems Hardening (OSH), Topics: 11; IT Systems Components (ISC), Topics: 13	Hyper-V	2 Hours	2 Hours	38 minutes, 42 seconds	33 seconds
Analysis and Recommendation Report	Students will do a Vulnerability Assessment on a network. Students will then analyze the		Operating Systems Hardening (OSH), Topics: 11; IT Systems Components (ISC), Topics: 13	Hyper-V	2 Hours	2 Hours	1 minute, 49 seconds	1 minute, 9 seconds
Analyze and Classify Malware	In this lab you will attempt to conduct basic analysis on some malware samples that were found on the internal network	CYBRScore Labs	Software Security Analysis (SSA); Topics: 1, 2, 3, 4, 5	Hyper-V	1 Hour	1 Hour	29 minutes, 14 seconds	20 seconds
Analyze and Classify Malware	In this lab you will attempt to conduct basic analysis on some malware samples that were found on the internal network.	CYBRScore Scored Labs	Software Security Analysis (SSA); Topics: 1, 2, 3, 4, 5	Hyper-V	1 Hour	1 Hour	20 minutes, 12 seconds	1 minute, 37 seconds
Analyze and Update a Company BCP/BIA/DRP/CIRP	Students will become familiar with the Business Continuity Plan (BCP), Business Impact Assessment (BM), Disaster Recovery Plan (DRP) and Computer Incident Response Plan (DRP). Each of these documents are used to address different, but related, aspects of confinuing or recovering business functionality during/after an incident. During the course of the lab, students will perform a gap analysis using the provided BCP, BM and DRP, and make the necessary fixes to the DRP.	CYBRScore Labs	Cybersecurity Planning and Management (CPM); Topics: 2, 4, 5, 6, 8, 9	Hyper-V	1 Hour, 30 Minutes	2 Hours	13 minutes, 14 seconds	28 seconds
Analyze and Update a Company BCP/BIA/DRP/CIRP	Students will become familiar with the Business Continuity Plan (BCP), Business Impact Assessment (BM), Disaster Recovery Plan (DRP) and Computer Incident Response Plan (DRP). Each of these documents are used to address different, but related, aspects of confinuing or recovering business functionality during/after an incident. During the course of the lab, students will perform a gap analysis using the provided BCP, BMs and DRP, and make the necessary fixes to the DRP.	CYBRScore Scored Labs	Cybersecurity Planning and Management (CPM); Topics: 2, 4, 5, 6, 8, 9	Hyper-V	1 Hour, 30 Minutes	2 Hours	38 minutes, 6 seconds	1 minute, 15 seconds
Analyze Browser-based Heap Spray Attack	Students will identify a browser-based attack used against a corporate asset using a network protocol analyzer. Students will determine the type of attack used and pinpoint exploit code in network traffic.	CYBRScore Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10	Hyper-V	43 Minutes	1 Hour	53 minutes, 50 seconds	17 seconds
Analyze DoomJuice Infection to Identify Attack Vector and Payload	Students will use popular system analysis tools on an infected machine in order to identify signs of infection. Afterwards, students will manually remove malware from the system.	CYBRScore Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10	Hyper-V	45 Minutes	1 Hour, 30 Minutes	11 minutes, 30 seconds	57 seconds
Analyze Malicious Activity in Memory Using Volatility	Students will use the open source Volatility tool to analyze a memory snapshot and determine what malicious software has infected the victim machine.	CYBRScore Scored Labs	Software Security Analysis (SSA); Topics: 1, 2, 3, 4, 5	Hyper-V	1 Hour	2 Hours	26 minutes, 23 seconds	1 minute
Analyze Malicious Activity in Memory Using Volatility	Students will use the open source Volatility tool to analyze a memory snapshot and determine what malicious software has infected the victim machine.	CYBRScore Labs	Software Security Analysis (SSA); Topics: 1, 2, 3, 4, 5	Hyper-V	1 Hour	2 Hours	11 minutes, 11 seconds	20 seconds
Analyze Malicious Network Traffic	Students will take some time to review malicious traffic within a controlled environment. Using Wireshark and some pointers from a previous technical report on the FlashPack Exploit kit, they will focus their attention on finding in two traffic captures) evidence of when and how a victim system was infected with the exploit kit.	CYBRScore Labs	Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a	Hyper-V	1 Hour, 30 Minutes	3 Hours	37 minutes, 30 seconds	28 seconds
Analyze Packed Executable to Identify Attack Vector and Payload	Students will use the CFF Explorer and Hacker Process tools in order to perform an initial analysis of a suspicious executable.	CYBRScore Labs	Software Security Analysis (SSA); Topics: 1, 2, 3, 4, 5	Hyper-V	45 Minutes	1 Hour, 30 Minutes	1 minute, 5 seconds	18 seconds
Analyze Packed Executable to Identify Attack Vector and Payload	Students will use a handful of tools to analyze a provided suspicious file. Using CFF Explorer, they will modify how the suspicious program stores variables in memory, deter what packer it was packed with, unpack that file and then save it han unpacked state. Using ExeinfoPE, they will double-check and ensure that the processed version of the program has been successfully unpacked. The students will then run the suspicious program while Process tacker is running and then dump all strings associated with the suspicious process to a tent file. Using the dumped strings they will piece together what the program was designed to do.	CYBRScore Scored Labs	Software Security Analysis (SSA); Topics: 1, 2, 3, 4, 5	Hyper-V	45 Minutes	1 Hour	31 minutes, 38 seconds	1 minute, 37 seconds
Analyze SQL Injection Attack	Students will Identify the use of an SQL Injection through the use of Wireshark. The students will also isolate the different aspects of the SQL Injection and execute the selected code.	CYBRScore Labs	Software Security Analysis (SSA); Topics: 1, 2, 3, 4, 5	Hyper-V	1 Hour	2 Hours	20 minutes, 43 seconds	21 seconds
Analyze SQL Injection Attack	Students will identify the use of an SQL Injection through the use of Wireshark. The students will also isolate the different aspects of the SQL Injection and execute the selected code.	CYBRScore Scored Labs	Software Security Analysis (SSA); Topics: 1, 2, 3, 4, 5	Hyper-V	1 Hour	2 Hours	24 minutes, 58 seconds	1 minute, 16 seconds
Analyze Structured Exception Handler Buffer Overflow Exploit	Students will identify the use of a Buffer Overflow exploit through the use of Wireshark and by analyzing items found in the captured traffic. The students will also find the exploit code and isolate the different aspects of a Buffer Overflow exploit.	CYBRScore Labs	Software Security Analysis (SSA); Topics: 1, 2, 3, 4, 5	Hyper-V	32 Minutes	1 Hour	10 minutes, 30 seconds	16 seconds
Analyze Structured Exception Handler Buffer Overflow Exploit	Students will identify the use of a Buffer Overflow exploit through the use of Wireshark and by analyzing items found in the captured traffic. The students will also find the exploit code and isolate the different aspects of a Buffer Overflow exploit.	CYBRScore Scored Labs	Software Security Analysis (SSA); Topics: 1, 2, 3, 4, 5	Hyper-V	32 Minutes	1 Hour	28 minutes, 15 seconds	1 minute, 4 seconds

Analyze Various Data Sources to Confirm Suspected Infection	Students will review network traffic to confirm the presence of malicious activity using	CYRRC Labo	W. 187 AMERICAN	Ib was M	1 Hour	1 Hour	35 minutes, 59 seconds	30ds
-,	various tools including Wireshark and VirusTotal.com. Students will review network traffic to confirm the presence of malicious activity using		Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a	Hyper-V				
Analyze Various Data Sources to Confirm Suspected Infection	various tools including Wireshark and VirusTotal.com.	CYBRScore Scored Labs	Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a	Hyper-V	1 Hour	1 Hour	34 minutes, 38 seconds	1 minute, 15 seconds
Applying Filters to TCPDump and Wireshark	This lab exercise is designed to allow the trainee to become familiar with applying a capture filter to TCPDump and Wireshark using Berkley Packet Filter (BPF) syntax.	CYBRScore Labs	Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a	vSphere	1 Hour	1 Hour	29 minutes, 2 seconds	11 seconds
Applying Filters to TCPDump and Wireshark	This lab exercise is designed to allow the trainee to become familiar with applying a capture filter to TCPDump and Wireshark using Berkley Packet Filter (BPF) syntax.	CYBRScore Scored Labs	Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a	vSphere	1 Hour	1 Hour	31 minutes, 14 seconds	20 seconds
Assembly Language Fundamentals	Competency in assembly is critical across a variety of development and information security professions ranging from reverse engineers and malware analysis to firmware and exploit developers. DEV-50 provides sudents with a strong foundation in assembly language programming and the architectures for x88 and intel64 processors. Students who take this course will use the Microsoft Marco Assembler (MASM) and Netwide Assembler (MASM) to create a variety of binaries, to include shellcode, during the course. Attendees are strongly encouraged to take DEV-00 (Intrio to Programming C) or have basic programming experience in C/Java, knowledge of networking correspts and basic OS functionality like processes, threading, and memory management prior to taking this class.		Software Security Analysis (SSA); Topics: 1, 2, 3, 4, 5	Hyper-V	8 Hours	8 Hours, 20 Minutes	5 minutes, 22 seconds	1 minute, 23 seconds
Assess A High-Risk System	Systems that are required to provide remote or public customer access should be placed in a Demilitarized Zone (DMZ). The DMZ is separate space set aside for public access but does not allow attackers access to sensitive internal network assets. If public accessing (Internet) servers were hosted on the internal network then an attacker could easily breach the server and use trust relationships or configurations to burrow further into the internal network.	CYBRScore Labs	Operating Systems Hardening (OSH); Topics: 1, 2, 3, 4, 5, 6, 7, 8, 10, 11	Hyper-V	1 Hour	1 Hour	1 minute, 15 seconds	18 seconds
Assess A High-Risk System	breach the server and use trust relationships or configurations to burrow further into the internal network.	CYBRScore Scored Labs	Operating Systems Hardening (OSH); Topics: 1, 2, 3, 4, 5, 6, 7, 8, 10, 11	Hyper-V	1 Hour	1 Hour	31 minutes, 22 seconds	1 minute, 35 seconds
Assessing Vulnerabilities Post Addressal	Students will use Snorby against multiple systems to identify and mitigate any vulnerabilities found.	CYBRScore Labs	Operating Systems Hardening (OSH); Topics: 1, 2, 3, 4, 5, 6, 7, 8, 10, 11	Hyper-V	1 Hour	1 Hour	19 minutes, 37 seconds	33 seconds
Assessing Vulnerabilities Post Addressal	Students will use Snorby against multiple systems to identify and mitigate any vulnerabilities found.	CYBRScore Scored Labs	Operating Systems Hardening (OSH); Topics: 1, 2, 3, 4, 5, 6, 7, 8, 10, 11	Hyper-V	1 Hour	1 Hour	35 minutes, 19 seconds	1 minute, 24 seconds
Attack and Defend - Arena	This lab profile serves as a shared class environment. It must be launched in the context of a class.	CYBRScore Labs	GROUP CTF ENVIRONMENT (MANY)	Hyper-V	100 Hours	100 Hours	7 hours, 49 minutes	1 minute, 40 seconds
Attack and Defend - Competitor	This lab profile serves as a shared class environment. It must be launched in the context	CYBRScore Labs	GROUP CTF ENVIRONMENT (MANY)	Hyper-V	12 Hours	12 Hours	2 hours, 40 minutes	1 minute, 35 seconds
Auditing Service Accounts	of a class. Students will audit service accounts in a Windows Server environment. They will note the services that are running with the help of the server Administrator account and make necessary corrections to them. The corrections will minimize the chance of a successful attack against those services allowing for privilege escalation attempts, leveraging the associated service account, from going anywhere.	CYBRScore Labs	Operating Systems Hardening (OSH); Topics: 1, 2, 3, 4, 5, 6, 7, 8, 10, 11	Hyper-V	40 Minutes	1 Hour	43 seconds	12 seconds
Auditing Service Accounts	Students will audit service accounts in a Windows Server environment. They will not the services that are running with the help of the server Administrator account and make necessary corrections to them. The corrections will minimate the chance of a successful against those services alsouing for privilege escalation attempts, leveraging the associated service account, from going anywhere.	CYBRScore Scored Labs	Operating System Concepts, Topics: 1, 9: Windows System Administration (WSA), Topics: 2, 7	Hyper-V	40 Minutes	1 Hour	32 minutes, 34 seconds	1 minute, 31 seconds
Auditing Service Accounts and Creation of Service Accounts To Run Specifi	Students will explore the auditing of service accounts in a Windows Environment. It Students will then replace services running with the administrator account with accounts that are appropriate for that running service.	CYBRScore Labs	Operating System Concepts, Topics: 1, 9; Windows System Administration (WSA), Topics: 2, 7	Hyper-V	1 Hour	1 Hour	17 minutes, 40 seconds	34 seconds
Auditing Service Accounts and Setting Up Automated Log Collection	Students will explore information-gathering techniques, audit service accounts in a Windows Environment, collect Windows logs, and automate log transfer with Syslog.	CYBRScore Scored Labs	Windows System Administration (WSA), Topics: 2, 4, 6	Hyper-V	1 Hour, 30 Minutes	2 Hours	58 minutes	51 seconds
Auditing Service Accounts and Setting Up Automated Log Collection	network firewall, to ensure system changes and logs are sent to a remote archiving server for future use during incident response events.	CYBRScore Labs	Windows System Administration (WSA), Topics: 2, 4, 6	Hyper-V	1 Hour	1 Hour, 30 Minutes	33 minutes, 2 seconds	32 seconds
Automated in-Depth Packet Decoding Automated in-Depth Packet Decoding	Students will use Network Miner to analyze network traffic. Students will use Network Miner to analyze network traffic.	CYBRScore Network Forensics CYBRScore Labs	Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a	Hyper-V Hyper-V	1 Hour	1 Hour	10 minutes, 58 seconds	37 seconds
Automated Vulnerability Assessments	Students will use Core Impact to conduct an automated vulnerability scan of specific systems in order to identify potential threat vectors.	CYBRScore Labs	Operating Systems Hardening (OSH), Topics: 11; IT Systems Components (ISC), Topics: 13	Hyper-V	1 Hour	1 Hour	4 minutes, 52 seconds	1 minute, 14 seconds
Baseline Systems in Accordance with Policy Documentation	Students are provided a whitelist of applications allowed for installation on a system. Students will compare the list against multiple hosts and remove the installed applications which are not on the list.	CYBRScore Scored Labs	Operating Systems Hardening (OSH); Topics: 1, 2, 3, 4, 5, 6, 7, 8, 10, 11	Hyper-V	1 Hour	1 Hour	16 minutes, 37 seconds	1 minute, 32 seconds
Baseline Systems in Accordance with Policy Documentation	Students will compare the list against multiple hosts and remove the installed applications which are not on the list.	CYBRScore Labs	Operating Systems Hardening (OSH); Topics: 1, 2, 3, 4, 5, 6, 7, 8, 10, 11	Hyper-V	1 Hour	1 Hour	8 minutes, 18 seconds	35 seconds
Basic Linux x64 Binary Exploitation Challenge	In this lab, you are presented with a challenge binary. Combining all the skills that you learned in the Binary Exploitation Lab Series, you will need to write an exploit for this binary.	CYBRScore Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10	Hyper-V	10 Hours	10 Hours	13 minutes, 57 seconds	1 minute, 2 seconds
Basic Linux x64 Binary Exploitation with pwntools	In this lab, we will look at some basic binary exploitation in 64 bit Linux. We will be looking at assembly code as part of the exploit development process. You don't need to be an expert with assembly code, and we will be explaining all the code that we examine.	CYBRScore Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10	Hyper-V	2 Hours	2 Hours	8 hours, 25 minutes	1 minute, 46 seconds
Basics of Metasploit	In this lab we will dive into exploiting machines in our test environment. Some of the machines in this network are easy to exploit, and some are a bit more challenging. Throughout the process, we will wait through how to use Metasploit and a few additional tools to gather information and exploit the vulnerabilities.	CYBRScore Scored Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10	Hyper-V	1 Hour	1 Hour, 30 Minutes	1 hour, 7 minutes	38 seconds
BCP DRP and Test Planning	Students will become familiar with the Business Continuity Plan (BCP), Business Impact Assessment (BIA) and Disaster Recovery Plan (DRP). During the course of the lab, students will perform a gap analysis on the provided BCP, BIAs and DRP, and make the necessary fixes to those documents. After revising the previous documents the students	CYBRScore Labs	Cybersecurity Planning and Management (CPM); Topics: 2, 4, 5, 6, 8, 9	Hyper-V	4 Hours	4 Hours	54 minutes, 27 seconds	30 seconds
	will create a test for the covered assets, procedures and personnel.							
BitCoin Mining Web Application on Corporate Network	will create a test for the covered assets, procedures and personnel. Students will identify unauthorized activity on a corporate network. Students will then identify what type of cyber incident may have occurred and determine the attack vector. Finally, Students will collect information on the incident in order to prepare an incident Response report.	CYBRScore Labs	Vulnerability Analysis (VLA); Topics: 1, 3, 4, 5, 6, 7, 8, 10	Hyper-V	45 Minutes	45 Minutes	24 minutes, 46 seconds	41 seconds
BitCoin Mining Web Application on Corporate Network BitLocker Setup	Students will identify unauthorized activity on a corporate network. Students will then identify what type of cyber incident may have occurred and determine the attack vector. Finally, Students will collect information on the incident in order to prepare an incident	CYBRScore Labs	Vulnerability Analysis (VLA); Topics: 1, 3, 4, 5, 6, 7, 8, 10 Operating Systems Hardening (OSH); Topics: 1, 2, 3, 4, 5, 6, 7, 8, 10, 11	Hyper-V	45 Minutes 30 Minutes	45 Minutes 45 Minutes	24 minutes, 46 seconds	

Block Incoming Traffic on Known Port	In this lab, the student will respond to an incident by blocking incoming traffic on a	CYBRScore Scored Labs	Network Defense (NDF). Topics: 1a. 1c. 1d. 2a. 2b. 4a	Hyper-V	1 Hour	1 Hour	20 minutes, 53 seconds	1 minute, 41 seconds
Block Incoming Traffic on Known Port	known port from a specific IP. In this lab, the student will respond to an incident by blocking incoming traffic on a	CYBRScore Labs	Network Defense (NDF), Topics. 1a, 1c, 1d, 2a, 2b, 4a	Hyper-V	1 Hour	1 Hour	18 minutes, 30 seconds	49 seconds
Block Incoming Traffic on Known Port	known port from a specific IP. In this lab, the student will respond to an incident by blocking incoming traffic on a	CYBRScore Network Forensics	Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a	Hyper-V	1 Hour	1 Hour	19 minutes, 20 seconds	26 seconds
	known port from a specific IP. In this lab you will manually upload log data to Splunk. You will also configure Splunk and							
Centralized Monitoring	linux sysiog to automate the process of centrally locating log data.		Windows System Administration (WSA), Topics: 2, 4, 6	Hyper-V	1 Hour	1 Hour	23 minutes, 22 seconds	26 seconds 28 seconds
Check for Indicators of Other Attack Activity (Debug PE File) CIRP Creation After Cyber Attacks	Students will check for indications of other attack activity. With the help of a template and a good deal of supporting documentation (to include various Computer Incident Recovery Team reports, the Disaster Recovery Plan and other sources) Students will create a Computer Incident Recovery Plan.	CYBRScore Labs CYBRScore Labs	Software Security Analysis (SSA); Topics: 1, 2, 3, 4, 5 Cybersecurity Planning and Management (CPM); Topics: 2, 4, 5, 6, 8, 9	Hyper-V Hyper-V	1 Hour, 30 Minutes	1 Hour, 30 Minutes 1 Hour, 30 Minutes	50 minutes, 33 seconds 51 seconds	28 seconds 45 seconds
CIRP Creation After Cyber Attacks	With the help of a template and a good deal of supporting documentation, students will create a Computer Incident Recovery Plan.		Cybersecurity Planning and Management (CPM); Topics: 2, 4, 5, 6, 8, 9	Hyper-V	1 Hour	1 Hour, 30 Minutes	1 hour, 20 minutes	43 seconds
CIRP Creation After Cyber Attacks Capstone	With the help of a template and a good deal of supporting documentation, students will create a Computer Incident Recovery Plan.	CYBRScore Capstones	Cybersecurity Planning and Management (CPM): Topics: 2, 4, 5, 6, 8, 9	Hyper-V	1 Hour, 30 Minutes	2 Hours	1 minute, 1 second	
CIRP Creation and Disaster	create a Computer Incoent Necovery Plan. Students will become familiar with the creation of a Cyber Incident Response Plan (CIRP). During the course of the lab, the student will also run through a table-top run simulated cyber incident within will help them validate the earlier changes made to the Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP), as well as the newly created CIRP.	CYBRScore Labs	Cybersecurity Planning and Management (CPM); Topics: 2, 4, 5, 6, 8, 9	Hyper-V	2 Hours, 30 Minutes	5 Hours	46 minutes, 38 seconds	27 seconds
CIRP Creation and Disaster	Continuity Plan (BCP) and Disaster Recovery Plan (DRP), as well as the newly created CIRP.	CYBRScore Scored Labs	Cybersecurity Planning and Management (CPM); Topics: 2, 4, 5, 6, 8, 9	Hyper-V	1 Hour, 30 Minutes	3 Hours	52 minutes, 1 second	1 minute, 23 seconds
CIRP Creation and Review of BCP and DRP	Students will become familiar with the creation of a Cyber Incident Response Plan (IRP). During the course of the lab, the student will also run through a table-top on simulated cyber incident which will help them validate the earlier changes made to the Business Continuity Plan (BCP) and Disaster Recovery Plan (IRP), as well as the newly created (IRP.	CYBRScore Labs	Cybersecutity Planning and Management (CPM); Topics: 2, 4, 5, 6, 8, 9	Hyper-V	1 Hour, 30 Minutes	3 Hours	58 minutes, 52 seconds	24 seconds
Client Side Exploitation with Social Engineering	and how easy it is to fall victim to one.	CYBRScore Scored Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10	Hyper-V	1 Hour	1 Hour	1 hour, 23 minutes	44 seconds
Client Side Exploitation with Social Engineering (External)	In this lab you will practice a social engineering attack, performing actions as both the attacker and as the victim, in order to demonstrate how a simple phishing attack looks, and how easy it is to fall victim to one.	CYBRScore Scored Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10	Hyper-V	1 Hour	1 Hour	39 minutes, 28 seconds	34 seconds
Client Side Exploitation with Social Engineering (Scored)	In this lab you will practice a social engineering attack, performing actions as both the attacker and as the victim, in order to demonstrate how a simple phishing attack looks, and how easy it is to fall victim to one.	CYBRScore Scored Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10	Hyper-V	1 Hour	1 Hour	38 minutes, 20 seconds	1 minute, 8 seconds
Clonezilla_Network	As a incident responder, it's important to understand how to create baseline templates. You will learn how Clonezilla may be used to create a baseline Windows 7 image. You'll also learn how to deploy a PXE boot image using WDS.	CYBRScore Labs	Network Forensics; Topics: 1, 2, 6	Hyper-V	46 Minutes	1 Hour	7 minutes, 47 seconds	23 seconds
Collecting Logs and Verifying Syslog Aggregation	Collecting and aggregating logs are very essential to any organization. There are many methods of collecting logs. Two methods are the push method (the target systems send the logs) and the pull method (where the logging device less) frough the logs (and the logs) and the pull method (where the logging device less) fluid loss (and the log aggregation, that is, ie. Syslog or RFC 5424. This lab will break this process up into a micro-step where logs will be aggregated in a virtual environment and then then verified that they are actually being received.	CYBRScore Labs	Operating System Concepts (OSC), Topics: 2, 4; Windows System Administration (WSA), Topics: 2, 7	Hyper-V	1 Hour, 30 Minutes	1 Hour, 30 Minutes	31 minutes, 56 seconds	30 seconds
Collecting Logs and Verifying Syslog Aggregation	Collecting and aggregating logs are very essential to any organization. There are many methods of collecting logs. Two methods are the push method (the target systems send the logs) and the goal method of where the logging device less plus list leg log off logs devices.). This lab will deal with the most common method, pull method, used today in log aggregation, that is, is. Syslog or RFC 5424. This lab will break this process up into a micro-step where logs will be aggregated in a virtual environment and then then verified that they are actually being received.	CYBRScore Scored Labs	Operating System Concepts (OSC), Topics: 2, 4; Windows System Administration (WSA), Topics: 2, 7	Hyper-V	1 Hour, 30 Minutes	1 Hour, 30 Minutes	32 minutes	1 minute, 4 seconds
Command-Line Python	Python for Network Security Administrators is an introductory Python course weighted toward security and networking topics. The course exposes students to common Python types, data manipulation, networking, command-line scripting, and parallel processing. This course introduces students to programming with Python, and upon completion, students will be able to script common security and networking functions.	CYBRScore Labs	Low Level Programming (LEP) — This isn't low level; however, no other specific KU exists for learning to code in this bootcamp-like setting	g Hyper-V	1 Hour	1 Hour	9 minutes, 34 seconds	52 seconds
Comparing Controls	Students will evaluate policies in place on a domain and apply those policies in accordance to organizational standards.	CYBRScore Labs	Operating Systems Hardening (OSH); Topics: 1, 2, 3, 4, 5, 6, 7, 8, 10, 11	Hyper-V	1 Hour	1 Hour	18 minutes, 14 seconds	37 seconds
Comparing Controls	Students will evaluate policies in place on a domain and apply those policies in accordance to organizational standards.	CYBRScore Scored Labs	Operating Systems Hardening (OSH); Topics: 1, 2, 3, 4, 5, 6, 7, 8, 10, 11	Hyper-V	1 Hour	1 Hour	5 minutes, 22 seconds	1 minute, 1 second
Comprehensive Threat Response	In this final lab, we will attempt to exercise all the relevant skills found in this domain. We are focusing on responding to incidents and the skills needed to address these sorts of problems at a practitioner level.	CYBRScore Labs	Operating Systems Hardening (OSH); Topics: 1, 2, 3, 4, 5, 6, 7, 8, 10, 11	Hyper-V	2 Hours	2 Hours	34 minutes, 57 seconds	40 seconds
Comprehensive Threat Response	In this final lab, we will attempt to exercise all the relevant skills found in this domain. We are focusing on responding to incidents and the skills needed to address these sorts of problems at a practitioner level.	CYBRScore Scored Labs	Operating Systems Hardening (OSH); Topics: 1, 2, 3, 4, 5, 6, 7, 8, 10, 11	Hyper-V	2 Hours	2 Hours	53 minutes, 38 seconds	1 minute, 24 seconds
Compromise Assessment with Crowd Response	In this lids students will nun Crowd Response to conduct an incident response that will generate incident response files that can be analyzed and used to conduct compromise assessment. Crowd Response is a part of a suite of tools sold by crowdstrike.com. The Crowd Response component if fire and can replace the traditional response tools by Synitemetals and a spood alternative.	CYBRScore Labs	Operating Systems Hardening (OSH); Topics: 1, 2, 3, 4, 5, 6, 7, 8, 10, 11	Hyper-V	48 Minutes	1 Hour	34 minutes, 1 second	39 seconds
Conduct Baseline Comparison for Indicators of Compromise	Learners will create a system baseline operating snapshot using the Window Forensic Toolchest (WFT) and compare it against a previously created baseline using the KDiff3 application to identify any deviations from the known-good baseline.	CYBRScore Labs	Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10	Hyper-V	1 Hour	1 Hour	31 minutes, 32 seconds	46 seconds
Conduct Log Analysis and Cross Examination for False Positives	Students will confirm the validity of event-data analysis to eliminate false-positive events.	CYBRScore Scored Labs	Windows System Administration (WSA), Topics: 2, 4, 6, 7 - Operating System Concepts (OSC), Topics: 2, 4	Hyper-V	30 Minutes	1 Hour	18 minutes, 54 seconds	1 minute, 9 seconds
Conduct Log Analysis and Cross Examination for False Positives	Students will confirm the validity of event-data analysis to eliminate false-positive events.	CYBRScore Labs	Windows System Administration (WSA), Topics: 2, 4, 6, 7 - Operating System Concepts (OSC), Topics: 2, 4	Hyper-V	1 Hour	1 Hour	15 minutes, 23 seconds	21 seconds
	events.		Topica. 2, 4					

Conduct Root Cause Analysis for System Crashes	Students will use utilize a specially loaded system to conduct analysis on a captured memory dump from a machine suffering from repeating system craches. Using a memory analysis tool the students will waith through the process of discovering what is running on the affected system and will be these odd behaviors are classing the craches. This lab will foster tool familiarization and will provide the students with another layer of detail on how the Windows kernel interacts with memory, as well as the various processes involved.	CYBRScore Scored Labs	Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10	Hyper-V	45 Minutes	1 Hour	34 minutes, 7 seconds	1 minute, 1 second
Conduct Root Cause Analysis for System Crashes	Students will use utilize a specially loaded system to conduct analysis on a captured memory dump from a machine that suffers from repeating system crashes. Using a memory analysis tool the students will wait hrough the proses of discovering what is running on the affected system and why these odd behaviors are causing the crashes. This lab will foster tool familiarization and will provide the students another layer of detail on the foster tool familiarization and will provide the students another layer of detail on the Vindows kernel interacts with memory, as well as various processes.	CYBRScore Labs	Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10	Hyper-V	45 Minutes	1 Hour	18 minutes, 4 seconds	17 seconds
Conduct Root Cause Analysis for System Crashes Capstone	This lab will foster tool familiarization and will provide the students with another layer of detail on how the Windows kernel interacts with memory, as well as the various processes involved.	CYBRScore Capstones	Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10	Hyper-V	45 Minutes	1 Hour	18 minutes, 29 seconds	1 minute, 27 seconds
Conduct Supplemental Monitoring	In this lab you implement supplemental monitoring solutions on a network using various	CYBRScore Labs	Network Security Administration (NSA); Topics: 2, 5, 7, 8, 9, 10	Hyper-V	30 Minutes	30 Minutes	13 minutes, 15 seconds	39 seconds
Control Assessment and Evaluation	Microsoft security tools and built-ins. Sudents start off the lab by reviewing are a list of security controls which are to be applied to systems on a fictifious corporate network. They will follow up by using a couple of security auditing tools to perform a real-world assessment of a system on this network. The goal is to have students determine if the system has the required controls in place and if not for them to draft a report concerning their findings.	CYBRScore Labs	Operating Systems Concepts (OSC), Topics: 8	Hyper-V	1 Hour	1 Hour	1 minute, 13 seconds	18 seconds
Control Assessment and Evaluation	Students are provided a list of controls and a system. They are to ensure that the controls that are provided in the documentation are present on the system.	CYBRScore Scored Labs	Operating Systems Concepts (OSC), Topics: 8	Hyper-V	1 Hour	1 Hour	30 minutes, 18 seconds	1 minute, 4 seconds
Control Assessment and Evaluation	Students start off the lab by reviewing are a list of security controls which are to be applied to systems on a fictibious corporate network. They will follow up by using a couple of security adulting tools to perform a real-world assessment of a system on this network. The goal is to have students determine if the system has the required controls in place and if not for them to draft a report concerning life infindings.	CYBRScore Scored Labs	Operating Systems Concepts (OSC), Topics: 8	Hyper-V	1 Hour	1 Hour	24 minutes, 33 seconds	40 seconds
Core Impact Vulnerability Scan	This exercise will introduce students to the advanced settings within the Core Impact. Students will modify scan settings to perform different types of scans and to learn about the different functionalities Core Impact provides. Students will then compare the results of a Core Impact scan to the results of a port scan against the same target and discuss the differences and similarities between the two tools. Lastly, students will use the reporting feature to generate Core Impact reports.	CYBRScore Labs	Operating Systems Hardening (OSH), Topics: 11; IT Systems Components (ISC), Topics: 13	Hyper-V	2 Hours	2 Hours	11 minutes, 35 seconds	38 seconds
Core Impact Vulnerability Scan	This exercise will introduce students to the advanced settings within the Core Impact. Students will modify scan settings to perform different types of scans and to learn about the different functionalities Core Impact provides. Students will then compare the results of a Core Impact scan to the results of a port scan against the same target and discuss the differences and similarities between the two tools. Lastly, students will use the reporting feature to generate Core Impact reports.	CYBRScore Scored Labs	Operating Systems Hardening (OSH), Topics: 11; IT Systems Components (ISC), Topics: 13	Hyper-V	1 Hour, 30 Minutes	3 Hours	29 minutes, 22 seconds	2 minutes, 36 seconds
Core Impact Web Application Penetration Testing	This lab introduces students to the web application penetration testing suite within the Core Impact application.	CYBRScore Scored Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10	Hyper-V	10 Hours	10 Hours	23 minutes, 15 seconds	54 seconds
Core Impact Web Application Penetration Testing	This lab introduces students to the web application penetration testing suite within the Core Impact application.	CYBRScore Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10	Hyper-V	1 Hour	1 Hour	1 hour, 11 minutes	42 seconds
Create Custom Snort Rules	You will configure snort as an IDS. Additionally, you have received the following indicators during an active intrusion investigation. You are going to eliminate the existing snort rules and run a packet capture against this snort rule which will be later deployed to detect network activity using these indicators.	CYBRScore Scored Labs	Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a	Hyper-V	1 Hour, 30 Minutes	3 Hours	46 minutes, 32 seconds	1 minute, 22 seconds
Create Custom Snort Rules	You will configure snort as an IDS. Additionally, you have received the following indicators during an active intrusion investigation. You are going to eliminate the existing snort nuks and run a packet capture against this snort rule which will be later deployed to detect network activity using these indicators.	CYBRScore Labs	Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a	Hyper-V	1 Hour	1 Hour	24 minutes, 41 seconds	35 seconds
Create Custom Snort Rules Create Custom Snort Rules	Indicators during an active intrusion investigation. You are going to eliminate the existing snort use and run a packet capture against this sort to lew hich will be later deployed to detect network activity using these indicators. You will configure snort as an IDS. Additionally, you have received the following indicators during an active intrusion investigation. You are going to eliminate the existing snort rules and run a packet capture against this snort rule which will be later deployed to detect network activity, using these indicators.	CYBRScore Labs CYBRScore Network Forensics	Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a	Hyper-V	1 Hour	1 Hour		35 seconds 46 seconds
	Indicators during an active intrusion investigation. You are going to eliminate the estings non-tunk and man packet capture against this nort to lew hich will be later deployed to detect network activity using these indicators. You will configure sont as an IDS. Additionally, you have received the following indicators during an active intrusion investigation. You are going to eliminate the existing snort rules and run a packet capture against this snort rule which will be later deployed to detect network activity using these indicators. Students will run Windows Forensis Toolchest against an existing system to create a baseline that will be used for future analysis.						28 minutes, 22 seconds	
Create Custom Snort Rules	indicator during an active intrusion investigation. You are going to eliminate the existing snort rules and run a packet capture against this sort it elsewhich will be later deployed to detect network activity using these indicators. You will configure snort as an IDS. Additionally, you have received the following indicators during an active intrusion intestigation. You are going to eliminate the existing snort rules and run a packet capture against this snort rule which will be later deployed to detect network activity suign these indicators. Students will run Windows Forensk Todchest against an existing system to create a baseline that will be used for future analysis. Students will run Windows Forensk Todchest against an existing system to create a baseline that will be used for future analysis.	CYBRScore Network Forensics CYBRScore Scored Labs CYBRScore Labs	Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a	Hyper-V	1 Hour	1 Hour	28 minutes, 22 seconds 29 minutes, 19 seconds	46 seconds
Create Custom Snort Rules Creating a Baseline Using the Windows Forensic Toolchest (WFT)	Indicators during an active intrusion investigation. You are going to eliminate the existing snort lives and on a packet capture against this sort live which will be later deployed to detect network activity using these indicators. You will configure snort as an IDS. Additionally, you have received the following indicators during an active intrusion investigation. You are going to eliminate the existing snort rules and run a packet capture against this snort rule which will be later deployed to detect network activity sign these indicators. Students will run Windows Forensic Toolchest against an existing system to create a baseline that will be used for future analysis. Students will run Windows Forensic Toolchest against an existing system to create a baseline that will be used for future analysis.	CYBRScore Network Forensics CYBRScore Scored Labs CYBRScore Labs CYBRScore Labs	Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10	Hyper-V	1 Hour 30 Minutes	1 Hour 30 Minutes	28 minutes, 22 seconds 29 minutes, 19 seconds	46 seconds 1 minute, 17 seconds
Create Custom Snort Rules Creating a Baseline Using the Windows Forensic Toolchest (WFT) Creating a Baseline Using the Windows Forensic Toolchest (WFT)	Indicators during an active intrusion investigation. You are going to eliminate the existing snort rules and run a packet capture against this sort rule which will be later deployed to detect network activity using these indicators. You will configure snort as an IDS. Additionally, you have received the following indicators during an active intrusion investigation. You are going to eliminate the existing snort rules and run a packet capture against this snort rule which will be later deployed to detect network activity sign these indicators. Students will run Windows Forensic Toolchest against an existing system to create a baseline that will be used for future analysis. Students will run Windows Forensic Toolchest against an existing system to create a baseline that will be used for future analysis. In this lab students will become family with creating a lab in Autopsy. Students will also that the students of the properties of the properties of the students will be some family with creating a lab in Autopsy. Students will also baseness familiar with creating a lab in Autopsy. Students will also baseness familiar with creating a lab in Autopsy. Students will also baseness familiar with creating a lab in Autopsy. Students will also	CYBRScore Network Forensics CYBRScore Scored Labs CYBRScore Labs CYBRScore Labs CYBRScore Labs	Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10	Hyper-V Hyper-V	1 Hour 30 Minutes 30 Minutes	1 Hour 30 Minutes 30 Minutes	28 minutes, 22 seconds 29 minutes, 19 seconds 5 minutes, 20 seconds	46 seconds 1 minute, 17 seconds 49 seconds
Create Custom Snort Rules Creating a Baseline Using the Windows Forensic Tookchest (WFT) Creating a Baseline Using the Windows Forensic Tookchest (WFT) Creating a Case in Autopsy	noticators during an active intrusion investigation. You are going to eliminate the existing sont rules and run a packet capture against this sont rule which will be later deployed to detect network activity using these indicators. You will configure sont as an IDS. Additionally, you have received the following indicators during an active intrusion investigation. You are going to eliminate the existing sont rules and run a packet capture against this sont rule which will be later deployed to detect network activity using these indicators. Students will run Windows Forensic Tochest against an existing system to create a baseline that will be used for future analysis. Students will run Windows Forensic Tochest against an existing system to create a baseline that will be used for future analysis. In this lab students will become familiar with creating a lab in Autopsy. Students will also become familiar with the use of Autopsy. In this lab students will become familiar with creating a lab in Autopsy. Students will also become familiar with the use of Autopsy.	CYBRScore Network Forensics CYBRScore Scored Labs CYBRScore Labs CYBRScore Labs CYBRScore Labs	Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10	Hyper-V Hyper-V Hyper-V	1 Hour 30 Minutes 30 Minutes 2 Hours 2 Hours	1 Hour 30 Minutes 30 Minutes 3 Hours	28 minutes, 22 seconds 29 minutes, 19 seconds 5 minutes, 20 seconds 14 minutes, 41 seconds	46 seconds 1 minute, 17 seconds 49 seconds 44 seconds
Create Custom Snort Rules Creating a Baseline Using the Windows Forensic Tookchest (WFT) Creating a Baseline Using the Windows Forensic Tookchest (WFT) Creating a Case in Autopsy Creating a Case in Autopsy	Indicators during an active intrusion investigation. You are going to eliminate the existing snort fuels and nat packet capture against this sort to lew hich will be later deployed to detect network activity using these indicators. You will configure snort as an IDS. Additionally, you have received the following indicators during an active intrusion investigation. You are going to eliminate the existing snort rules and run a packet capture against this snort rule which will be later deployed to detect network activity using these indicators. Students will run Windows Forensic Toolchest against an existing system to create a baseline that will be used for future analysis. Students will run Windows Forensic Toolchest against an existing system to create a baseline that will be used for future analysis. Students will run Windows Forensic Toolchest against an existing system to create a baseline that will be used for future analysis. In this is students will become familiar with creating a lab in Autopsy. Students will also become familiar with the use of Autopsy. In this lab students will become familiar with creating a lab in Autopsy. Students will also become familiar with the use of Autopsy.	CYBRScore Network Forensics CYBRScore Scored Labs CYBRScore Labs CYBRScore Labs CYBRScore Labs	Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10	Hyper-V Hyper-V Hyper-V Hyper-V	1 Hour 30 Minutes 30 Minutes 2 Hours 2 Hours 2 Hours	1 Hour 30 Minutes 30 Minutes 3 Hours 3 Hours	28 minutes, 22 seconds 29 minutes, 19 seconds 5 minutes, 20 seconds 14 minutes, 41 seconds 36 minutes, 51 seconds	46 seconds 1 minute, 17 seconds 49 seconds 44 seconds
Create Custom Snort Rules Creating a Baseline Using the Windows Forensic Toolchest (WFT) Creating a Baseline Using the Windows Forensic Toolchest (WFT) Creating a Case in Autopsy Creating a Case in Autopsy Creating a Case in Autopsy	Indicators during an active intrusion investigation. You are going to eliminate the estings non-tules and nur a packet capture against this nort to lew hich will be later deployed to detect network activity using these indicators. You will configure sont as an IDS. Additionally, you have received the following indicators during an active intrusion investigation. You are going to eliminate the existing snort rules and run a packet capture against this snort rule which will be later deployed to detect network activity using these indicators. Students will run Windows Forensic Toolchest against an existing system to create a basseline that will be used for future analysis. Students will run Windows Forensic Toolchest against an existing system to create a basseline that will be used for future analysis. In this lib students will become familiar with creating a lab in Autopsy. Students will also become familiar with the use of Autopsy. In this lib students will become familiar with creating a lab in Autopsy. Students will also become familiar with the use of Autopsy. The control of Autopsy is the students will also become familiar with the use of Autopsy. In this lib students will also the control familiar with the use of Autopsy. In this lib students will become familiar with creating a lab in FTK. Students will also become familiar with the use of Autopsy.	CYBRScore Network Forensics CYBRScore Scored Labs CYBRScore Labs CYBRScore Scored Labs CYBRScore Digital Media Forensics CYBRScore Scored Labs	Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a Host Forensics (HOP); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOP); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOP); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOP); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOP); Topics: 1, 5, 6, 7, 8, 9, 10	Hyper-V Hyper-V Hyper-V Hyper-V Hyper-V	1 Hour 30 Minutes 30 Minutes 2 Hours 2 Hours 2 Hours	1 Hour 30 Minutes 30 Minutes 31 Hours 3 Hours 3 Hours	28 minutes, 22 seconds 29 minutes, 19 seconds 5 minutes, 20 seconds 14 minutes, 41 seconds 36 minutes, 51 seconds	46 seconds 1 minute, 17 seconds 49 seconds 44 seconds 44 seconds
Create Custom Snort Rules Creating a Baseline Using the Windows Forensic Toolchest (WFT) Creating a Baseline Using the Windows Forensic Toolchest (WFT) Creating a Case in Autopsy Creating a Case in Autopsy Creating a Case in Autopsy Creating a Case in FTK	Indicator during an active intrusion investigation. You are going to eliminate the esting snort rules and run a packet capture against this sort rule which will be later deployed to detect network activity using these indicators. You will configure snort as an IDS. Additionally, you have received the following indicators during an active intrusion investigation. You are going to eliminate the existing snort rules and run a packet capture against this snort rule which will be later deployed to detect network activity using these indicators. Students will run Windows Forensic Toolchest against an existing system to create a basseline that will be used for future analysis. Students will run Windows Forensic Toolchest against an existing system to create a basseline that will be used for future analysis. In this list students will become familiar with creating a lab in Autopsy. Students will also become familiar with the use of Autopsy. In this list students will become familiar with creating a lab in Autopsy. Students will also become familiar with the use of Autopsy. In this list students will become familiar with creating a lab in FTK. Students will also become familiar with the use of Autopsy. In this list students will become familiar with creating a lab in FTK. Students will also become familiar with the use of FTK. In this list is students will become familiar with creating a lab in FTK. Students will also become familiar with the use of FTK.	CYBRScore Network Forensics CYBRScore Scored Labs CYBRScore Labs CYBRScore Scored Labs CYBRScore Digital Media Forensics CYBRScore Scored Labs	Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10	Hyper-V Hyper-V Hyper-V Hyper-V Hyper-V Hyper-V	1 Hour 30 Minutes 30 Minutes 2 Hours 2 Hours 2 Hours 2 Hours 2 Hours	1 Hour 30 Minutes 30 Minutes 3 Hours 3 Hours 2 Hours, 30 Minutes	28 minutes, 22 seconds 29 minutes, 19 seconds 5 minutes, 20 seconds 14 minutes, 41 seconds 36 minutes, 51 seconds 52 minutes, 28 seconds	46 seconds 1 minute, 17 seconds 49 seconds 44 seconds 44 seconds
Create Custom Snort Rules Creating a Baseline Using the Windows Forensic Toolchest (WFT) Creating a Baseline Using the Windows Forensic Toolchest (WFT) Creating a Case in Autopsy Creating a Case in Autopsy Creating a Case in Autopsy Creating a Case in FTK Creating a Case in FTK	indicators during an active intrusion investigation. You are going to eliminate the existing snort rules and run a packet capture against this sort rule which will be later deployed to detect network activity using these indicators. You will configure snort as an IDS. Additionally, you have received the following indicators during an active intrusion investigation. You are going to eliminate the existing snort rules and run a packet capture against this snort rule which will be later deployed to detect network activity using these indicators. Students will run Windows Forensis Toolchest against an existing system to create a baseline that will be used for future analysis. Students will run Windows Forensis Toolchest against an existing system to create a baseline that will be used for future analysis. In this lab students will become familiar with creating a lab in Autopsy. Students will also become familiar with the use of Autopsy. In this lab students will become familiar with creating a lab in Autopsy. Students will also become familiar with the use of Autopsy for creating a lab in FTK. Students will also become familiar with the use of Autopsy in the creating a lab in FTK. Students will also become familiar with the use of Autopsy with creating a lab in FTK. Students will also become familiar with the use of Autopsy will also become familiar with the use of FTK.	CYBRScore Network Forensics CYBRScore Scored Labs CYBRScore Labs CYBRScore Labs CYBRScore Labs CYBRScore Digital Media Forensics CYBRScore Scored Labs CYBRScore Digital Media Forensics CYBRScore Digital Media Forensics CYBRScore Digital Media Forensics CYBRScore Digital Media Forensics	Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10	Hyper-V Hyper-V Hyper-V Hyper-V Hyper-V Hyper-V Hyper-V	1 Hour 30 Minutes 30 Minutes 2 Hours 2 Hours 2 Hours 2 Hours 2 Hours 2 Hours	1 Hour 30 Minutes 30 Minutes 3 Hours 3 Hours 2 Hours, 30 Minutes 2 Hours, 30 Minutes	28 minutes, 22 seconds 29 minutes, 19 seconds 5 minutes, 20 seconds 14 minutes, 41 seconds 36 minutes, 51 seconds 52 minutes, 28 seconds	46 seconds 1 minute, 17 seconds 49 seconds 44 seconds 44 seconds 1 minute, 33 seconds
Create Custom Snort Rules Creating a Baseline Using the Windows Forensic Toolchest (WFT) Creating a Baseline Using the Windows Forensic Toolchest (WFT) Creating a Case in Autopsy Creating a Case in Autopsy Creating a Case in Autopsy Creating a Case in FTK Creating a Case in FTK Creating a Case in FTK Creating a Case in OSF	indicators during an active intrusion investigation. You are going to eliminate the existing snort rules and run a packet capture against this sort rule which will be later deployed to detect network activity using these indicators. You will configure snort as an IDS. Additionally, you have received the following indicators during an active intrusion investigation. You are going to eliminate the existing snort rules and run a packet capture against this snort rule which will be later deployed to detect network activity using these indicators. Students will run Windows Forensis Toolchest against an existing system to create a baseline that will be used for future analysis. Students will run Windows Forensis Toolchest against an existing system to create a baseline that will be used for future analysis. In this lab students will become familiar with creating a lab in Autopsy. Students will also become familiar with the use of Autopsy. In this lab students will become familiar with creating a lab in Autopsy. Students will also become familiar with the use of Autopsy. In this lab students will become familiar with creating a lab in FTK. Students will also become familiar with the use of Autopsy. In this lab students will become familiar with creating a lab in FTK. Students will also become familiar with the use of Autopsy with reating a lab in FTK. Students will also become familiar with the use of Autopsy with creating a lab in FTK. Students will also become familiar with the use of Otsomeriscs.	CYBRScore Network Forensics CYBRScore Scored Labs CYBRScore Labs CYBRScore Labs CYBRScore Labs CYBRScore Digital Media Forensics CYBRScore Digital Media Forensics CYBRScore Digital Media Forensics CYBRScore Digital Media Forensics CYBRScore Labs CYBRScore Labs	Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10	Hyper-V Hyper-V Hyper-V Hyper-V Hyper-V Hyper-V Hyper-V Hyper-V Hyper-V	1 Hour 30 Minutes 30 Minutes 2 Hours 2 Hours 2 Hours 2 Hours 2 Hours 2 Hours	1 Hour 30 Minutes 30 Minutes 3 Hours 3 Hours 2 Hours, 30 Minutes 2 Hours, 30 Minutes 2 Hours, 30 Minutes 2 Hours, 30 Minutes	28 minutes, 22 seconds 29 minutes, 19 seconds 5 minutes, 20 seconds 14 minutes, 41 seconds 36 minutes, 51 seconds 52 minutes, 28 seconds	46 seconds 1 minute, 17 seconds 49 seconds 44 seconds 44 seconds 1 minute, 33 seconds
Create Custom Snort Rules Creating a Baseline Using the Windows Forensic Toolchest (WFT) Creating a Baseline Using the Windows Forensic Toolchest (WFT) Creating a Case in Autopsy Creating a Case in Autopsy Creating a Case in Autopsy Creating a Case in FTK Creating a Case in FTK Creating a Case in FTK Creating a Case in OSF Creating a Case in OSF	Indicators during an active intrusion investigation. You are going to eliminate the estings not rule as oft an apacket capture against this nort to lew which will be later deployed to detect network activity using these indicators. You will configure sont as an IDS. Additionally, you have received the following indicators during an active intrusion investigation. You are going to eliminate the existing snort rules and run a packet capture against this snort rule which will be later deployed to detect network activity using these indicators. Students will run Windows Forensic Toolchest against an existing system to create a basseline that will be used for future analysis. Students will run Windows Forensic Toolchest against an existing system to create a basseline that will be used for future analysis. In this lab students will become familiar with creating a lab in Autopsy. Students will also become familiar with the use of Autopsy. In this lab students will become familiar with creating a lab in Autopsy. Students will also become familiar with the use of Autopsy in the Control of Autopsy. In this lab students will become familiar with creating a lab in FTC. Students will also become familiar with the use of Autopsy in the creating a lab in FTC. Students will also become familiar with the use of TFC. In this lab students will become familiar with creating a lab in FTC. Students will also become familiar with the use of OSForensics. In this lab students will become familiar with creating a lab in OSForensics. Students will also become familiar with the use of OSForensics.	CYBRScore Network Forensics CYBRScore Scored Labs CYBRScore Labs CYBRScore Labs CYBRScore Labs CYBRScore Digital Media Forensics CYBRScore Labs CYBRScore Scored Labs	Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10	Hyper-V	1 Mour 30 Minutes 30 Minutes 2 Hours 2 Hours 2 Hours 2 Hours 1 Hours 1 Hours 1 Hours	1 Hour 30 Minutes 30 Minutes 3 Hours 3 Hours 3 Hours 2 Hours, 30 Minutes 2 Hours, 30 Minutes 1 Hours, 30 Minutes 1 Hour, 30 Minutes	28 minutes, 22 seconds 29 minutes, 19 seconds 36 minutes, 20 seconds 14 minutes, 13 seconds 36 minutes, 51 seconds 152 minutes, 28 seconds 1 hour, 19 minutes 24 minutes, 47 seconds	46 seconds 1 minute, 17 seconds 49 seconds 44 seconds 1 minute, 33 seconds 1 minute, 35 seconds 53 seconds
Create Custom Snort Rules Creating a Baseline Using the Windows Forensic Toolchest (WFT) Creating a Baseline Using the Windows Forensic Toolchest (WFT) Creating a Case in Autopsy Creating a Case in Autopsy Creating a Case in Autopsy Creating a Case in FTK Creating a Case in FTK Creating a Case in FTK Creating a Case in OSF Creating a Case in OSF	indicators during an active intrusion investigation. You are going to eliminate the estiting snort rules and run a packet capture against this sort rule which will be later deployed to detect network activity using these indicators. You will configure snort as an IOS. Additionally, you have received the following indicators during an active intrusion investigation. You are going to eliminate the existing snort rules and run a packet capture against this snort rule which will be later deployed to detect network activity using these indicators. Students will run Windows Forenski Toolchest against an existing system to create a baseline that will be used for future analysis. Students will run Windows Forenski Toolchest against an existing system to create a baseline that will be used for future analysis. Students will run Windows Forenski Toolchest against an existing system to create a baseline that will be used for future analysis. In this lab students will become familiar with creating a lab in Autopsy. Students will also become familiar with the use of Autopsy. In this lab students will become familiar with creating a lab in FFK. Students will also become familiar with the use of Autopsy. In this lab students will become familiar with creating a lab in FFK. Students will also become familiar with the use of Autopsy. In this lab students will become familiar with creating a lab in FFK. Students will also become familiar with the creating a lab in FFK. Students will also become familiar with creating a lab in GSForensics. Students will also become familiar with creating a lab in GSForensics. Students will also become familiar with the creating a lab in GSForensics. Students will also become familiar with the creating a lab in GSForensics. Students will also become familiar with the will creating a lab in GSForensics. Students will also become familiar with the will creating a lab in GSForensics. Students will also become familiar with the will creating a lab in GSForensics. Students will also become fami	CYBRScore Network Forensics CYBRScore Scored Labs CYBRScore Labs CYBRScore Labs CYBRScore Digital Media Forensics	Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10	Hyper-V	1 Hour 30 Minutes 30 Minutes 2 Hours 2 Hours 2 Hours 2 Hours 1 Hour 1 Hour	1 Hour 30 Minutes 30 Minutes 3 Hours 3 Hours 3 Hours 2 Hours, 30 Minutes 2 Hours, 30 Minutes 1 Hour, 30 Minutes 1 Hour, 30 Minutes 1 Hour, 30 Minutes	28 minutes, 22 seconds 29 minutes, 19 seconds 5 minutes, 20 seconds 14 minutes, 11 seconds 36 minutes, 51 seconds 1 minutes, 28 seconds 1 hour, 19 minutes 24 minutes, 47 seconds 54 minutes, 47 seconds	46 seconds 1 minute, 17 seconds 49 seconds 44 seconds 44 seconds 1 minute, 33 seconds 1 minute, 26 seconds 53 seconds
Create Custom Snort Rules Creating a Baseline Using the Windows Forensic Tookhest (WFT) Creating a Baseline Using the Windows Forensic Tookhest (WFT) Creating a Case in Autopsy Creating a Case in Autopsy Creating a Case in Autopsy Creating a Case in FTK Creating a Case in FTK Creating a Case in FTK Creating a Case in OSF	Indicators during an active intrusion investigation. You are going to eliminate the existing snort uses and na packet capture against this sont the which will be later deployed to detect network activity using these indicators. You will configure snort as an IDS. Additionally, you have received the following indicators during an active intrusion investigation. You are going to eliminate the existing snort rules and un a packet capture against this snort rule which will be later deployed to detect network activity using these indicators. Students will run Windows Forensic Toolchest against an existing system to create a baseline that will be used for future analysis. Students will run Windows Forensic Toolchest against an existing system to create a baseline that will be used for future analysis. In this list students will become familiar with creating a lab in Autopsy. Students will also become familiar with the use of Autopsy. In this list students will become familiar with creating a lab in Autopsy. Students will also become familiar with the use of Autopsy. In this list students will become familiar with creating a lab in FTK. Students will also become familiar with the use of Autopsy. In this list students will become familiar with creating a lab in FTK. Students will also become familiar with the use of FTK. In this list students will become familiar with creating a lab in FTK. Students will also become familiar with the use of FTK. In this list students will become familiar with creating a lab in OSForensics. Students will also become familiar with the use of OSForensics. In this list students will become familiar with creating a lab in OSForensics. Students will also become familiar with the use of OSForensics. In this list students will become familiar with creating a lab in OSForensics. Students will also become familiar with the use of OSForensics.	CYBRScore Network Forensics CYBRScore Scored Labs CYBRScore Labs CYBRScore Labs CYBRScore Digital Media Forensics	Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10	Hyper-V	1 Hour 30 Minutes 30 Minutes 2 Hours 2 Hours 2 Hours 2 Hours 1 Hour 1 Hour 1 Hour	1 Hour 30 Minutes 30 Minutes 3 Hours 3 Hours 3 Hours 2 Hours, 30 Minutes 2 Hours, 30 Minutes 1 Hours, 30 Minutes 1 Hour, 30 Minutes	28 minutes, 22 seconds 29 minutes, 19 seconds 5 minutes, 20 seconds 14 minutes, 21 seconds 36 minutes, 51 seconds 52 minutes, 28 seconds 1 hour, 19 minutes 24 minutes, 47 seconds 54 minutes, 26 seconds	46 seconds 1 minute, 17 seconds 49 seconds 44 seconds 1 minute, 33 seconds 1 minute, 23 seconds 53 seconds 1 minute, 17 seconds 5 minute, 17 seconds 6 seconds
Create Custom Snort Rules Creating a Baseline Using the Windows Forensic Toolchest (WFT) Creating a Baseline Using the Windows Forensic Toolchest (WFT) Creating a Case in Autopsy Creating a Case in Autopsy Creating a Case in Autopsy Creating a Case in FTK Creating a Case in FTK Creating a Case in FTK Creating a Case in OSF Creating a Forensic Image Creating a Forensic Image	Indicators during an active intrusion investigation. You are going to eliminate the existing snort uses and na packet capture against this sont the which will be later deployed to detect network activity using these indicators. You will configure snort as an IDS. Additionally, you have received the following indicators during an active intrusion investigation. You are going to eliminate the existing snort rules and run a packet capture against this snort rule which will be later deployed to detect network activity using these indicators. Students will run Windows Forensic Toolchest against an existing system to create a baseline that will be used for future analysis. Students will run Windows Forensic Toolchest against an existing system to create a baseline that will be used for future analysis. Students will run Windows Forensic Toolchest against an existing system to create a baseline that will be used for future analysis. In this lab students will become familiar with creating a lab in Autopsy. Students will also become familiar with the cere of Autopsy. In this lab students will become familiar with creating a lab in Autopsy. Students will also become familiar with the use of Autopsy. In this lab students will become familiar with creating a lab in FTK. Students will also become familiar with the use of Title. In this lab students will become familiar with creating a lab in FTK. Students will also become familiar with the use of TFK. In this lab students will become familiar with creating a lab in OSforensics. Students will also become familiar with the use of OSforensics. In this lab students will become familiar with creating a lab in OSforensics. Students will also become familiar with the use of OSforensics. In this lab students will become familiar with creating a lab in OSforensics. Students will also become familiar with the use of OSforensics. In this lab students will become familiar with creating a lab in OSforensics. Students will asso become familiar with the use of OSforensics.	CYBRScore Network Forensics CYBRScore Labs CYBRScore Labs CYBRScore Labs CYBRScore Digital Media Forensics CYBRScore Labs CYBRScore Labs CYBRScore Labs CYBRScore Digital Media Forensics CYBRScore Digital Media Forensics CYBRScore Digital Media Forensics CYBRScore Digital Media Forensics CYBRScore Labs CYBRScore Labs CYBRScore Scored Labs CYBRScore Scored Labs CYBRScore Digital Media Forensics CYBRScore Digital Media Forensics CYBRScore Scored Labs CYBRScore Scored Labs	Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10	Hyper-V	1 Hour 30 Minutes 30 Minutes 2 Hours 2 Hours 2 Hours 2 Hours 1 Hour 1 Hour 1 Hour 1 Hour 1 Hour	1 Hour 30 Minutes 30 Minutes 3 Mours 3 Mours 3 Hours 2 Hours, 30 Minutes 2 Hours, 30 Minutes 1 Hour, 30 Minutes	28 minutes, 22 seconds 29 minutes, 19 seconds 5 minutes, 20 seconds 14 minutes, 21 seconds 36 minutes, 21 seconds 14 minutes, 21 seconds 15 minutes, 28 seconds 1 hour, 19 minutes 24 minutes, 47 seconds 54 minutes, 26 seconds 1 minutes, 13 seconds 15 minutes, 43 seconds	46 seconds 1 minute, 17 seconds 49 seconds 44 seconds 1 minute, 33 seconds 1 minute, 33 seconds 53 seconds 1 minute, 17 seconds 1 minute, 26 seconds 53 seconds 1 minute, 27 seconds
Create Custom Snort Rules Creating a Baseline Using the Windows Forensic Toolchest (WFT) Creating a Baseline Using the Windows Forensic Toolchest (WFT) Creating a Case in Autopsy Creating a Case in Autopsy Creating a Case in Autopsy Creating a Case in FTK Creating a Case in FTK Creating a Case in OSF	indicators during an active intrusion investigation. You are going to eliminate the estiting snort rules and run a packet capture against this sort rule which will be later deployed to detect network activity using these indicators. You will configure snort as an IOS. Additionally, you have received the following indicators during an active intrusion investigation. You are going to eliminate the existing snort rules and run a packet capture against this snort rule which will be later deployed to detect network activity using these indicators. Students will run Windows Forensic Toolchest against an existing system to create a baseline that will be used for future analysis. Students will run Windows Forensic Toolchest against an existing system to create a baseline that will be used for future analysis. Students will run Windows Forensic Toolchest against an existing system to create a baseline that will be used for future analysis. In this lab students will become familiar with creating a lab in Autopsy. Students will also become familiar with the use of Autopsy. In this lab students will become familiar with creating a lab in Autopsy. Students will also become familiar with the use of Autopsy. In this lab students will become familiar with creating a lab in FTK. Students will also become familiar with the use of Autopsy. In this lab students will become familiar with the control of Autopsy. It is that the students will become familiar with the use of Autopsy. It is that is the students will become familiar with the control of Autopsy. It is that the students will become familiar with creating a lab in FTK. Students will also become familiar with the use of AUTopsy. It is not that the students will become familiar with the control of Autopsy. It is not that the students will become familiar with the use of AUTopsy. It is not that the students will become familiar with the use of AUTopsy. It is not the students will also become familiar with the use of AUTopsy. It is not that the students will also become fa	CYBRScore Network Forensics CYBRScore Scored Labs CYBRScore Labs CYBRScore Labs CYBRScore Labs CYBRScore Digital Media Forensics CYBRScore Labs CYBRScore Digital Media Forensics CYBRScore Labs CYBRScore Labs CYBRScore Labs CYBRScore Digital Media Forensics CYBRScore Digital Media Forensics	Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10	Hyper-V	1 Hour 30 Minutes 30 Minutes 2 Hours 2 Hours 2 Hours 2 Hours 1 Hour 1 Hour	1 Hour 30 Minutes 30 Minutes 3 Hours 3 Hours 3 Hours 2 Hours, 30 Minutes 2 Hours, 30 Minutes 1 Hour, 30 Minutes	28 minutes, 22 seconds 29 minutes, 19 seconds 5 minutes, 20 seconds 14 minutes, 21 seconds 36 minutes, 51 seconds 52 minutes, 28 seconds 1 hour, 19 minutes 24 minutes, 47 seconds 54 minutes, 26 seconds	46 seconds 1 minute, 17 seconds 49 seconds 44 seconds 1 minute, 33 seconds 1 minute, 33 seconds 53 seconds 1 minute, 17 seconds 5 minute, 17 seconds 6 seconds

Cesting a list of headerful regress, Sonotes and Least Accounts from a part of presental presentation and comments of the comment of the comm
Obesing a Secondary Baselina and Conducting Comparison Consider a Secondary Conduction (Consider a Secondary Consideration (1997) (Consideration Consideration Considerat
Operating Specimen and Companies and Companies and Expensional Companies and Expensional Companies and Expensional Companies and Companies and Expensional Companies and Expen
Uniforcity system and discover new own. They will preform an a study of the following and determining study of the following and determ
Coating Recommendations Based on Vulnerability Assessments Incling and effortier in the special per training of the following and special may be provided by the coation of special per training of the following and per provided by the coation of special per provided by the coation of specia
Well-reading Systems and discover new Ones. They will perform a risk analysis of the findings and entermine steps to be that no migrate the stores descreent. Findings and any supposed and report as an example, they will find to the recessing of determined steps to be readings and the responsible steps to the reliable steps. Creating SERM Reports with Splank Suderns will wait through the creation of SERM reports with Splank Suderns will wait through the creation of SERM reports with Splank Suderns will wait through the creation of SERM reports with Splank Suderns will wait through the creation of SERM reports with Splank Suderns will wait through the creation of SERM reports with Splank (Capstone) Suderns will wait through the creation of SERM reports with Splank (Capstone) Suderns will wait through the creation of SERM reports with Splank (Capstone) Suderns will wait through the creation of SERM reports with Splank (Capstone) Suderns will wait through the creation of SERM reports with Splank (Capstone) Suderns will wait through the creation of SERM reports with Splank (Capstone) Suderns will wait through the creation of SERM reports with Splank (Capstone) Suderns will wait through the creation of SERM reports with Splank (Capstone) Suderns will wait through the creation of SERM reports with Splank (Capstone) Suderns will wait through the creation of SERM reports with Splank (Capstone) Suderns will wait through the creation of SERM reports with Splank (Capstone) Suderns will wait through the creation of SERM reports with Splank (Capstone) Suderns will wait through the creation of SERM reports with Splank (Capstone) Suderns will be a capstone (Capsto
Creating SIEM Reports with Splunk Students will walk through the creation of SIEM reports using the SPLUNK tool. Creating SIEM Reports with Splunk (Capstone) Students will walk through the creation of SIEM reports using the SPLUNK tool. Creation of BCP and DRP Students will be required to create two documents: a Business Continuity Plan (BCP) and a Disaster Recovery Plan (DRP). Both documents deal with worst case scenarios concerning how to kneep business ping despite the occurrence of a natural disaster, catastrophic accident or serious man-made incident. This lab is designed to have the trainee become familiar with a "cradle to grave" approach dealing with universide machines, assessing them, resemble, blow to mitigate the threatily and penetrating a Standard Operating Procedures for Incident Recovery The lab is designed to have the trainee become familiar with a "cradle to grave" approach dealing with universide machines, assessing them, resemble, they have the threating a standard Operating procedures for Incident Recovery busines ping despited procedures for Incident Recovery and procedures for Incident Recovery and procedures for Incident Recovery and procedures for Recovery and procedures for Recovery approach dealing with universide machines, and as a sample windows 2008 server. They will perform any necessary remediations to the server be trained and penalized procedure to help others with the machine a Standard Operating Procedures to help others with the machine a Standard Operating procedure to help others with the machine a Standard Operating procedure to help others with the machine a Standard Operating procedure to help others with the machine a Standard Operating procedure to help others with the machine a standard operating procedure to help others with the machine a standard operating procedure to help others with the machine a standard operating procedure to help others with the machine a standard operating procedure to help others with the machine a standard operating procedure to hel
Creation of Standard Operating Procedures for Incident Recovery Creation of Standard Operating Procedures for Incident Recovery Creation of Standard Operating Procedures for Recovery Creation of Standard Operating Procedure for Recovery Crea
Students will be required to create two documents: a Business Continuity Plan (BCP) and a Disaster Recovery Plan (DRP). Both documents call with worst case scenarios concerning, how to keep business going depite the occurrence of a natural disaster, catastrophic accident or serious man-made incident. Creation of Standard Operating Procedures for Incident Recovery This lab is designed to have the trainee become familiar with "credite to grave" This lab is designed to have the trainee become familiar with "credite to grave" This lab is designed to have the trainee become familiar with "credite to grave" This lab is designed to have the trainee become familiar with "credite to grave" This lab is designed to have the trainee become familiar with "credite to grave" This lab is designed to have the trainee become familiar with "credite to grave" This lab is designed to have the trainee become familiar with "credite to grave" This lab is designed to have the trainee become familiar with "credite to grave" This lab is designed to have the trainee become familiar with "credite to grave" This lab is designed to have the trainee become familiar with "credite to grave" This lab is designed to have the trainee become familiar with "credite to grave" This lab is designed to have the trainee become familiar with "credite to grave" This lab is designed to have the trainee become familiar with "credit to grave" This lab is designed to have the trainee become familiar with "credit to grave" This lab is designed to have the trainee become familiar with "credit to grave" This lab is designed to have the trainee become familiar with a familiar to grave the standard of perating the credit (SOPI) for each standard of perating the credit (SOPI) for each standard of perating the procedure (SOPI) for each standard of pe
Ceation of BCP and DRP a Disaster Recovery Plan (DRP). Soft documents deal with worst case scenarios concerning, how to keep business going depite the occurrence of a natural disaster, concerning, how to keep business going depite the occurrence of a natural disaster, concerning how to keep business going depite the occurrence of a natural disaster, concerning how to keep business going depite the occurrence of a natural disaster, concerning how to keep business going depite the occurrence of a natural disaster. This lab is designed to have the traince become familiar with "cradle to grave" This lab is designed to have the traince become familiar with "cradle to grave" This lab is designed to have the traince become familiar with "cradle to grave" This lab is designed to have the traince become familiar with "cradle to grave" This lab is designed to have the traince become familiar with "cradle to grave" This lab is designed to have the traince become familiar with "cradle to grave" This lab is designed to have the traince become familiar with "cradle to grave" This lab is designed to have the traince become familiar with "cradle to grave" This lab is designed to have the traince become familiar with "cradle to grave" This lab is designed to have the traince become familiar with "cradle to grave" This lab is designed to have the traince become familiar with "cradle to grave" This lab is designed to have the traince become familiar with "cradle to grave" This lab is designed to have the traince become familiar with "cradle to grave" This lab is designed to have the traince become familiar with "cradle to grave" This lab is designed to have the traince become familiar with "cradle to grave" This lab is designed to have the traince become familiar with "cradle to grave" This lab is designed to have the traince become familiar with "cradle to grave" This lab is designed to have the traince become familiar with "cradle to grave" This lab is designed to have the traince become familiar with "cradl
percent dealing with vulnerable machines, assessing them, researching phone on miligate the threat(s) and generating a Standard Operating Procedures for Recovery Students will have access to the results of a vulnerability scan run again a sample Windows 2008 Server. They will perform any necessary remediations to the server by Windows 2008 Server. They will perform the same actions on other Windows 2008 Server. They will perform any necessary remediations to the server by Windows 2008 Server. They will perform the same actions on other Windows 2008 Server. They will perform any necessary remediations to the server by Windows 2008 Server. They will perform any necessary remediations to the server by Windows 2008 Server. They will perform the same actions on the Windows 2008 Server. They will perform any necessary remediations to the server by Windows 2008 Server. They will perform any necessary remediations to the server by Windows 2008 Server. They will perform any necessary remediations to the server by Windows 2008 Server. They will perform any necessary remediations to the server by Windows 2008 Server. They will perform any necessary remediations to the server by Windows 2008 Server. They will perform any necessary remediations to the server by Windows 2008 Server. They will perform any necessary remediations to the server by Windows 2008 Server. They will perform any necessary remediations to the server by Windows 2008 Server. They will perform any necessary remediations to the server by Windows 2008 Server. They will perform any necessary remediations to the server by Windows 2008 Server. They will perform any necessary remediations to the server by Windows 2008 Server. They will perform any necessary remediations to the server by Windows 2008 Server. They will perform any necessary remediations to the server by Windows 2008 Server. They will perform any necessary remediations to the server by Windows 2008 Server. They will perform any necessary remediations to the server by Windows 2008 Server. They wil
Window 2008 Server. They will perform any necessary remediations to the server by applying a variety port patches, systems/level to the size received by a phyling a variety port patches, systems/level to the size received by a phyling a variety port patches, systems/level to pa
Windows 2008 Server. They will perform any necessary remediations to the server by
been miligated down to a reasonable level of risk. After the verification scan has been completed, they will then author a Standard Operating Procedure to help others walk through the same miligation process they went through - enabling others to perform the same actions on other Windows 2008 servers.
Cyptography-Attacking Gassic Ciphers Training on how to use GPG with a GPG challenge at the end. CYBRSCORE Scored Labs Advanced Cryptography-(ACR); Topics: 1:11 Hyper-V 1 Hour, 30 Minutes 1 Training on how to use GPG with a GPG challenge at the end. CYBRSCORE Labs Advanced Cryptography-(ACR); Topics: 1:11 Hyper-V 1 Hour, 30 Minutes 1
Training in thor do use on-s with a sprc planeting at the em. This lab walks subjects through not to attack a repeated key XRR clipher, and then provides a chillenge to the subject with a modern Key
This lab walks students through how to attack a repeated key XDR Opher, and then crowleds a challenge to the dustent in the form of a lined plange to the dustent in the form of a lined plange to the dustent in the form of a lined plange to the dustent in the form of a lined plange to the dustent in the form of a lined plange to the dustent in the form of a lined plange to the dustent in the form of a lined plange to the dustent in the form of a lined plange to the dustent in the form of a lined plange to the dustent in the form of a lined plange to the dustent in the form of a lined plange to the dustent in the form of a lined plange to the dustent in the form of a lined plange to the dustent in the form of a lined plane to the dustent in the form of a lined plane to the dustent in the form of a lined plane to the dust in the form of a lined plane to the dustent in the dustent in the form of a lined plane to the dustent in the
Students will be shown various tools for attacking and using RSA public key information. Cryptography: Breaking Weak RSA Keys They will then be given a weak public key and required to break it and decrypt a secret message. CYBRS.core Scored Labs Advanced Cryptography (ACR): Topics: 1-11 Advanced Cryptography (ACR): Topics: 1-11 Advanced Cryptography (ACR): Topics: 1-11 Timinute, 16 seconds 1 minute, 16 seconds 2 minutes, 25 secon
Students will be shown various tools for attacking and using RSA public key information. Cyptography: Breaking Weak RSA Keys They will then be given a week public key and decrypt at operation to be given a week public key and decrypt at operation to an add expty at secret. Students will be shown various tools for attacking and using RSA public key information. Students will be shown various tools for attacking and using RSA public key information.
Students will be shown various tools for attacking and using RSA public key information. Cryptography: Breaking Weak RSA Keys They will then be given a weak public key and derugate of such and deveyst a server. They will then be given a weak public key and derugate of such and deveyst a server. Advanced Cryptography (ACR): Topics: 1-11 Hyper-V 3 Hours 6 Hours 7 minutes, 44 seconds 38 seconds Students will be shown various tools for attacking and using RSA public key information.
Students was given two files and are charged with decrypting both. The first one has the Students are given two files and are charged with decrypting both. The first one has the
Cryptography: Decrypting Files With a Dictionary Attack password given, and the second they must brute force the password with a dictionary attack. CYBRScore Scored Labs Advanced Cryptography (ACR); Topics: 1:11 Hyper V 2 Hours 4 Hours 4 Hours 4 Hours 4 Individe, 13 seconds 1 minute, 13 seconds 1 mi
Students are given two files and are charged with decrypting poth. The first one has the password given, and the second they must brute force the password with a dictionary Attack CYPTOGRAPHY: Decrypting Files With a Dictionary Attack Advanced Cryptography (ACR); Topics: 1-11 CYBRScore Labs Advanced Cryptography (ACR); Topics: 1-11 Hyper-V 2 Hours 4 Hours 38 minutes, 43 seconds 32 seconds
Students will be given an IEE/amal Signature Oracle and Charged with recogniting an Insecure use of it, and exploiting that he exploit and exploiting that
Students will be given an Bischami Signature Oracle and charged with recognizing an insecure suse of it, and exploiting that to calculate the private key. Incert private key is obtained, they will need to create a signature on a given meriage using that private key. Obtained, they will need to create a signature on a given meriage using that private key. Obtained, they will need to create a signature on a given meriage using that private key. Obtained, they will need to create a signature on a given meriage using that private key.
Cryptography: Forging MACs With Side Channels Students will be faced with a MAC protocol and they must exploit a timing side channel information leak to forge a MAC on a message. CYBRScore Scored Labs Advanced Cryptography (ACR); Topics: 1-11 Hyper-V 2 Hours 4 Hours 1 hour, 5 minutes 2 minutes, 5 second
Cryptography: Forging MACs With Side Channels Students will be faced with a MMC protocol and they must exploit a timing side channel information leak to forge a MAC on a message. CYBRScore Labs Advanced Cryptography (ACR): Topics: 1-11 Hyper-V 2 Hours 4 Hours 4 Hours 4 minutes, 30 seconds
Cryptography: Hidden Veracrypt Containers Students will be shown how to create Veracrypt encrypted containers and will be challenged with creating a hidden container which contains provided files. CYBRScore Scored Labs CYBRScore Scored Labs Advanced Cryptography (ACR): Topics: 1-11 Hyper-V 1 Hour 2 Hours 34 minutes, 25 seconds I minute, 34 seconds

Cryptography: Hidden Veracrypt Containers	Students will be shown how to create Veracrypt encrypted containers and will be challenged with creating a hidden container which contains provided files.	CYBRScore Labs	Advanced Cryptography (ACR); Topics: 1-11	Hyper-V	1 Hour	2 Hours	3 minutes, 31 seconds	35 seconds
Cryptography: Man In the Middle Attack	Students will be placed in the middle of an encrypted chat session. They will be able to analyze the protocol, find the flaws, formulate an attack, and execute the attack.	CYBRScore Scored Labs	Advanced Cryptography (ACR); Topics: 1-11	Hyper-V	2 Hours	4 Hours	32 minutes, 15 seconds	1 minute, 21 seconds
Cryptography: Man In the Middle Attack	Students will be placed in the middle of an encrypted chat session. They will be able to analyze the protocol, find the flaws, formulate an attack, and execute the attack.	CYBRScore Labs	Advanced Cryptography (ACR); Topics: 1-11	Hyper-V	2 Hours	4 Hours	7 minutes, 13 seconds	43 seconds
Cryptography: Password Cracking	Training on how to use GPG with a GPG challenge at the end.	CYBRScore Scored Labs	Advanced Cryptography (ACR); Topics: 1-11	Hyper-V	1 Hour	1 Hour	1 hour	1 minute, 9 seconds
Cryptography: Password Cracking	Training on how to use GPG with a GPG challenge at the end.	CYBRScore Labs	Advanced Cryptography (ACR); Topics: 1-11	Hyper-V	1 Hour	1 Hour	42 minutes, 30 seconds	1 minute, 5 seconds
Cryptography: Setting Up HTTPS in Windows and Linux	Setting up HTTPS enabled Web Servers in Linux and Windows	CYBRScore Scored Labs	Advanced Cryptography (ACR); Topics: 1-11	Hyper-V	1 Hour, 30 Minutes	1 Hour, 30 Minutes	23 minutes, 6 seconds	1 minute, 41 seconds
Cryptography: Setting Up HTTPS in Windows and Linux	Setting up HTTPS enabled Web Servers in Linux and Windows	CYBRScore Labs	Advanced Cryptography (ACR); Topics: 1-11	Hyper-V	1 Hour, 30 Minutes	1 Hour, 30 Minutes	1 hour, 1 minute	1 minute, 34 seconds
Cryptography: Setting Up Two Factor Authentication	Set up 2FA in Windows and Linux	CYBRScore Scored Labs	Advanced Cryptography (ACR); Topics: 1-11	Hyper-V	1 Hour, 30 Minutes	1 Hour, 30 Minutes	32 minutes, 1 second	1 minute, 12 seconds
Cryptography: Setting Up Two Factor Authentication	Set up 2FA in Windows and Linux In this lab, students will learn:	CYBRScore Labs	Advanced Cryptography (ACR); Topics: 1-11	Hyper-V	1 Hour, 30 Minutes	1 Hour, 30 Minutes	47 minutes, 58 seconds	55 seconds
Cryptography: Steganography	How information can be hidden in cover files. How to recognize and search for hidden information. How to steganalyze a file to identify that message was hidden inside.	CYBRScore Scored Labs	Advanced Cryptography (ACR); Topics: 1-11	Hyper-V	1 Hour, 30 Minutes	2 Hours	44 minutes, 52 seconds	1 minute, 23 seconds
Cryptography: Using GPG for Encryption and Key Management	Training on how to use GPG with a GPG challenge at the end.	CYBRScore Scored Labs	Advanced Cryptography (ACR); Topics: 1-11	Hyper-V	1 Hour, 30 Minutes	2 Hours	33 minutes, 7 seconds	1 minute, 16 seconds
Cryptography: Using GPG for Encryption and Key Management	Training on how to use GPG with a GPG challenge at the end.	CYBRScore Labs	Advanced Cryptography (ACR); Topics: 1-11	Hyper-V	1 Hour, 30 Minutes	2 Hours	1 hour, 6 minutes	55 seconds
Cryptography: Using the OpenSSL CLI Tool	Training on how to use OpenSSL CLI tool with a challenge at the end.	CYBRScore Scored Labs	Advanced Cryptography (ACR); Topics: 1-11	Hyper-V	1 Hour, 30 Minutes	1 Hour, 30 Minutes	1 hour, 32 minutes	54 seconds
Cryptography: Using the OpenSSL CLI Tool	Training on how to use OpenSSL CLI tool with a challenge at the end.	CYBRScore Labs	Advanced Cryptography (ACR); Topics: 1-11	Hyper-V	1 Hour, 30 Minutes	1 Hour, 30 Minutes	51 minutes, 4 seconds	31 seconds
CTF Environment	This lab hosts a set of CTF challenges that will be automatically scored.	CYBRScore Scored Labs	CTF ENVIRONMENT (MANY)	Hyper-V	8 Hours	8 Hours	2 hours, 58 minutes	1 minute, 13 seconds
Cyber Defense Analyst - Incident Handling Methodology	This assessment is one of five and is focused specifically on items related to incident handling and response.	CYBRScore	Assessment - Covers dozens of KU	Hyper-V	45 Minutes	1 Hour	34 minutes, 50 seconds	1 minute, 44 seconds
Cyber Defense Analyst - Intrusion Detection	This assessment is one of five and is focused specifically on items related to intrusion detection and prevention.	CYBRScore	Assessment - Covers dozens of KU	Hyper-V	45 Minutes	1 Hour	32 minutes, 36 seconds	1 minute, 41 seconds
Cyber Defense Analyst - Network Attack Analysis	This assessment is one of five and is focused specifically on items related to penetration testing.		Assessment - Covers dozens of KU	Hyper-V	45 Minutes	1 Hour	43 minutes, 18 seconds	2 minutes, 7 seconds
Cyber Defense Analyst - Network Attack Analysis - DEMO	This is a DEMO lab profile intended for use to showcase integration between assessment and training labs This processment is one of five and is focused considerable on those soluted to unless billing.		Assessment - Covers dozens of KU	Hyper-V	45 Minutes	1 Hour	19 minutes, 22 seconds	2 minutes, 14 seconds
Cyber Defense Analyst - Network Defense Analysis	This assessment is one of five and is focused specifically on items related to vulnerability assessments. This assessment is one of five and is focused specifically on items related to protocol		Assessment - Covers dozens of KU	Hyper-V	45 Minutes	1 Hour	41 minutes, 12 seconds	2 minutes, 37 seconds
Cyber Defense Analyst - Protocol Analysis	This assessment is one of five and is focused specifically on items related to protocol analysis.	CYBRScore	Assessment - Covers dozens of KU	Hyper-V	45 Minutes	1 Hour	38 minutes, 38 seconds	1 minute, 18 seconds
Cybersecurity Testing with Core Impact	Students use Core Impact to enumerate a local area network and discovery vulnerable machines through a vulnerability scan. Based on the results of the vulnerability scan, students use foce impact to conduct a penetration test against a previously identified vulnerable machine. Finally, students use the reporting mechanism built into Core impact to create a host-based assessment outlining the entire vulnerability/penetration test process with a focus on possible remediation actions.	CYBRScore Scored Labs	Operating Systems Hardening (OSH), Topics: 11; IT Systems Components (ISC), Topics: 13	Hyper-V	1 Hour	1 Hour, 30 Minutes	1 hour, 2 minutes	1 minute, 6 seconds
Cybersecurity Testing with Core Impact	Students will use Core Impact to enumerate a LAN and determine any vulnerable virtual machines through the use of a vulnerability scan. Based on the results of the vulnerability scan, students continue to use Core Impact to conduct a penetration test against a previously identified vulnerable machine. Finally, students use the reporting mechanism but lint to Core Impact to create a host-based assessment outling the entire vulnerability/penetration test process with a focus on possible remediation actions.	CYBRScore Labs	Operating Systems Hardening (OSH), Topics: 11; IT Systems Components (ISC), Topics: 13	Hyper-V	1 Hour	1 Hour, 30 Minutes	59 seconds	23 seconds
Cybersecurity Testing with Core Impact Capstone	Students use Core Impact to enumerate a local area network and discovery vulnerable machines through a vulnerability scan. Based on the results of the vulnerability scan, students use core impact to conduct a penetration test against a previously identified vulnerable machine. Finally, students use the reporting mechanism bulbt into Core impact to create a host-based assessment outlining the entire vulnerability/penetration test process with a focus on possible remediation actions.	CYBRScore Capstones	Operating Systems Hardening (OSH), Topics: 11; IT Systems Components (ISC), Topics: 13	Hyper-V	1 Hour	1 Hour, 30 Minutes		
CYBRScore Cyber Range - Incident Handling	This assessment is one of five and is focused specifically on items related to incident handling and response.	CYBRScore	Assessment - Covers dozens of KU	Hyper-V	45 Minutes	1 Hour		
CYBRScore Cyber Range - Intrusion Detection	This assessment is one of five and is focused specifically on items related to intrusion detection and prevention.	CYBRScore	Assessment - Covers dozens of KU	Hyper-V	45 Minutes	1 Hour		
CYBRScore Cyber Range - Network Attack Analysis	This assessment is one of five and is focused specifically on items related to penetration testing	CYBRScore	Assessment - Covers dozens of KU	Hyper-V	45 Minutes	1 Hour		
CYBRScore Cyber Range - Network Defense Analysis	This assessment is one of five and is focused specifically on items related to vulnerability assessments.	CYBRScore	Assessment - Covers dozens of KU	Hyper-V	45 Minutes	1 Hour		
CYBRScore Cyber Range - Protocol Analysis	This assessment is one of five and is focused specifically on items related to protocol analysis.	CYBRScore	Assessment - Covers dozens of KU	Hyper-V	45 Minutes	1 Hour		
CYBRScore Pentesting Assessment_Merge	analysis. N/A	CYBRScore	Assessment - Covers dozens of KU	vSphere	4 Hours	8 Hours		
CYBRScore Skills Assessment Demo	This is a demo assessment designed to showcase the functionality of CYBRScore	CYBRScore	Assessment - Covers dozens of KU Assessment - Covers dozens of KU	vSphere	1 Hour	2 Hours	44 minutes, 44 seconds	2 minutes, 11 seconds
CYBRScore System Administration Assessment	assessments. This assessment is designed to test your knowledge, skill, and ability in tackling common		Assessment - Covers dozens of KU Assessment - Covers dozens of KU	vSphere	3 Hours	3 Hours	1 hour, 55 minutes	2 minutes, 11 seconds
	system problems and ensuring network policy adherence. This assessment is designed to test your knowledge, skill, and ability in assessing,	CYBRScore						
CYBRScore Vulnerability Assessment Management	exploiting, and mitigating network vulnerabilities. This assessment is designed to test your knowledge, skill, and ability in assessing,		Assessment - Covers dozens of KU	vSphere	3 Hours	4 Hours	47 minutes, 48 seconds	1 minute, 4 seconds
CYBRScore Vulnerability Assessment Management (b)	exploiting, and mitigating network vulnerabilities. In this lab we will simulate the recovery phase where we must perform a backup in a	CYBRScore Labs	Assessment - Covers dozens of KU	vSphere	4 Hours	8 Hours	14 minutes, 4 seconds	22
Data Backup and Recovery	server environment. In this lab we will simulate the recovery phase where we must perform a backup in a		Operating Systems Administration (OSA); Topics: 2, 4, 5, 6, 9, 11	Hyper-V	1 Hour		,	23 seconds
Data Backup to Prep for Recovery	server environment. In this lab we will simulate the recovery phase where we must perform a backup in a	CYBRScore Labs	Operating Systems Administration (OSA); Topics: 2, 4, 5, 6, 9, 11	Hyper-V	1 Hour	1 Hour	10 minutes, 40 seconds	25 seconds
Data Backup to Prep for Recovery	server environment.	CYBRScore Scored Labs	Operating Systems Administration (OSA); Topics: 2, 4, 5, 6, 9, 11	Hyper-V	1 Hour	1 Hour	6 minutes, 16 seconds	37 seconds
Data Recovery with Autopsy	Students will ingest and process a previously acquired forensic image using Autopsy. Th focus of the lab will be on recovering data from the image, reviewing the supplied forensic report and verifying that the image is forensically sound.	e CYBRScore Labs	Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10	Hyper-V	30 Minutes	45 Minutes	21 minutes, 4 seconds	28 seconds
Data Recovery with Autopsy	Students will ingest and process a previously acquired forensic image using Autopsy. The focus of the lab will be on recovering data from the image, reviewing the supplied forensic report and verifying that the image is forensically sound.	e CYBRScore Scored Labs	Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10	Hyper-V	30 Minutes	45 Minutes	22 minutes, 56 seconds	56 seconds
Denial of Service PCAP Analysis	The student will act as attacker and defender in this scenario. They will receive experience using a custom denial of service python script, and then will switch over to the defensive side. On defense they will need to detect the activity, design firewall rules to block the DoS, implement the rules and then check their effectiveness.	CYBRScore Labs	Network Security Administration (NSA); Topics: 2, 5, 7, 8, 9, 10	Hyper-V	45 Minutes	1 Hour	32 minutes, 6 seconds	47 seconds
Denial of Service PCAP Analysis	The student will act as attacker and defender in this scenario. They will receive experience using a custom denial of service python script, and then will switch over to the defensive side. On defense they will need to detect the activity, design firewall rules to block the DoS, implement the rules and then check their effectiveness.	CYBRScore Scored Labs	Network Security Administration (NSA); Topics: 2, 5, 7, 8, 9, 10	Hyper-V	45 Minutes	1 Hour	26 minutes, 34 seconds	1 minute, 9 seconds
	· · · · · · · · · · · · · · · · · · ·							

	Malware can take many forms. Microsoft Office documents can act as a vehicle for a							
Detect Embedded Shellcode in a Microsoft Office Document	variety of ingenious attacks. Students will detect shellcode embedded in a Microsoft document. In this lab, the student will simulate the download of a malicious file from a website.	CYBRScore Labs	Software Security Analysis (SSA); Topics: 1, 2, 3, 4, 5	Hyper-V	1 Hour	1 Hour	7 minutes, 1 second	16 seconds
Detect the Introduction of a Malicious Application	They will then learn how to detect the introduction of malicious programs on a Win7 machine using Microsoft Security Essentials.	CYBRScore Labs	Software Security Analysis (SSA); Topics: 1, 2, 3, 4, 5	Hyper-V	30 Minutes	1 Hour	49 minutes, 13 seconds	29 seconds
Detect the Introduction of a Malicious Application	In this lab, the student will simulate the download of a malicious file from a website. They will then learn how to detect the introduction of malicious programs on a Win7 machine using Microsoft Security Essentials.	CYBRScore Scored Labs	Software Security Analysis (SSA); Topics: 1, 2, 3, 4, 5	Hyper-V	1 Hour	1 Hour		
Detect Unauthorized Changes by Comparing to Approved Configurations	Students will use a variety of tools to record and snapshot different aspects of a Windows workstation, and then compare those recent state updates to approved configurations. The goal is to have them learn to detect and recognize unauthorized changes or deviations to this workstation.	CYBRScore Labs	Host Forensics (HOF), Topics: 1; Windows System Administration (WSA), Topics: 13	Hyper-V	1 Hour, 30 Minutes	1 Hour, 30 Minutes	30 minutes	26 seconds
Detect Unauthorized Changes by Comparing to Approved Configurations	Students will use a variety of tools to record and snapshot different aspects of a Windows workstation, and then compare those recent state updates to approved configurations. The goal is to have them learn to detect and recognize unauthorized changes or deviations to this workstation.	CYBRScore Scored Labs	Host Forensics (HOF), Topics: 1; Windows System Administration (WSA), Topics: 13	Hyper-V	1 Hour, 30 Minutes	1 Hour, 30 Minutes	1 hour, 13 minutes	1 minute, 4 seconds
Detecting Changes to System Configurations	Students will use a couple of the popular Sysinternals Sulte tools to observe configuration changes on a known good/clean system. The senaria will knew them perform a running system snapshot using Reghot, TCPView, ListDLIs, Process Explorer and Process Monitor prior to executing a suspicious program. After execution, they will unit the same tools, compare the results and not early difference. This lish forsets tool familiarization and will provide an "under the hood" perspective of a running Windows environment.	CYBRScore Labs	Operating Systems Hardening (OSH); Topics: 1, 2, 3, 4, 5, 6, 7, 8, 10, 11	Hyper-V	45 Minutes	1 Hour, 30 Minutes	1 hour, 11 minutes	14 seconds
Detecting Changes to System Configurations	Students will use a couple of the popular Sysintemals Suite tools to observe configuration changes on a known good/clean system. The scenario Will have them perform a running system napablo sain Regibbl, (T.Pive, ILSTUD, Process Explorer and Process Monttop prior to executing a suspicious program. After execution, they will not the same tools, compare the results and note any officences. This bid fosters tool familiarization and will provide an "under the hood" perspective of a running Windows environment.	CYBRScore Scored Labs	Operating Systems Hardening (OSH); Topics: 1, 2, 3, 4, 5, 6, 7, 8, 10, 11	Hyper-V	45 Minutes	1 Hour, 30 Minutes	34 minutes, 22 seconds	1 minute, 19 seconds
Dev0 - Introduction to Windows Socket Programming in C/C++	Welcome to DEV O, Welcome to Intro to Windows System and Socket Programming with C/Cr+. In this course you will learn the basics of programming in C which will give you the needed foundation to progress on to Windows System and Socket Programming with the Windows API. We will strive to keep the lecture portions of this course to what we feel is the minimum needed to give you a good grounding in the concepts needed to write programs in C. As we progress through the class we will do our best to employ the Socratic method of teaching whereby we won't necessarily always tell you the answer rather we will provide you with core information and ask you to think and employ logic, problem solving and bother skills to create the answer. However, I you're suck and if you've given a good elfort at trying to find an answer or solve a problem, please ask the instructor. With that in mind if the toply ow wish to discuss fills ousside of the scope of the course learning objectives, we may ask you to revisit the question on break or after other students don't need any further assistance.	CYBRScore Labs	Low Level Programming (LEP) — This isn't low level; however, no other specific KU exists for learning to code in this bootcamp-like setting	g Hyper-V	60 Hours	120 Hours	44 minutes, 28 seconds	31 seconds
Disable User Account on Windows 10	In this lab, the student will respond to a suspected insider threat incident by disabling user accounts in Windows. Additionally, the student will learn to search for and conduct basic analysis on suspected malicious events via the mmc Event Viewer snap-in.	CYBRScore Scored Labs	Operating Systems Hardening (OSH); Topics: 1, 2, 3, 4, 5, 6, 7, 8, 10, 11	Hyper-V	45 Minutes	45 Minutes	15 minutes, 23 seconds	1 minute, 6 seconds
Disable User Account on Windows 7	In this lab, the student will respond to a suspected insider threat incident by disabling user accounts in Windows. Additionally, the student will learn to search for and conduct basic analysis on suspected malicious events via the mmc Event Viewer snap-in.	CYBRScore Labs	Operating Systems Hardening (OSH); Topics: 1, 2, 3, 4, 5, 6, 7, 8, 10, 11	Hyper-V	45 Minutes	45 Minutes	14 minutes, 40 seconds	22 seconds
DLL Editing	This exercise will demonstrate the functions of Dynamic Link Libraries (DLLs). Upon completing this exercise, the trainee will have a better understanding of how DLLs affect the user's ability to run various programs.	CYBRScore Labs	Operating Systems Administration (OSA); Topics: 2, 4, 5, 6, 9, 11	vSphere	1 Hour	1 Hour	14 minutes, 43 seconds	6 seconds
DNS as a Remote Shell	This lab outgries is designed to allow the trained to become familiar with recognizing	CYBRScore Labs	Operating Systems Hardening (OSH); Topics: 1, 2, 3, 4, 5, 6, 7, 8, 10, 11	vSphere	1 Hour	1 Hour	15 minutes, 28 seconds	10 seconds
Dynamic Malware Analysis	Students will use utilize two virtual machines, inside a protected network, to observe configuration changes on a known good / clean system and all of the unusual network traffe generated by the suspect software they will be analyzing. On the clean system they will use Regishot, Appon Network Switcher, Process Hacker, Process Monitor and Norben to gather details on what the suspectious program is actually doing. On another support machine they will set up a fake DNS server to receive all suspicious traffic, and assist hat Varific over to Witershaf of Further analysis. This lab will continue to foster tool familiarization and will provide the students an introduction to capturing network traffic by using a simple manni-ther endides "system.	CYBRScore Scored Labs	Software Security Analysis (SSA): Topics: 1, 2, 3, 4, 5	Hyper-V	1 Hour	1 Hour	30 minutes, 4 seconds	1 minute, 56 seconds
Dynamic Malware Analysis Capstone	Students will use utilize two virtual machines, inside a protected network, to observe configuration changes on a known good / clean system and all of the unusual network furfix generated by the suspects oftware they will be analyzing. On the clean system they will use Regibnot, Algon Network Switcher, Process Hacker, Process Monitor and Norries to gather details on what the suspicious program is actually doing. On another support mentine they will set up a falle DNS server to receive all suspicious traffic, and associated the support machine they will write ranalysis. This list will continue to foster tool familiarization and will provide the students an introduction to capturing network traffic by single simple "man-in-the-middle" system.	CYBRScore Capstones	Software Security Analysis (SSA); Topics: 1, 2, 3, 4, 5	Hyper-V	1 Hour	1 Hour	18 minutes, 58 seconds	1 minute, 16 seconds
Entering Information into a CMDB	Students will review an old asset list and enter all of the contained information into a Configuration Management Database (CMDB). Students will then gather information from two systems (a Windows and Linux system) and a	CYBRScore Scored Labs	Cybersecurity Principles (CSP), Topics: j; Operating System Concepts (OSC), Topics: 1, 9 - Windows System Administration (WSA), Topics: 2, 4, 6	Hyper-V	1 Hour	1 Hour, 30 Minutes	39 minutes, 17 seconds	1 minute, 37 seconds
Evasive Maneuvers and Post Exploitation	In this lab, you will practice enumeration of outbound egress policy, which is necessary when attempting to perform reverse connections, or exfiltrate data.	CYBRScore Scored Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10	Hyper-V	1 Hour	1 Hour	32 minutes, 13 seconds	59 seconds
Evasive Maneuvers and Post Exploitation (External)	In this lab, you will practice enumeration of outbound egress policy, which is necessary when attempting to perform reverse connections, or exfiltrate data.	CYBRScore Scored Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10	Hyper-V	1 Hour	1 Hour	29 minutes, 48 seconds	1 minute, 2 seconds
Evasive Maneuvers and Post Exploitation (Scored)	when attempting to perform reverse connections, or exfiltrate data.	CYBRScore Scored Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10	Hyper-V	1 Hour	1 Hour	32 minutes	1 minute, 27 seconds
Event Log	In this lab, the trainee will have the opportunity to review event log files associated with the Windows 7 operating system.	CYBRScore Labs	Windows System Administration (WSA), Topics: 2, 4, 6, 7 - Operating System Concepts (OSC), Topics: 2, 4	vSphere	1 Hour	1 Hour	19 minutes, 30 seconds	12 seconds
Event Log Collection	In this lab you will use Splunk Enterprise to ingest logs from a local host for analysis	CYBRScore Labs	Windows System Administration (WSA), Topics: 2, 4, 6, 7 - Operating System Concepts (OSC), Topics: 2, 4	Hyper-V	1 Hour	1 Hour	8 minutes, 41 seconds	21 seconds
Event Log Collection	In this lab you will use Splunk Enterprise to ingest logs from a local host for analysis	CYBRScore Scored Labs	Windows System Administration (WSA), Topics: 2, 4, 6, 7 - Operating System Concepts (OSC), Topics: 2, 4	Hyper-V	1 Hour	1 Hour		
Event Logs	Students will learn what Event Logs are, how to view them, and what kind of information can be found in them.	CYBRScore Labs	Windows System Administration (WSA), Topics: 2, 4, 6, 7 - Operating System Concepts (OSC), Topics: 2, 4	Hyper-V	1 Hour	1 Hour, 30 Minutes	36 minutes, 39 seconds	38 seconds

March Standard Stan	ent Logs	Students will learn what Event Logs are, how to view them, and what kind of information	CVDDCcore Seared Labo	Windows System Administration (WSA), Topics: 2, 4, 6, 7 - Operating System Concepts (OSC),	Hyper-V	1 Hour	1 Hour, 30 Minutes	38 minutes, 54 seconds	1 minute, 21 seconds
Processing the content in part of the content in				Topics: 2, 4				36 minutes, 34 seconds	1 minute, 21 seconds
March Content Conten	ent Logs			Topics: 2, 4	Hyper-V	1 Hour	1 Hour, 30 Minutes		
Marie Mari	ld Technologist - Technical Support Specialist	This assessment is designed to test your knowledge, skill, and ability in tackling common system problems and ensuring network policy adherence.	CYBRScore	Assessment - Covers dozens of KU	Hyper-V	10 Hours	10 Hours	1 hour, 18 minutes	2 minutes, 10 seconds
Tread into an Conference Tread into an Conf	ld Technologist - Network Support Specialist	This assessment is designed to test your knowledge, skill, and ability in configuring	CYBRScore	Assessment - Covers dozens of KU	Hyper-V	1 Hour	1 Hour	32 minutes, 29 seconds	2 minutes, 11 seconds
Paral time of Configerion Control (Septiment Configerion) Contro	ewall Setup and Configuration	In this lab you will perform the steps necessary to set up a pfSense firewall from the basic command line interface and then configure the firewall using the web configuration GUI on a Windows makine. This lab will provide an understanding how network interfaces are configured to allow network connectivity. You will also view and create a firewall rule which enforces your understanding of how network traffic can be managed at different		Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a	Hyper-V	1 Hour	1 Hour	19 minutes, 54 seconds	32 seconds
Present Series and Configeration Configera	ewall Setup and Configuration	command line interface and then configure the firewall using the web configuration GUI on a Windows machine. This lab will provide an understanding how network interfaces are configured to allow network connectivity. You will also view and create a firewall rule which enforces your understanding of how network traffic can be managed at different	CYBRScore Scored Labs	Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a	Hyper-V	1 Hour	1 Hour	27 minutes, 54 seconds	55 seconds
Security String and Configuration Captation Personal String and Configuration Captation And Configura	ewall Setup and Configuration	command line interface and then configure the firewall using the web configuration GUI on a Windows machine. This lab will provide an understanding how network interfaces are configured to allow network connectivity. You will also view and create a firewall rule which enforces your understanding of how network traffic can be managed at different		Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a	Hyper-V	1 Hour	1 Hour	18 minutes, 46 seconds	1 minute, 20 seconds
In this king you did preferred in exercisor points to the layer of the preferred from the company of the preferred with the company of the pre	ewall Setup and Configuration Capstone	command line, and you will then continue configuring the firewall using the web configuration GUI from a separate network-connected Windows machine. Listly, you will view and create a firewall rule which enforces your undestanding of how network traffic can be managed at different levels – it-based, protocol-based, machine-based, and so forth. This lab provides an understanding of how network interfaces are configured to allow	CYBRScore Scored Labs	Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a	Hyper-V	1 Hour	1 Hour	14 minutes, 55 seconds	1 minute, 18 seconds
In this bill you will gradient the excessive parts for sit or a place formation from the command time, and you will be controlled. Complete feeders and you will be controlled from the command time, and you will be controlled from the command time, and you will be controlled from the command time, and you will be controlled from the command time, and you will be controlled from the controlled from the command time, and you will be controlled from the controlled f	ewall Setup and Configuration Capstone	In this lab you will perform the necessary steps to set up a pfSense firewall from the command line, and you will then confluince onfluing the firewall using the web configuration GUI from a separate network-connected Windows machine. Lastly, you will view and create a freewall use which enforces your understanding of how networking of how networking or how retworking on the commanded at different levels—IP-based, protocol-based, machine-based, and so forth. This lab provides an understanding of how network interfaces are configured to allow	CYBRScore Capstones	Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a	Hyper-V	1 Hour	1 Hour		
Substantial blustomer familiar with blustomer with the plants controlling blustomer familiar with blus	ewall Setup and Configuration Capstone - Skills Passport	In this lab you will perform the necessary steps to set up a pSense firewall from the command line, and you will then continue configurate the result using the web configuration GUI from a separate network-connected Windows machine. Lastly, you will view and create a firewall rule which enforces your understanding of how network traffic can be managed at different levels – iP-based, protocol-based, machine-based, and so forth.	CYBRScore Capstones	Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a	Hyper-V	1 Hour	1 Hour	18 minutes, 20 seconds	37 seconds
Assessment (BM, Disaster Recovery Plan (DRP) and Computer incident Response Plan (CPR). During the course of the lab, students will become familiar with the Business Continuity Plan (BCP). Business from the Business Continuity Plan (BCP). Busines	ing a Company BCP, DRP and CIRP	Students will become familiar with the Business Continuity Plan (BCP), Business Impact Assessment (BIA), Disaster Recovery Plan (DRP) and Computer Incident Response Plan (CIRP). During the course of the lab, students will perform a gap analysis using the	CYBRScore Labs	Cybersecurity Planning and Management (CPM); Topics: 2, 4, 5, 6, 8, 9	Hyper-V	1 Hour, 30 Minutes	2 Hours	54 seconds	24 seconds
Assessment (BAL) Disaster Recovery Plan (DRP) and Computer Incident Response Plan (CRP). Langth decided Style performs and Analysis using the provided BCP, BIAs and DRP, and make the necessary flues to the DRP. This assessment is one of three, and is specifically focused on Items related to Network Perensic Operations. This assessment is one of three, and is specifically focused on Items related to Malware Analysis This assessment is one of three, and is specifically focused on Items related to Malware Analysis This assessment is one of three, and is specifically focused on Items related to Malware Analysis Forensic Analyst- Network Collection and Handling This assessment is one of three, and is specifically focused on Items related to Network Perensic Operations. This assessment is one of three, and is specifically focused on Items related to Network Perensic Operations. This assessment is one of three, and is specifically focused on Items related to Network Collection and Handling This assessment is one of three, and is specifically focused on Items related to Network Collection and Handling This assessment is one of three, and is specifically focused on Items related to Network Collection and Handling The prensic Operations. This assessment is one of three, and is specifically focused on Items related to Network Collection and Handling This assessment is one of three, and is specifically focused on Items related to Network Collection and Handling This assessment is one of three, and is specifically focused on Items related to Network Collection and Handling This assessment is one of three, and is specifically focused on Items related to Network Collection and Handling This assessment is one of three, and is specifically focused on Items related to Network Collection and Handling The period Collection and Handling This assessment is one of three, and is specifically focused on Items related to Network Collection and Handling The period Collection and Handling This assessment is one of thre	ing a Company BCP, DRP and CIRP	Assessment (BIA), Disaster Recovery Plan (DRP) and Computer Incident Response Plan (CIRP). During the course of the lab, students will perform a gap analysis using the	CYBRScore Scored Labs	Cybersecurity Planning and Management (CPM); Topics: 2, 4, 5, 6, 8, 9	Hyper-V	1 Hour, 30 Minutes	2 Hours	55 minutes, 55 seconds	41 seconds
Forensic Analyst - Melware Analysis Forensic Incident Response Capstone Forensic Incident Response Capstone Forensic Incident Response Capstone Forensic Incident Response Capstone Forensic Septone Forensic Septone Forensic Septone Forensic Septone Forensic Septone Forensic Incident Response Capstone Forensic Incident Response Capst	ing a Company BCP, DRP and CIRP Capstone	Assessment (BIA), Disaster Recovery Plan (DRP) and Computer Incident Response Plan (CIRP). During the course of the lab, students will perform a gap analysis using the	CYBRScore Capstones	Cybersecurity Planning and Management (CPM); Topics: 2, 4, 5, 6, 8, 9	Hyper-V	1 Hour, 30 Minutes	2 Hours	1 minute, 56 seconds	1 minute, 11 seconds
This assessment is one of three, and is specifically focused on Items related to Malware Analysis. Forensic Analysts - Malware Analysis Forensic Analysts - Network Collection and Handling This assessment is one of three, and is specifically focused on Items related to Network Forensic Incident Response Capstone In this capstone, students will analyze given evidence to detentify an intrusion on an enterwork, identify in a intrusion on an enterwork (analysts - Network Collection and Handling Forensic Incident Response Capstone Forensic Incident Response Capstone The affected system, what to fix or remove on an affected system and what potential charges need to be made in policy. Forensic Capstone This assessment is one of three, and is specifically focused on Items related to Network Pages Core Assessment - Covers dozens of KU Hyper-V 55 Minutes 1 hour, 5 Minutes 1 hour, 5 Minutes 1 hour, 5 Minutes 1 hour, 5 Minutes 1 minute, 29 1 minute, 29 1 minute, 29 1 minute, 29 2 minute, 21 2 minute, 29 2 minute, 21 2 minute, 29 2 minute, 29 3 Hours 4	rensic Analyst - File Collection and Analysis		CYBRScore	Assessment - Covers dozens of KU	Hyper-V	45 Minutes	1 Hour, 5 Minutes	29 minutes, 51 seconds	1 minute, 55 seconds
Analysts - Network Collection and Handling Frensic Analyst - Network Collection and Handling This assessment is one of three, and is specifically focused on items related to Network Forensic operations. In this capations, students will analyze given evidence to identify an intrusion on a new order. In this capations, students will analyze given evidence to identify an intrusion on a new order. In this capations, students will analyze given evidence to identify an intrusion on a new order. In this capations, students will analyze given evidence to identify an intrusion on a new order. In this capations, students will analyze given evidence to identify an intrusion on a new order. In this capations, students will analyze given evidence to identify an intrusion on a new order. In this capations, students will analyze given evidence to identify an intrusion on a new order. In this capations, students will analyze given evidence to identify an intrusion on a new order. In this capations, students will analyze given evidence to identify an intrusion on a new order. In this capations, students will analyze given evidence to identify an intrusion on a new order. In this capations, students will analyze given evidence to identify an intrusion on a new order. In this capations, students will analyze given evidence to identify an intrusion on a new order. In this capations, students will analyze given evidence to identify an intrusion on a new order. In this capations, students will analyze given evidence to identify an intrusion on a new order. In this capations, students will analyze given evidence to identify an intrusion on a new order. In this capations, students will analyze given evidence to identify an intrusion on a new order. In this capation, students will analyze given evidence to identify an intrusion on a new order. In this capation, students will analyze given evidence to identify an intrusion on a new order. In this capation, students will analyze given evidence to identify an intrusio	rensic Analyst - Malware Analysis	This assessment is one of three, and is specifically focused on items related to Malware	CYBRScore	Assessment - Covers dozens of KU	Hyper-V	45 Minutes	1 Hour, 5 Minutes	57 minutes, 11 seconds	1 minute, 29 seconds
Foresic persistions. In this captions, students will analyze given evidence to identify an intrusion on a network, identify if an intrusion course on a system, what it for or emote on an affected system, what to fix or emote on an affected system and what potential changes on the affected system, what to fix or remove on an affected system and what potential changes ended to be made in policy. Forensic Incident Response Captione Forensic Incident Response Captione Forensic Incident Response Captione Forensic System of the affected system, what to fix or remove on an affected system and what potential changes need to be made in policy. Forensic System of the affected system and what potential changes need to be made in policy. Forensic Spottone In Development. CYBRSCORE Digital Media Forensics, HOFJ; Topics: 1, 5, 6, 7, 8, 9, 10 Hyper-V 3 Hours 4 Hours 5 Bi Hours, 20 Minutes 5 Bi Hours, 20 Minutes 5 Bi Hours, 30 Minutes 5 Bi Hours, 30 Minutes 6 Bi Hours, 30 Minutes 1 Development. CYBRSCORE Digital Media Forensics (HOFJ; Topics: 1, 5, 6, 7, 8, 9, 10 1 Development. CYBRSCORE Digital Media Forensics (HOFJ; Topics: 1, 5, 6, 7, 8, 9, 10 1 Development. CYBRSCORE Digital Media Forensics (HOFJ; Topics: 1, 5, 6, 7, 8, 9, 10 1 Development. CYBRSCORE Digital Media Forensics (HOFJ; Topics: 1, 5, 6, 7, 8, 9, 10 1 Development. CYBRSCORE Digital Media Forensics (HOFJ; Topics: 1, 5, 6, 7, 8, 9, 10 1 Development. CYBRSCORE Digital Media Forensics (HOFJ; Topics: 1, 5, 6, 7, 8, 9, 10 1 Development. CYBRSCORE Digital Media Forensics (HOFJ; Topics: 1, 5, 6, 7, 8, 9, 10 1 Development. CYBRSCORE Digital Media Forensics (HOFJ; Topics: 1, 5, 6, 7, 8, 9, 10 1 Development. CYBRSCORE Digital Media Forensics (HOFJ; Topics: 1, 5, 6, 7, 8, 9, 10 1 Development. CYBRSCORE Digital Media Forensics (HOFJ; Topics: 1, 5, 6, 7, 8, 9, 10 1 Development. CYBRSCORE Digital Media Forensics (HOFJ; Topics: 1, 5, 6, 7, 8, 9, 10 1 Development. CYBRSCORE Digital Medi	<u> </u>	This assessment is an a fighter and is an effective former day there exhaust a New and	CYBRScore				· ·		1 minute, 43 seconds
In this captone, student leading analyze given evidence to defently an intrusion on a network, identify in intrusion on a system, which to five remove on an affected system and what potential changes need to be made in policy. Forensic Septone In Development. CYBS.core Digital Media Forensics. (CYBS.core Digital Media Forensics.) (A) Topics: 1, 5, 6, 7, 8, 9, 10 (A) Topics: 1, 5, 6, 7, 8, 9, 10 (A) Topics: 1, 5, 6, 7, 8, 9, 10 (A) Topics: 1, 5, 6, 7, 8, 9, 10 (A) Topics: 1, 5, 6, 7, 8, 9, 10 (A) Topics: 1, 5, 6, 7, 8, 9, 10 (A) Topics: 1, 5, 6, 7, 8, 9, 10 (A) Topics: 1, 5, 6, 7, 8, 9, 10 (A) Topics: 1, 5, 6, 7, 8, 9, 10 (A) Topics: 1, 5, 6, 7, 8, 9, 10 (B) Topics: 1, 5, 6, 7, 8, 9, 10 (B) Topics: 1, 5, 6, 7, 8, 9, 10 (B) Topics: 1, 5, 6, 7, 8, 9, 10 (B) Topics: 1, 5, 6, 7, 8, 9, 10 (CYBS.core Digital Media Forensics (HOF): Topics: 1, 5, 6, 7, 8, 9, 10 (B) Topics: 1, 5, 6, 7,		Forensic operations. In this capstone, students will analyze given evidence to identify an intrusion on a network, identify if an intrusion occurred on a system, what (if anything) was changed on the affected system, what to fix or remove on an affected system and what potential							1 minute, 3 seconds
Forensic Capatone In Development CYBES.core Digital Media Forensic; Host, Forensic, (HOF); Forens		In this capstone, students will analyze given evidence to identify an intrusion on a network, identify if an intrusion occurred on a system, what (if anything) was changed on the affected system, what to fix or remove on an affected system and what potential changes need to be made in policy.							
Tourissic suppliation 10 Development 10 Developme		In Development							
		In Development Exploit Development		Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10				1 minute, 39 seconds	1 minute, 6 seconds
MAL400 exposes students to the theoretical knowledge and hands-on techniques used to analyze malware. In MAL400, students will learn how to identify and analysis and tearn how to identify and analysis assembly, and an introduction to debuggers and disassemblers. WARS.core Labs Software Security Analysis (SSA); Topics: 1, 2, 3, 4, 5 VSphere 40 Hours 41 Hours, 40 Minutes 2 hours, 31 minutes 15 seconds overview of the malware analysis process followed by dynamic analysis, assembly, and an introduction to debuggers and disassemblers.	ndamentals of Malware Analysis	MAI.400 exposes students to the theoretical knowledge and hands-on techniques used to analyze malware. In MAI.400, students will learn how to identify and analyze software that causes harm to users, computers, and networks. Students will dissect malware learn how to identify it, how it works, and how to defeat it. The course begins with an overview of the malware analysic process followed by dynamic analysis, assembly, and an introduction to debuggers and disassemblers.	CYBRScore Labs		vSphere	40 Hours	41 Hours, 40 Minutes	2 hours, 31 minutes	15 seconds
Students will log into an organization's frewall, document existing firewall rules, analyze these rules and making recommendations based on this analysis. Students will then make make the necessary changes. VYBRScore Labs Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a Hyper-V 2 Hours 4 Hours 32 minutes, 22 seconds 38 seconds	p Analysis of Firewall Rules	these rules and making recommendations based on this analysis. Students will then make make the necessary changes.	CYBRScore Labs	Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a	Hyper-V	2 Hours	4 Hours	32 minutes, 22 seconds	38 seconds
Students will log into an organization's freewall, document existing firewall rules, analyze Gap Analysis of Firewall Rules Students will log into an organization's freewall, document existing firewall rules, analyze Organization's freewall rules, analyze Students will log into an organization's freewall, document existing firewall rules, analyze Network Defense (NDF). Topics: 1a, 1c, 1d, 2a, 2b, 4a Hyper-V 1 Hour, 30 Minutes 53 minutes, 14 seconds 2 minutes, 27 2 minutes, 28 2 minutes	p Analysis of Firewall Rules	these rules and making recommendations based on this analysis. Students will then make make the necessary changes.	CYBRScore Scored Labs	Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a	Hyper-V	1 Hour, 30 Minutes	1 Hour, 30 Minutes	53 minutes, 14 seconds	2 minutes, 27 seconds
Students will log into an organization's frewall, document existing firewall mules, analyze these rules and making recommendations based on this analysis. Students will then make make the necessary changes. CYBRScore Network Forensics Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a Hyper-V 1 Hour, 30 Minutes 1 Hour, 30 Minutes 32 minutes, 41 seconds 38 seconds	p Analysis of Firewall Rules	these rules and making recommendations based on this analysis. Students will then	CYBRScore Network Forensics	Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a	Hyper-V	1 Hour, 30 Minutes	1 Hour, 30 Minutes	32 minutes, 41 seconds	38 seconds

Hardening C#.NET Web Apps - Broken Access Control	In this lab, we will show an exploit on a user's cookie, then apply remediation measures, and then reattempt the exploit.	CYBRScore Labs		Hyper-V	1 Hour	1 Hour		
Hardening C#.NET Web Apps - Broken Authentication	This lab teaches methods to secure the authentication methods in a web application written in CN.	CYBRScore Labs		Hyper-V	1 Hour	1 Hour		
Bardening C#.NET Web Apps - Cross Site Scripting	This lab teaches methods to secure web applications written in CII against XSS attacks.							
Hardening C#.NET Web Apps - CSRF	This lab teaches methods to secure web applications written in CII against Cross Site Request Forgery attacks.	CYBRScore Labs		Hyper-V	1 Hour	1 Hour		
Hardening C#.NET Web Apps - File Uploads	This lab teaches methods to secure web applications written in CII with respect to file upload capabilities.							
Hardening C#.NET Web Apps - OS Command Injection	This lab teaches methods to secure a web application written in CN against OS Command	CYBRScore Labs		Hyper-V	30 Minutes	30 Minutes		
Hardening C#.NET Web Apps - Overposting	Injection attacks. N/A							
Hardening C#.NET Web Apps - Password Hashing	This lab teaches how to properly use password hashing in a CII web application.	CYBRScore Labs		Hyper-V	1 Hour	1 Hour		
Hardening C#.NET Web Apps - Secure Deserialization	This lab teaches methods to secure web applications written in CIII against Insecure Deserialization attacks.	CYBRScore Labs		Hyper-V	1 Hour	1 Hour		
Hardening C#.NET Web Apps - Sensitive Data Exposure	This lab teaches how to prevent sensitive data exposure in a PHP web application.							
Hardening C#.NET Web Apps - SQL Injection	This lab teaches methods to secure a web application written in CN against SQL Injection attacks.			Hyper-V	1 Hour	1 Hour		
Hardening C#.NET Web Apps - Two Factor Authentication	This lab teaches how to deploy Google Authenticator in a CII web application in order to deploy Two Factor Authentication.	CYBRScore Labs		Hyper-V	1 Hour	1 Hour		
Hardening C#.NET Web Apps - Web Configuration	This lab teaches methods to secure the CW configuration for web applications written in CW.							
Bardening C#.NET Web Apps - XXE	This lab teaches methods to secure a web application written in CN against XXE attacks.	CYBRScore Labs		Hyper-V	30 Minutes	30 Minutes		
Hash Verification	Students will understand and use hash verification to identify and compare files and forensic images.	CYBRScore Labs	Operating Systems Administration (OSA); Topics: 2, 4, 5, 6, 9, 11	Hyper-V	30 Minutes	1 Hour	47 minutes, 18 seconds	1 minute, 9 seconds
Hash Verification	Students will understand and use hash verification to identify and compare files and	CYBRScore Scored Labs	Operating Systems Administration (OSA); Topics: 2, 4, 5, 6, 9, 11	Hyper-V	1 Hour	1 Hour, 30 Minutes	36 minutes, 31 seconds	1 minute, 30 seconds
Hash Verification	forensic images. Students will understand and use hash verification to identify and compare files and		Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10	Hyper-V	30 Minutes	1 Hour		
Holistic Network Identification and Protection	formsic images. This exercise provides students an opportunity to exercise their network identification and protection capabilities learned in the last week. They are responsible for identifying and leveraging the appropriate tools (of those provided) to identify all components of the network and assess it for potential vulnerabilities.		Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a	Hyper-V	2 Hours	2 Hours		
Host Data Integrity Baselining	This lab takes the trainee into basic concepts regarding establishing baselines of files and directories with Kali Linux and Windows 7. In the first part of the lab, the trainee will establish a baseline of the passwel file within Kali Linux, and in the second part the trainee will establish a baseline of the C\> drive within Windows 7.	CYBRScore Labs	Operating Systems Hardening (OSH); Topics: 1, 2, 3, 4, 5, 6, 7, 8, 10, 11	Hyper-V	1 Hour	1 Hour	17 minutes, 11 seconds	30 seconds
Host Identification Scanning via Windows	Students will leverage Scanline, a Windows network discovery and mapping tool, to identify the systems on a network of responsibility. Students will utilize non-traditional scans to attempt avoiding an Intrusion Detection System (IDS).	CYBRScore Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10	Hyper-V	25 Minutes	45 Minutes	16 minutes, 25 seconds	43 seconds
Host Identification Scanning with Linux	Students will utilize Nmap, a network discovery and mapping tool to identify the systems on a network of responsibility. Using the tool, students will identify other devices on the laboratory network, to include computers and network infrastructure devices, such as routers.		Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10	Hyper-V	1 Hour	1 Hour	41 seconds	29 seconds
Host Identification Scanning with Linux	Students will utilize Nmap, a network discovery and mapping tool to identify the systems on a network of responsibility. Using the tool, students will identify other devices on the laboratory network, to include computers and network infrastructure devices, such as routers.	CYBRScore Scored Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10	Hyper-V	1 Hour	1 Hour	19 minutes, 1 second	1 minute, 3 seconds
Identify Access to a LINUX Firewall Through SYSLOG Service	Students will identify access to a PFSENSE firewall through the forwarding of SYSLOG (System logs) from a Firewall to the SYSLOG service we have configured and set up on the Network. Students will then identify malicious activity through system logs.	CYBRScore Labs	Network Defense (NDF), Topics: 1a, 1c, 1d, 2b, 4a	Hyper-V	30 Minutes	1 Hour	10 minutes, 33 seconds	1 minute, 20 seconds
Identify Access to a LINUX Firewall Through SYSLOG Service	Students will identify access to a PFSENSE firewall through the forwarding of SYSLOG (System logs) from a Firewall to the SYSLOG service we have configured and set up on the Network. Students will then identify malicious activity through system logs.	CYBRScore Scored Labs	Network Defense (NDF), Topics: 1a, 1c, 1d, 2b, 4a	Hyper-V	30 Minutes	1 Hour	34 minutes, 3 seconds	1 minute, 47 seconds
Identify and Remove Trojan Using Various Tools	Students will detect malicious files and processes using various tools. Students will then remove the malicious files and/or processes.	CYBRScore Labs	Operating Systems Administration (OSA); Topics: 2, 4, 5, 6, 9, 11	Hyper-V	45 Minutes	1 Hour	29 minutes, 3 seconds	29 seconds
Identify Rootkit and DLL Injection Activity	Students will use Oily Debugger to debug a suspect program and determine if any of the observed behavior is malicious or not. They will also us Process Hacker to confirm if a possible OLL injection was successful. This lab fosters an understanding of debuggers, shows one possible way malicious software hooks into legitimate programs and will provide an "under the hood" perspective on how programs work in the Windows environment.	CYBRScore Labs	Software Security Analysis (SSA); Topics: 1, 2, 3, 4, 5	Hyper-V	40 Minutes	1 Hour	54 seconds	18 seconds
Identify Rootkit and DLL Injection Activity	Students will use Oily Debugger to debug a suspect program and determine if any of the observed behavior is malicious or not. They will also use Process trakefur to conflict a possible DLI nijection was successful. This lab floaters an understanding of debuggers, howes one possible way malicious software hooks into legitizate programs and will provide an "under the hood" perspective on how programs work in the Windows environment.	CYBRScore Scored Labs	Software Security Analysis (SSA); Topics: 1, 2, 3, 4, 5	Hyper-V	40 Minutes	1 Hour	16 minutes, 8 seconds	1 minute, 32 seconds
Identify Rootkit and DLL Injection Activity Capstone	Students will use DIly bebugger to debug a suspect program and determine if any off the observed behavior is mallicious or not. They will also use Process traker to confirm a possible DLI rijection was successful. This lab fosters an understanding of debuggers, shows one possible way mallicious Sorbare hooks into legitizate programs and use provide an "under the hood" perspective on how programs work in the Windows environment.	CYBRScore Scored Labs	Software Security Analysis (SSA); Topics: 1, 2, 3, 4, 5	Hyper-V	40 Minutes	1 Hour	5 minutes, 7 seconds	1 minute, 8 seconds
Identify Suspicious Information in VM Snapshots	Students will identify known IOCs for Stuxnet and save them for analysis. Students will	CYBRScore Labs	Software Security Analysis (SSA); Topics: 1, 2, 3, 4, 5	Hyper-V	1 Hour	1 Hour	9 minutes, 35 seconds	42 seconds
Identify Whether High-Risk Systems Were Affected	The highest risk systems are the ones with internet facing Applications. One an attacker from the internet is able to compromise the internal network, then it is very likely they will attempt to move to other machines on the network. The machines in the Demilitariest Zone (DMZ) are at high risk because they are not usually as protected as the computers which are part of the internal hetwork.	CYBRScore Labs	Network Security Administration (NSA); Topics: 2, 5, 7, 8, 9, 10	Hyper-V	1 Hour	1 Hour	36 minutes, 16 seconds	28 seconds
Identify Whether High-Risk Systems Were Affected	The highest risk systems are the ones with internet facing Applications. One an attacker from the internet is able to compromise the internal network, then it is very likely they will attempt to move to other machines on the network. The machines in the Demilitarized Zone (DNZ) are at high risk because they are not usually as protected as the computers which are part of the internal Network.	CYBRScore Scored Labs	Network Security Administration (NSA); Topics: 2, 5, 7, 8, 9, 10	Hyper-V	30 Minutes	1 Hour	32 minutes, 27 seconds	1 minute, 54 seconds
Identifying Anomalous ARP	This lab exercise is designed to allow the trainee to become familiar with identifying anomalous ARP traffic.	CYBRScore Labs	Network Defense (NDF), Topics: 1a, 1c, 1d, 2b, 4a	vSphere	1 Hour	1 Hour	34 minutes, 19 seconds	11 seconds
			+	-		-	-	

Identifying Intrusion and Mitigating Attacks with RHEL Server	This last lab is similar to the Windows incident Response lab, but different in that this one requires you from through the flar process in a law, one specifically a fine dividal, environment. The same if methodologies and procedures apply in both environments the same like methodologies and procedures apply in both environments as beta is a possible, removing any present threats if found, recovery, and report-generation. Making sure you account for all of these is the key to sound fit work.	CYBRScore Labs	Linux System Administration (LSA), Topics: 2, 3, 4, 6, - Operating System Concepts (OSC), Topics: 2, 4	Hyper-V	45 Minutes	1 Hour	46 minutes, 45 seconds	56 seconds
Identifying Intrusion and Mitigating Attacks with RHEL Server Capstone	This list lab is similar to the Windows incident Response lab, but different in that this one requires you to nu through the IR process in a linux, more specifically a Red Haten convioument. The same IR methodologies and procedure supply in both environments; these include identifying any security-issues and their scope, containing the Issues as best as possible, removing any present threats if found, recovery, and report-generation. Making sure you account for all of these is the key to sound IR work.	CYBRScore Scored Labs	Linux System Administration (LSA), Topics: 2, 3, 4, 6, - Operating System Concepts (OSC), Topics: 2, 4	Hyper-V	45 Minutes	1 Hour	50 minutes, 46 seconds	1 minute, 13 seconds
Identifying Intrusion and Mitigating Attacks with RHEL Server Capstone	This last lab is similar to the Windows Incident Response lab, but different in that this one requires you to no through the IR process in a linux, more specifically a Red +1xt environment. The same IR methodologies and procedure stayp in both environments; these include identifying any security-issues and their scope, containing the issues as best as possible, removing any present threats if found, recovery, and report-generation. Making sure you account for all of these is the key to sound IR work.	CYBRScore Capstones	Linux System Administration (LSA), Topics: 2, 3, 4, 6, - Operating System Concepts (OSC), Topics: 2, 4	Hyper-V	45 Minutes	1 Hour		
Identifying Key Assets	Students will use nmap to identify specific assets on their network. Students will use nmap to identify specific assets on their network.	CYBRScore Labs CYBRScore Scored Labs	Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a	Hyper-V Hyper-V	1 Hour	1 Hour	38 minutes, 10 seconds 36 minutes, 51 seconds	35 seconds 1 minute, 20 seconds
Identifying Key Assets Identifying Malicious Callbacks	Students will use imap to usentify specific assets on their network. Students will try to identify suspicious behavior on a compromised machine using volatility. Students will then look at processes, parent processes, connections, unlinked DLLs, and mailcious kernel callbacks that are associated with suspected malware.	CYBRScore Labs	Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a	Hyper-V	1 Hour	1 Hour	2 minutes, 26 seconds	33 seconds
Identifying Malicious Callbacks	Students will try to identify suspicious behavior on a compromised machine using volatility. Students will then look at processes, parent processes, connections, unlinked DLLs, and malicious kernel callbacks that are associated with suspected malware.	CYBRScore Scored Labs	Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a	Hyper-V	1 Hour	1 Hour		
Identifying Malicious Network Connections	When investigating a cybersecurity incident it's important to take memory snapshots of affected systems for further analysis. Students will conduct analysis and look for malicious network connections, processes, and other artifacts.	CYBRScore Labs	Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a	Hyper-V	1 Hour	1 Hour	16 minutes, 45 seconds	42 seconds
Identifying Malicious Network Connections	When investigating a cybersecurity incident it's important to take memory snapshots of affected systems for further analysis. Students will conduct analysis and look for malicious network connections, processes, and other artifacts.	CYBRScore Scored Labs	Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a	Hyper-V	1 Hour	1 Hour	19 minutes, 5 seconds	1 minute, 6 seconds
Identifying System Vulnerabilities with OpenVAS	Students will scan a system in OpenVAS (Open Vulnerability Assessment) to discover and identify systems on the network that have vulnerabilities.	CYBRScore Labs	Operating Systems Hardening (OSH), Topics: 11; IT Systems Components (ISC), Topics: 13	Hyper-V	1 Hour	1 Hour	30 minutes, 35 seconds	30 seconds
Identifying System Vulnerabilities with OpenVAS	identify systems on the network that have vulnerabilities. Students will scan a system in OpenVAS (Open Vulnerability Assessment) to discover and		Operating Systems Hardening (OSH), Topics: 11; IT Systems Components (ISC), Topics: 13	Hyner-V	2 Hours	2 Hours	1 hour 6 minutes	1 minute 26 seconds
identifying system vuinerabilities with OpenVAS	identify systems on the network that have vulnerabilities.	CYBRSCOTE SCOTED Labs	Operating Systems Hardening (OSH), Topics: 11; 11 Systems Components (ISC), Topics: 13	nyper-v	2 Hours	2 Hours	1 nour, 6 minutes	1 minute, 26 seconds
IDS Setup and Configuration	Network and host based intrusion Detection Systems (IDS) analyze traffic and provide log and alert data for detected events and activity. Security Onion provides multiple IDS options including Host IDS and Rebords IDS. In this lay out will setup Security Onion to function as a network based IDS and Snorby, the GUI web interface for Snort.	CYBRScore Labs	Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a	Hyper-V	1 Hour, 30 Minutes	1 Hour, 30 Minutes	26 minutes, 2 seconds	29 seconds
IDS Setup and Configuration	Network and host based intrusion Detection Systems (IDS) analyze traffic and provide log and alert data for detected events and activity. Security Onion provides multiple IDS options including Host IDS and Network IDS. In this lay ou will setup Security Onion to function as a network based IDS and Snorby, the GUI web interface for Snort.	CYBRScore Network Forensics	Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a	Hyper-V	1 Hour, 30 Minutes	1 Hour, 30 Minutes	40 minutes, 45 seconds	2 minutes, 1 second
IDS Setup and Configuration	Network and host based intrusion Detection Systems (IDS) analyze traffic and provide log and alert data for detected events and activity. Security Onion provides multiple IDS options including Host IDS and Network IDS. In this lay ou will steep Security Onion to function as a network based IDS and Snorby, the GUI web interface for Snort.	CYBRScore Scored Labs	Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a	Hyper-V	45 Minutes	1 Hour, 30 Minutes	46 minutes, 37 seconds	S8 seconds
Image Forensics Capstone	Students will create a live image using FTK Imager and verify that the image was created	CYBRScore Scored Labs	Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10	Hyper-V	1 Hour	2 Hours	45 minutes, 29 seconds	1 minute, 1 second
	successfully. In this lab, you will make changes to the pfSense firewall in order to block specific ports	CYBRScore Labs			45 Minutes	45 Minutes		
Implement Single System Changes in Firewall	and types of traffic.		Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a	Hyper-V			16 minutes, 22 seconds	27 seconds
Implement Single System Changes in Firewall	In this lab you will make changes to the PFSense Firewall in order to block specific ports and types of traffic.	CYBRScore Network Forensics	Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a	Hyper-V	45 Minutes	45 Minutes	21 minutes, 53 seconds	31 seconds
Implementing Least-Privilege on Windows	Least-privilege is an important concept across many domains (e.g., Windows server/workstation management, networking. Linux management, etc.) and requires great discipline to implement properly. This lab walks students through implementing least privilege in both an Active Directory setup and a normal Windows-based workstation.	CYBRScore Labs	Cybersecurity Principles (CSP), Topics: j; Operating System Concepts (OSC), Topics: 1, 9	Hyper-V	45 Minutes	1 Hour	28 minutes, 53 seconds	27 seconds
Implementing Least-Privilege on Windows	Least-privilege is an important concept across many domains (e.g., Windows server/workstation management, networking, Linux management, etc.) and requires great discipline to implement properly. This lab walks students through implementing least privilege in both an Active Directory setup and a normal Windows-based workstation.	CYBRScore Scored Labs	Cybersecurity Principles (CSP), Topics: J. Operating System Concepts (OSC), Topics: 1, 9	Hyper-V	45 Minutes	1 Hour	41 minutes, 18 seconds	53 seconds
Incident Detection and Identification	Students will demonstrate their capabilities to identify network components and detect potential incident. "MOTE" This is a scenario-based lab. Students receive minimal guidance intentionally this lib reflects environments similar to the certification environment.	CYBRScore Network Forensics	Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a	Hyper-V	2 Hours, 30 Minutes	2 Hours, 30 Minutes	44 minutes, 43 seconds	S1 seconds
Incident Responder - File Collection and Analysis Incident Responder - Reporting and Remediation		CYBRScore CYBRScore	Assessment - Covers dozens of KU	Hyper-V Hyper-V	45 Minutes 45 Minutes	1 Hour	40 minutes, 30 seconds 54 minutes	1 minute, 21 seconds 1 minute, 34 seconds
incident Responder - Reporting and Remediation	In this lab the student will install Microsoft's Enhanced Mitigation Enhanced Toolkit	LTBR3C0fe	Assessment - Covers dozens of KU	nyper-v	45 minutes	1 nouf	54 minutes	1 minute, 34 seconds
Install EMET and Edit Host Files	(EMET) and edit the the computer's /etc/host file to redirect a system to localhost for the purposes of DNS sink-holing.	CYBRScore Labs	Operating Systems Hardening (OSH); Topics: 1, 2, 3, 4, 5, 6, 7, 8, 10, 11	Hyper-V	1 Hour	1 Hour	1 minute, 20 seconds	18 seconds
Installing Patches and Testing Software	Students will identify if a vulnerability is present in the systems and remediate the vulnerability if necessary.	CYBRScore Labs	IT Systems Components (ISC), Topics: 12; Windows System Administration (WSA), Topics: 5; Operating System Hardening (OSH), Topics: 9	Hyper-V	1 Hour, 30 Minutes	1 Hour, 30 Minutes	34 minutes, 20 seconds	28 seconds
Internet History	In this lab, students will look at how to find and identify internet history in a forensic	CYBRScore Labs	Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10	Hyper-V	45 Minutes	1 Hour, 30 Minutes	22 minutes, 24 seconds	1 minute, 30 seconds
	image. In this lab, students will look at how to find and identify internet history in a forensic						,	*******
Internet History	Image.	-	Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10	Hyper-V	45 Minutes	1 Hour, 30 Minutes		
Internet History	In this lab, students will look at how to find and identify internet history in a forensic image.	CYBRScore Scored Labs	Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10	Hyper-V	45 Minutes	1 Hour, 30 Minutes	26 minutes, 36 seconds	1 minute, 32 seconds
Interoffice Communications Correction	Students will identify an inoperable office chat client and fix the issue. The student will then identify a rogue server on a system.	CYBRScore Labs	Cybersecurity Planning and Management (CPM); Topics: 2, 4, 5, 6, 8, 9	Hyper-V	30 Minutes	30 Minutes	11 minutes, 6 seconds	19 seconds
Intro To Linux - Backing Up, Compression, and Scheduling	In this lab we will consider tools that can be used to backup your data. In covering this, we will also look at compression tools and scheduling, which can be used in conjunction with backups to achieve efficient and regular backups.	CYBRScore Scored Labs	Linux System Administration (LSA), Topics: 2, 3, 4, 6 - Cybersecurity Principles (CSP), Topics: j; Operating System Concepts (OSC), Topics: 1, 9	Hyper-V	1 Hour, 30 Minutes	1 Hour, 30 Minutes	1 hour, 55 minutes	2 minutes
Intro to Linux - Bash Scripting	In this lab, you will learn how to write simple programs in Bash. There are many different shells available in Linux that have different features. The features we will cover are specific to Bash.	CYBRScore Scored Labs	Linux System Administration (LSA), Topics: 2, 3, 4, 6 - Cybersecurity Principles (CSP), Topics: j: Operating System Concepts (OSC), Topics: 1, 9	Hyper-V	3 Hours	3 Hours		

Intro To Linux - Capstone	In this lab, we will bring many of the Intro to Linux topics together into a larger challenge lab. You will be given several tasks to complete but you will not be given step by step instructions for completing them.	CYBRScore Labs	Linux System Administration (LSA), Topics: 2, 3, 4, 6 - Cybersecurity Principles (CSP), Topics: j. Operating System Concepts (OSC), Topics: 1, 9	Hyper-V	5 Hours	5 Hours	54 minutes, 18 seconds	1 minute, 43 seconds
Intro To Linux - Command Line Basics	In this lab, you will learn a variety of commands that are useful to know when navigating the Linux command line interface.	CYBRScore Labs	Linux System Administration (LSA), Topics: 2, 3, 4, 6 - Cybersecurity Principles (CSP), Topics: j; Operating System Concepts (OSC), Topics: 1, 9	Hyper-V	1 Hour	1 Hour	1 hour, 20 minutes	47 seconds
Intro To Linux - File Systems	In this lab, we will learn about how the file system is organized in a Linux Operating System, and the location of some of the more important files and directories.	CYBRScore Labs	Linux System Administration (LSA), Topics: 2, 3, 4, 6 - Cybersecurity Principles (CSP), Topics: j. Operating System Concepts (OSC), Topics: 1, 9	Hyper-V	1 Hour	1 Hour	50 minutes, 57 seconds	1 minute, 15 seconds
Intro To Linux - Installing Software	In this lab, we will learn about how to install and update software, both manually, and also with the distribution's package manager. We will focus on two package managers in particular, apt and yum.	CYBRScore Scored Labs	Linux System Administration (LSA), Topics: 2, 3, 4, 6 - Cybersecurity Principles (CSP), Topics: j. Operating System Concepts (OSC), Topics: 1, 9	Hyper-V	1 Hour	1 Hour	26 minutes, 5 seconds	1 minute, 27 seconds
Intro To Linux - Kernel	In this lab, we will look at the Linux Kernel. We will cover kernel modules, custom kernel compilation, kernel configuration tuning, and system commands.	CYBRScore Scored Labs	Linux System Administration (LSA), Topics: 2, 3, 4, 6 - Cybersecurity Principles (CSP), Topics: j. Operating System Concepts (OSC), Topics: 1, 9	Hyper-V	45 Minutes	45 Minutes	1 hour, 11 minutes	1 minute, 8 seconds
Intro To Linux - Networking Tools	In this lab, we will look at the different networking tools in Linux and how to configure networking.	CYBRScore Scored Labs	Linux System Administration (LSA), Topics: 2, 3, 4, 6 - Cybersecurity Principles (CSP), Topics: j; Operating System Concepts (OSC), Topics: 1, 9	Hyper-V	1 Hour	1 Hour	1 hour, 28 minutes	1 minute, 21 seconds
Intro to Linux - Pipes and Filters	In this lab, you will learn how to chain multiple commands together to achieve more complex goals. You will also be exposed to regular expressions and how they can be used in combination with pipes and filters.	CYBRScore Scored Labs	Linux System Administration (LSA), Topics: 2, 3, 4, 6 - Cybersecurity Principles (CSP), Topics: ; Operating System Concepts (OSC), Topics: 1, 9	Hyper-V	2 Hours, 30 Minutes	2 Hours, 30 Minutes		
Intro To Linux - Processes and Booting	In this lab, we will learn how to work with processes in Linux and how the system boots up and the services are managed. Newer versions of Linux use systemd to manage the services, and older versions use System V, and we will look at both.	CYBRScore Scored Labs	Linux System Administration (LSA), Topics: 2, 3, 4, 6 - Cybersecurity Principles (CSP), Topics: j; Operating System Concepts (OSC), Topics: 1, 9	Hyper-V	45 Minutes	45 Minutes	3 hours, 3 minutes	54 seconds
Intro to Linux - Routing and SSH Tunnels	Routing is an important networking concept. Routing is typically done by dedicated routes, but can also be done by host systems, such as pSente or even a regular Linux machine. In a production network, you would likely not use a Linux machine to perform routing, but by experimenting with routing on Linux, you can gain a deeper understanding of how it works and how to configure it.	CYBRScore Scored Labs	Linux System Administration (LSA), Topicx: 2, 3, 4, 6 - Cybersecurity Principles (CSP), Topics: ‡ Operating System Concepts (OSC), Topicx: 1, 9	Hyper-V	2 Hours	2 Hours, 30 Minutes		
Intro To Linux - Sed and Awk	In this lab we will learn how to use some of the more useful parts of Sed and Awk. These two tools are incredibly powerful and can greatly improve your ability to function effectively in a Linux command line environment.	CYBRScore Scored Labs		Hyper-V	3 Hours	3 Hours	4 hours, 33 minutes	37 seconds
Intro To Linux - Text Editors	In this lab, we will learn how to edit basic text files from the command line, as well as a GUI tool for the same. Text files are very common in Linux and are used often for storing data as well as configuration information. Being able to edit these files is of vital importance and if you use Linux regularly, will be a common task.	CYBRScore Scored Labs	Linux System Administration (LSA), Topics: 2, 3, 4, 6 - Cybersecurity Principles (CSP), Topics: ; Operating System Concepts (OSC), Topics: 1, 9	Hyper-V	1 Hour	1 Hour	2 hours, 59 minutes	54 seconds
Intro To Linux - Users and Groups	In this lab, we will look at managing users on a Linux system. In particular, we will cover how to create, modify, and delete users and groups. We will also look at how to assign a file a user and group, and how the basic permissions work in Linux.	CYBRScore Scored Labs	Linux System Administration (LSA), Topics: 2, 3, 4, 6 - Cybersecurity Principles (CSP), Topics: j. Operating System Concepts (OSC), Topics: 1, 9	Hyper-V	1 Hour, 30 Minutes	1 Hour, 30 Minutes	1 hour, 54 minutes	1 minute, 2 seconds
Intro to Python	This lab is a quick introduction to programming in Python. It assumes that you already understand how to program. The goal is to give you a quick familiarity to Python or refresh older knowledge.	CYBRScore Labs		Hyper-V	2 Hours	4 Hours		
Introduction To OWASP Top Ten Environment Setup	Using this environment to setup the testing environment and create a base profile for the OWASP Top Ten Labs.	CYBRScore Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10 - Web Application Security - all topics	Hyper-V	1666 Hours, 39 Minutes	1666 Hours, 39 Minutes		
Introduction To OWASP Top Ten: A1 - Injection	This module for the Introduction to OWASP Top Ten Module covers A1: Injection.	CYBRScore Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10 - Web Application Security - all topics	Hyper-V	45 Minutes	45 Minutes	12 minutes, 52 seconds	28 seconds
Introduction To OWASP Top Ten: A1 - Injection	This module for the Introduction to OWASP Top Ten Module covers A1: Injection.	CYBRScore Scored Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10 - Web Application Security - all topics	Hyper-V	45 Minutes	45 Minutes	34 minutes, 3 seconds	1 minute, 40 seconds
Introduction To OWASP Top Ten: A10 - Insufficient Logging and Monitoring		CYBRScore Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10 - Web Application Security - all topics	Hyper-V	25 Minutes	30 Minutes	9 minutes, 53 seconds	29 seconds
Introduction To OWASP Top Ten: A10 - Insufficient Logging and Monitoring	This module for the Introduction to OWASP Top Ten Module covers A10: Insufficient g Logging and Monitoring.	CYBRScore Scored Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10 - Web Application Security - all topics	Hyper-V	25 Minutes	30 Minutes	25 minutes, 40 seconds	1 minute, 8 seconds
Introduction To OWASP Top Ten: A2 - Broken Authentication	This module for the Introduction to OWASP Top Ten Module covers A2: Broken Authentication.	CYBRScore Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10 - Web Application Security - all topics	Hyper-V	25 Minutes	30 Minutes	11 minutes, 5 seconds	1 minute, 12 seconds
Introduction To OWASP Top Ten: A2 - Broken Authentication	This module for the introduction to OWASP Top Ten Module covers A2: Broken Authentication.	CYBRScore Scored Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10 - Web Application Security - all topics	Hyper-V	25 Minutes	30 Minutes	14 minutes, 45 seconds	1 minute, 10 seconds
Introduction To OWASP Top Ten: A3 - Sensitive Data Exposure	This module for the Introduction to OWASP Top Ten Module covers A3: Sensitive Data Exposure.	CYBRScore Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10 - Web Application Security - all topics	Hyper-V	40 Minutes	45 Minutes	32 minutes, 13 seconds	34 seconds
Introduction To OWASP Top Ten: A3 - Sensitive Data Exposure	This module for the Introduction to OWASP Top Ten Module covers A3: Sensitive Data Exposure.	CYBRScore Scored Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10 - Web Application Security - all topics	Hyper-V	40 Minutes	45 Minutes	28 minutes, 36 seconds	1 minute, 35 seconds
Introduction To OWASP Top Ten: A4 - XML External Entities	This module for the Introduction to OWASP Top Ten Module covers A4: XML External Entities.	CYBRScore Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10 - Web Application Security - all topics	Hyper-V	30 Minutes	30 Minutes	10 minutes, 40 seconds	31 seconds
Introduction To OWASP Top Ten: A4 - XML External Entities	This module for the Introduction to OWASP Top Ten Module covers A4: XML External Entities.	CYBRScore Scored Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10 - Web Application Security - all topics	Hyper-V	30 Minutes	30 Minutes	17 minutes, 32 seconds	1 minute, 19 seconds
Introduction To OWASP Top Ten: A5 - Broken Access Control	This module for the introduction to OWASP Top Ten Module covers A5: Broken Access Control. This module for the introduction to OWASP Top Ten Module covers A5: Broken Access	CYBRScore Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10 - Web Application Security - all topics	Hyper-V	30 Minutes	30 Minutes	32 minutes, 26 seconds	1 minute, 4 seconds
Introduction To OWASP Top Ten: A5 - Broken Access Control	Control.	CYBRScore Scored Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10 - Web Application Security - all topics	Hyper-V	30 Minutes	30 Minutes	22 minutes, 28 seconds	1 minute, 15 seconds
Introduction To OWASP Top Ten: A6 - Security Misconfiguration	This module for the introduction to OWASP Top Ten Module covers A6: Security Misconfiguration.	CYBRScore Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10 - Web Application Security - all topics	Hyper-V	25 Minutes	45 Minutes		
Introduction To OWASP Top Ten: A6 - Security Misconfiguration	This module for the Introduction to OWASP Top Ten Module covers A6: Security Misconfiguration.	CYBRScore Scored Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10 - Web Application Security - all topics	Hyper-V	25 Minutes	45 Minutes	22 minutes, 19 seconds	1 minute, 23 seconds
Introduction To OWASP Top Ten: A7 - Cross Site Scripting	This module for the Introduction to OWASP Top Ten Module covers A7: Cross Site Scripting	CYBRScore Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10 - Web Application Security - all topics	Hyper-V	1 Hour	1 Hour	27 minutes, 16 seconds	35 seconds
Introduction To OWASP Top Ten: A7 - Cross Site Scripting	This module for the Introduction to OWASP Top Ten Module covers A7: Cross Site Scripting	CYBRScore Scored Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10 - Web Application Security - all topics	Hyper-V	1 Hour	1 Hour	27 minutes, 48 seconds	1 minute, 26 seconds
Introduction To OWASP Top Ten: A8 - Insecure Deserialization	This module for the Introduction to OWASP Top Ten Module covers A8: Insecure Descrialization.	CYBRScore Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10 - Web Application Security - all topics	Hyper-V	25 Minutes	30 Minutes	9 minutes, 38 seconds	30 seconds
Introduction To OWASP Top Ten: A8 - Insecure Deserialization	This module for the Introduction to OWASP Top Ten Module covers A8: Insecure Descrialization.	CYBRScore Scored Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10 - Web Application Security - all topics	Hyper-V	25 Minutes	30 Minutes	10 minutes, 6 seconds	1 minute, 3 seconds
Introduction To OWASP Top Ten: A9 - Using Components With Known Vul	n This module for the Introduction to OWASP Top Ten Module covers A9: Using Components With Known Vulnerabilities.	CYBRScore Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10 - Web Application Security - all topics	Hyper-V	40 Minutes	40 Minutes	24 minutes, 56 seconds	34 seconds
Introduction To OWASP Top Ten: A9 - Using Components With Known Vul		CYBRScore Scored Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10 - Web Application Security - all topics	Hyper-V	40 Minutes	40 Minutes	32 minutes, 36 seconds	58 seconds
Introduction To OWASP Top Ten: Capstone	This lab is a capstone event for the ten Intro to the OWASP Top Ten labs. It incorporates all ten vulnerabilities in a simulated website.	CYBRScore Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10 - Web Application Security - all topics	Hyper-V	1 Hour, 30 Minutes	1 Hour, 30 Minutes	26 minutes, 36 seconds	42 seconds

Introduction to Squert Introduction to Squert In this lab, you will detected by the set The purpose of this strict and environment Orientation - Master Copy The purpose of this strict and environment Students will be the Students will be the Intelligence the plan Intelligence the plan posture of the plan strict and the st	s lab is to allow you to familiarize yourself with the Lab on Demand	CYBRScore Scored Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10 - Web Application Security - all topics	Hyper-V	1 Hour. 30 Minutes	1 Hour. 30 Minutes		
Introduction to Squert In this lab, you will to detected by these to detected by the secret do yet to yet the y	learn how to use Squert to view previously generated event data nsors. s lab is to allow you to familiarize yourself with the Lab on Demand				1 Hour, 50 Williates	1 riour, 50 minutes	29 minutes, 18 seconds	1 minute, 8 seconds
Lab Environment Orientation - Master Copy The purpose of this visual environment or survival environm	s lab is to allow you to familiarize yourself with the Lab on Demand	CYBRScore Labs	Network Defense (NDF), Topics: 1a, 1c, 1d, 2b, 4a	Hyper-V	30 Minutes	1 Hour	36 minutes, 26 seconds	1 minute, 42 seconds
Sudents Will levera to perform an intention to perform an intention posture of the device Sudents Will levera posture of the device Sudents Will levera order to perform an intelligence Resources the gas the devices on the Sudents Will levera order to perform a intelligence Resources the gas the devices on the Sudents Will levera order to perform a		CYBRScore Labs	NOT APPLICABLE	Hyper-V	6 Hours	6 Hours	42 minutes, 58 seconds	55 seconds
Students will levera order to perform an intelligence Resources intelligence they go the devices on the the devices on the Students will levera order to perform a students will levera order to perform an order to perform and order to perfor	age zenmap and Microsoft Baseline Security Analyzer (MBSA) in order mal scan of networked resources. They will, in turn, use the ave gathered about these scanned systems to evaluate the security ices on the network.		Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10	Hyper-V	45 Minutes	1 Hour	1 minute, 26 seconds	35 seconds
Louissaring Internal Intelligence Resources Constant	age a Zenmap and Microsoft Baseline Security Analyzer (MBSA) in internal scan of networked resources. They will, in turn, use the ather about these scanned systems to evaluate the security posture of network.	CYBRScore Scored Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10	Hyper-V	45 Minutes	1 Hour	51 minutes, 9 seconds	1 minute, 1 second
the devices on the		CYBRScore Capstones	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10	Hyper-V	45 Minutes	1 Hour	4 minutes, 8 seconds	1 minute, 59 seconds
Linux Analysis Students will use a interesting items in	given image to become familiar with where to find forensically a standard Linux distribution.	CYBRScore Digital Media Forensics	Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10	Hyper-V	1 Hour	2 Hours	56 seconds	29 seconds
Linux Analysis Students will use a		CYBRScore Labs	Host Forensics (HOF), Topics: 1	Hyper-V	1 Hour	2 Hours		
Linux Analysis Students will use a	given image to become familiar with where to find forensically	CYBRScore Scored Labs	Host Forensics (HOF), Topics: 1	Hyper-V	30 Minutes	1 Hour	35 minutes, 16 seconds	1 minute, 44 seconds
Linux Evaluitation During this lab, you	n a standard Linux distribution. u will use scanning and enumeration techniques to explore vulnerable	CYBRScore Scored Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10	Hyper-V	1 Hour	1 Hour	48 minutes, 1 second	51 seconds
services on two diff	Terent Linux servers.					1 Hour		
services on two diff	ferent Linux servers.		Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10 Linux System Administration (LSA), Topics: 2, 3, 4, 6 - Cybersecurity Principles (CSP), Topics: j:	Hyper-V			37 minutes, 8 seconds	1 minute, 26 seconds
Linux Familiarization Lab Lab to familiarize st		CYBRScore Labs	Operating System Concepts (OSC), Topics: 1, 9 Linux System Administration (LSA), Topics: 2, 3, 4, 6 - Cybersecurity Principles (CSP), Topics: 5 Operating System Concepts (OSC), Topics: 1, 9	vSphere		2 Hours	33 minutes, 59 seconds	11 seconds
Linux Familiarization Lab Lab to familiarize st		CYBRScore Scored Labs	Operating System Concepts (OSC), Topics: 1, 9	vSphere	1 Hour	2 Hours	30 minutes, 24 seconds	11 seconds
routers, but can also Linux Routing machine. In a produ routing, but by exp understanding of he	erimenting with routing on Linux, you can gain a deeper low it works and how to configure it.	erotecore mass	Linux System Administration (LSA), Topics: 2, 3, 4, 6 - Cybersecurity Principles (CSP), Topics: ; Operating System Concepts (OSC), Topics: 1, 9	Hyper-V	2 Hours	2 Hours, 30 Minutes	48 minutes, 29 seconds	1 minute, 13 seconds
	s will use command line tools to create, modify, and manage users and Linux operating environment.		Linux System Administration (LSA), Topics: 2, 3, 4, 6 - Cybersecurity Principles (CSP), Topics: j. Operating System Concepts (OSC), Topics: 1, 9	Hyper-V	1 Hour	1 Hour	17 minutes, 8 seconds	20 seconds
Linux Users and Groups In this lab students	will use command line tools to create, modify, and manage users and Linux operating environment.	CVBRScore Scored Lahs	Linux System Administration (LSA), Topics: 2, 3, 4, 6 - Cybersecurity Principles (CSP), Topics: j. Operating System Concepts (OSC), Topics: 1, 9	Hyper-V	1 Hour	1 Hour	22 minutes, 30 seconds	1 minute, 19 seconds
Linux x64 Binary Exploitation with ASLR and PIE Awaiting Verificatio	on	CYBRScore Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10			4 Hours		1 minute, 23 seconds
Linux x64 Binary Exploitation with NX and ROP Awaiting Verificatio Linux x64 Binary Exploitation with Stack Canaries (Part 1) Awaiting Verificatio			Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10 Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10	Hyper-V Hyper-V		4 Hours 2 Hours	1 day, 4 hours, 10 minutes 3 hours, 20 minutes	1 minute, 27 seconds 1 minute, 25 seconds
Linux x64 Binary Exploitation with Stack Canaries (Part 2) Awaiting Verificatio			Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10	Hyper-V	1 Hour, 30 Minutes	1 Hour, 30 Minutes	37 minutes, 9 seconds	56 seconds
Live Imaging with FTK Imager and Data Recovery with Autopsy Students will create successfully.	e a live image using FTK Imager and verify that the image was created	CYBRScore Scored Labs	Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10	Hyper-V	1 Hour, 30 Minutes	2 Hours	1 hour, 13 minutes	50 seconds
Live Imaging with FTK Imager Lite After they create th	TK Imager Lite to create a forensic image of a Windows 8 workstation. he image they will perform a hash check to ensure that the image that same as what is currently running on the live system.	CYBRScore Labs	Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10	Hyper-V	45 Minutes	1 Hour	39 minutes, 29 seconds	45 seconds
LNX101 - Bash Scripting In this lab, you will			Linux System Administration (LSA), Topics: 2, 3, 4, 6,	Hyper-V		3 Hours	3 hours, 34 minutes	38 seconds
the linux environme		CYBRScore Labs	Linux System Administration (LSA), Topics: 2, 3, 4, 6,	Hyper-V	1 Hour	1 Hour	24 minutes, 59 seconds	43 seconds
LNX101 - Fail2Ban Setup and Analysis environment.		CYBRScore Labs	Linux System Administration (LSA), Topics: 2, 3, 4, 6,	Hyper-V	1 Hour	1 Hour	20 minutes, 55 seconds	23 seconds
LNX101 - File System Structure In this lab, you will in this lab,	learn the basic file system layout and structure in a typical Linux	CYBRScore Scored Labs	Linux System Administration (LSA), Topics: 2, 3, 4, 6,	Hyper-V	1 Hour	1 Hour		
	learn how to install, configure, harden and test an OpenSSH server.	CYBRScore Labs						
LNX101 - OpenSSH Installation, Configuration, and Hardening In this lab, you will	0.7	CTDIGCOIC LUDG	Operating Systems Hardening (OSH), Topics: 2, 4, 8	Hyper-V	1 Hour	1 Hour	14 minutes, 14 seconds	24 seconds
LNX101 - Pines and Filters In this lab, you will I	to a contract of the contract		Operating Systems Hardening (OSH), Topics: 2, 4, 8 Linux System Administration (LSA), Topics: 2, 3, 4, 6,			1 Hour 2 Hours, 30 Minutes	14 minutes, 14 seconds 3 hours, 24 minutes	24 seconds 41 seconds
LNX101 - Pipes and Filters In this lab, you will complex goals. LNX101 - Sottler I.e Escuell With UEM and Escuelld In this lab, you will in this lab, you will not seen and the second of the seco	learn how to chain multiple commands together to achieve more	CYBRScore Labs		Hyper-V	2 Hours			
UNX101 - Pipes and Filters in this lab, you will like the complex goals. UNX101 - Setting Up a Firewall With UFW and Firewalld in this lab, you will receive the complex goals. UNX101 - Setting Up a Firewall With UFW and Firewalld or Uncomplexed in this lab, you will like lab. You will be set the complexed or Uncomplexed in this lab. You will not lab. You will not lab. You will be set to the complexed or Uncomplexed in this lab. You will not lab. You will n	learn how to chain multiple commands together to achieve more learn how to use two common firewall management tools called UFW Firewall and Firewalld. learn how to use telnet, an insecure protocol that sends its data over	CYBRScore Labs CYBRScore Labs	Linux System Administration (LSA), Topics: 2, 3, 4, 6,	Hyper-V	2 Hours 3 Hours	2 Hours, 30 Minutes	3 hours, 24 minutes	41 seconds
LNX101 - Pipes and Filters In this lab, you will complex goals. LNX101 - Setting Up a Firewall With UFW and Firewalld or Uncomplex goals. LNX101 - Telnet vs. SSH In this lab, you will the network in an up the network in an up in this lab, you will the network in an up in this lab students.	learn how to chain multiple commands together to achieve more learn how to use two common firewall management tools called UFW rirewall and if Frewald! Learn how to use telbett, an insecure protocol that sends its data over unencrypted form.	CYBRScore Labs CYBRScore Labs	Linux System Administration (LSA), Topics: 2, 3, 4, 6, Linux System Administration (LSA), Topics: 2, 3, 4, 6,	Hyper-V Hyper-V	2 Hours 3 Hours 1 Hour	2 Hours, 30 Minutes 3 Hours	3 hours, 24 minutes 59 minutes, 18 seconds	41 seconds 57 seconds
LNX101 - Pipes and Filters In this Ia, you will. LNX101 - Setting Up a Firewall With UFW and Firewalld UXX101 - Setting Up a Firewall With UFW and Firewalld UXX101 - Telnet vs. SSH Log Analysis Log Analysis In this Iab students	learn how to chain multiple commands together to achieve more learn how to use two common firewall management tools called UFW rirewall and Frewalld. learn how to use thete, an insecure protocol that sends its data over unencrypted form. If we have the opportunity to review various log files associated with stating system. Upon completing this exercise, the will be able to	CYBRScore Labs CYBRScore Labs CYBRScore Labs	Linux System Administration (LSA), Topics: 2, 3, 4, 6, Linux System Administration (LSA), Topics: 2, 3, 4, 6, Linux System Administration (LSA), Topics: 2, 3, 4, 6,	Hyper-V Hyper-V Hyper-V	2 Hours 3 Hours 1 Hour	2 Hours, 30 Minutes 3 Hours 1 Hour	3 hours, 24 minutes 59 minutes, 18 seconds 17 minutes, 6 seconds	41 seconds 57 seconds 21 seconds
LNX101 - Pipes and Filters In this lab, you will complex golds. LNX101 - Setting Up a Firewall With UFW and Firewalld in this lab, you will or Uncomplexed	learn how to chain multiple commands together to achieve more learn how to use two common firewall management tools called UFW irrewall and ifewalld! Learn how to use tehete, an insecure protocol that sends its data over unencrypted form. Will have the opportunity to review various log files associated with atting system. Upon completing this exercise, the will be able to to log events and analyse system events. Will have the opportunity to review various log files associated with atting system. Upon completing this exercise, the will be able to to log events and analyse system events.	CYBRScore Labs CYBRScore Labs CYBRScore Labs CYBRScore Labs	Linux System Administration (LSA), Topics: 2, 3, 4, 6, Linux System Administration (LSA), Topics: 2, 3, 4, 6, Linux System Administration (LSA), Topics: 2, 3, 4, 6, Host Forensics (HOP); Topics: 1, 5, 6, 7, 8, 9, 10	Hyper-V Hyper-V Hyper-V	2 Hours 3 Hours 1 Hour 45 Minutes 45 Minutes	2 Hours, 30 Minutes 3 Hours 1 Hour 45 Minutes	3 hours, 24 minutes 59 minutes, 18 seconds 17 minutes, 6 seconds 29 minutes, 46 seconds	41 seconds 57 seconds 21 seconds 40 seconds
LIXXIO1 - Pipes and Filters LIXXIO1 - Setting Up a Firewall With UFW and Firewalld In this lab, you will on this lab, you will on this lab, you will on the lab, you will on the lab, you will on the lab, you will not lab, you will not lab, you will not be lab, you will not so, you	learn how to chain multiple commands together to achieve more learn how to use two common firewall management tools called UFW rirewall and if Frewalds. Learn how to use tehest, an insecure protocol that sends its data over unencrypted form. Will have the opportunity to review various log files associated with atting system. Upon completing this exercise, the will be able to to governst and nauky system events. It will have the opportunity to review various log files associated with atting system. Upon completing this exercise, the will be able to to governst and nauky system events.	CYBRScore Labs CYBRScore Labs CYBRScore Labs CYBRScore Labs CYBRScore Scored Labs CYBRScore Scored Labs	Linux System Administration (LSA), Topics: 2, 3, 4, 6, Linux System Administration (LSA), Topics: 2, 3, 4, 6, Linux System Administration (LSA), Topics: 2, 3, 4, 6, Host Forensics (NOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (NOF); Topics: 1, 5, 6, 7, 8, 9, 10	Hyper-V Hyper-V Hyper-V Hyper-V	2 Hours 3 Hours 1 Hour 45 Minutes 45 Minutes	2 Hours, 30 Minutes 3 Hours 1 Hour 45 Minutes 45 Minutes	3 hours, 24 minutes 59 minutes, 18 seconds 17 minutes, 6 seconds 29 minutes, 46 seconds 15 minutes, 5 seconds	41 seconds 57 seconds 21 seconds 40 seconds 1 minute, 9 seconds
LIXX101 - Pipes and Filters LIXX101 - Setting Up a Firewall With UFW and Firewalld or Uncomplete golds. LIXX101 - Setting Up a Firewall With UFW and Firewalld or Uncompleted Firewall or Uncompleted Firewall or In this lab, you will be network in an In Inthia Students the Windows opera configure systems to Log Analysis Log Analysis Log Correlation Log Correlation Students Windows opera configure systems to the Windows opera configure syste	learn how to chain multiple commands together to achieve more learn how to sue two common frewall management tools called UTW frewall and firewall. He can be common frewall management tools called UTW frewall and firewall. He can be common to the can be common to the can be common to learn bow to sue teheet, an insecure protocol that sends its data over unemorpated form. When the common to the common to will have the opportunity to review various log files associated with sting system. Upon completing this exercise, the will be able to to log events and analyse system events. It will have the opportunity to review various log files associated with sting system. Upon completing this exercise, the will be able to to log events and analyse system events. And place to log events and analyse system events place to determine if a weeth has occurred, and if so, who may be behind it. etworked digital systems, attention must be paid to the logging place to detect suspicious behavior. In this lab, students will work correlate server logs, setten logs, and application logs in order to correlate server logs, setten logs, and application logs in order to correlate server logs, setten logs, and application logs in order to correlate server logs, setten logs, and application logs in order to correlate server logs, setten logs, and application logs in order to correlate server logs.	CYBRScore Labs CYBRScore Labs CYBRScore Labs CYBRScore Scored Labs CYBRScore Scored Labs CYBRScore Scored Labs CYBRScore Labs	Linux System Administration (LSA), Topics: 2, 3, 4, 6, Linux System Administration (LSA), Topics: 2, 3, 4, 6, Linux System Administration (LSA), Topics: 2, 3, 4, 6, Host Forensics (NOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (NOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (NOF); Topics: 1, 5, 6, 7, 8, 9, 10	Hyper-V Hyper-V Hyper-V Hyper-V Hyper-V Hyper-V	2 Hours 3 Hours 1 Hour 45 Minutes 45 Minutes 40 Minutes 49 Minutes	2 Hours, 30 Minutes 3 Hours 1 Hour 45 Minutes 45 Minutes 45 Minutes	3 hours, 24 minutes 59 minutes, 18 seconds 17 minutes, 6 seconds 29 minutes, 6 seconds 15 minutes, 5 seconds 45 minutes, 53 seconds	41 seconds 57 seconds 21 seconds 40 seconds 1 minute, 9 seconds 45 seconds
LNXIO1 - Pipes and Filters LNXIO1 - Setting Up a Firewall With UFW and Firewalld In this lab, you will or incomplex cods. In this lab, you will the network in an u In this lab, you will the network in an u In this lab, you will the network in an u In this lab students the Windows opera configure systems to In this lab students the Windows opera configure systems to Log Analysis Log Correlation Students will use Sp physical security ev When defending ne mechanisms set in j with Splunk to help determine if an atta When defending ne mechanisms set in j with Splunk to ledge determine set in atta Students will solve to deduction in this set of the security ev When defending ne mechanisms set in j with Splunk to help determine if an atta Students will splunk to help determine if an atta	learn how to chain multiple commands together to achieve more learn how to use two common ferwell management tools called UTW friewall and firewall. learn how to use teheet, an insecure protocol that sends its data over unemcrypted form. will have the apportunity to review various log files associated with atting system, upon completing this exercise, the will be able to to log events and analyze system events. will have the apportunity to review various log files associated with atting system. Upon completing this exercise, the will be able to to log events and analyze system events. Juliuh to repeat server logs and physical access log to determine if a went has occurred, and if so, who may be behind it. etworked digital systems, attention must be paid to the logging place to detect suspicious behavior. In this lab, students will work correlate server logs, yetten logs, and application logs in order to successful, and if no what happened and how they got in the velowed digital systems, attention must be paid to the logging place to detect suspicious behavior. In this lab, students will work where the control of the paid to the logging place to detect suspicious behavior. In this lab, students will work correlate server logs, system logs, and application logs in order to correlate server logs, system logs, and application logs in order to correlate server logs, system logs, and application logs in order to correlate server logs, system logs, and application logs in order to correlate server logs, system logs, and application logs in order to correlate server logs in order t	CYBRScore Labs CYBRScore Labs CYBRScore Labs CYBRScore Scored Labs CYBRScore Scored Labs CYBRScore Scored Labs CYBRScore Labs	Linux System Administration (LSA), Topics: 2, 3, 4, 6, Linux System Administration (LSA), Topics: 2, 3, 4, 6, Linux System Administration (LSA), Topics: 2, 3, 4, 6, Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Network Defense (NDF); Topics: 1a, 1c, 1d, 2a, 2b, 4a	Hyper-V Hyper-V Hyper-V Hyper-V Hyper-V Hyper-V Hyper-V Hyper-V	2 Hours 3 Hours 1 Hour 45 Minutes 45 Minutes 40 Minutes 49 Minutes	2 Hours, 30 Minutes 3 Hours 1 Hour 45 Minutes 45 Minutes 45 Minutes	3 hours, 24 minutes 59 minutes, 18 seconds 17 minutes, 6 seconds 29 minutes, 46 seconds 15 minutes, 5 seconds 45 minutes, 53 seconds	41 seconds 57 seconds 21 seconds 40 seconds 1 minute, 9 seconds 45 seconds
LIXXIO1 - Pipes and Filters LIXXIO1 - Setting Up a Firewall With UFW and Firewalld In this lab, you will or through a firewall with UFW and Firewalld In this lab, you will or through a firewall with UFW and Firewalld In this lab, you will the network in an u in this lab students the Windows opera congrue systems. Log Analysis In this lab students the Windows opera congrue systems to the Windows opera congrue systems. Log Correlation Students will use Sp physical security or when defending a mechanisms set in which splunk to help determine if an atta Upg Correlation & Analysis to Identify Potential IOC with Splunk to help determine if an atta Upg Correlation & Analysis to Identify Potential IOC which splunk to help determine if an atta Upg Correlation & Analysis to Identify Potential IOC with Splunk to help determine if an atta When defending a mechanisms set in with Splunk to help determine if an atta Students will corele be determined in a set of the splunk to help determined in a set of the splunk to h	learn how to chain multiple commands together to achieve more learn how to sue two common frewall management tools called UTW frewall and frewall. He can be common frewall management tools called UTW frewall and frewall. He can be common to such that sends its data over unemcrypted form. It will have the opportunity to review various log files associated with sting system. Upon completing this exercise, the will be able to to log events and analyse system events, which have the opportunity to review various log files associated with sting system. Upon completing this exercise, the will be able to to log events and analyse system events, and pulse to log events and analyse system events. The will be able to to log events and analyse system events plants to ingest server logs and a physical access log to determine if a vent has occurred, and if so, who may be behind it. etworked digital systems, attention must be paid to the logging place to detect suspicious behavior. In this lab, students will work correlate server logs, system logs, and application logs in order to acker was successful, and if so what happeend and how they got in. etworked digital systems, attention must be paid to the logging place to detect suspicious behavior. In this lab, students will work so correlate server logs, system logs, and application logs in order to acker was successful, and if so what happeend and how they got in. late server logs, system logs, and application logs to determine what colbinate to the system and what program was used to provide poblank to ingest server logs and a physical access log to determine if a event has occurred, and if so, who may be behind it.	CYBRScore Labs CYBRScore Labs CYBRScore Labs CYBRScore Scored Labs CYBRScore Scored Labs CYBRScore Scored Labs CYBRScore Labs CYBRScore Labs CYBRScore Labs CYBRScore Labs CYBRScore Scored Labs CYBRScore CAPSTONES CYBRSCORE CAPSTONES	Linux System Administration (LSA), Topics: 2, 3, 4, 6, Linux System Administration (LSA), Topics: 2, 3, 4, 6, Linux System Administration (LSA), Topics: 2, 3, 4, 6, Host Forensics (NOF), Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (NOF), Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (NOF), Topics: 1, 5, 6, 7, 8, 9, 10 Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a	Hyper-V	2 Hours 3 Hours 1 Hour 45 Minutes 45 Minutes 49 Minutes 49 Minutes 49 Minutes 49 Minutes	2 Hours, 30 Minutes 3 Hours 1 Hour 45 Minutes 45 Minutes 45 Minutes 1 Hour 1 Hour 45 Minutes 1 Hour 45 Minutes	3 hours, 24 minutes 59 minutes, 18 seconds 17 minutes, 6 seconds 29 minutes, 46 seconds 15 minutes, 5 seconds 45 minutes, 53 seconds 1 minute, 59 seconds 27 minutes, 58 seconds 35 minutes, 11 seconds 34 minutes, 32 seconds	41 seconds 57 seconds 21 seconds 40 seconds 1 minute, 9 seconds 45 seconds 1 minute, 6 seconds 1 minute, 6 seconds
LIXXIO1 - Pipes and Filters LIXXIO1 - Setting Up a Firewall With UFW and Firewalld In this lab, you will or thoropicated of LIXXIO1 - Telnet vs. SSH In this lab, you will or thoropicated or in this lab, you will the network in an u in this lab, you will the network in an u in this lab, you will the network in an u in this lab students the Windows opera configure systems to When defending ne mechanisms set up with Splank to help defermine if an att with Splank to help defermine and Analysis to Identify Potential IOC one characters set in with Splank to help defermine and Analysis Log Correlation and Analysis Log Correlation Capstone plysical security ev Students will use Sp Splightizal security ev Log Event Reports Students will use Sp	learn how to chain multiple commands together to achieve more learn how to use two common firewall management tools called UTW firewall and firewall. Itematical management to the service of the serv	CYBRScore Labs CYBRScore Labs CYBRScore Labs CYBRScore Scored Labs CYBRScore Scored Labs CYBRScore Scored Labs CYBRScore Scored Labs CYBRScore Labs CYBRScore Labs CYBRScore Labs CYBRScore Capstones CYBRScore Labs	Linux System Administration (LSA), Topics: 2, 3, 4, 6, Linux System Administration (LSA), Topics: 2, 3, 4, 6, Linux System Administration (LSA), Topics: 2, 3, 4, 6, Host Forensics (NOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (NOF); Topics: 1, 5, 6, 7, 8, 9, 10 Network Defense (NOF); Topics: 1, 5, 6, 7, 8, 9, 10 Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a	Hyper-V	2 Hours 3 Hours 1 Hour 45 Minutes 45 Minutes 49 Minutes 49 Minutes 49 Minutes 40 Minutes 41 Minutes 42 Minutes 43 Minutes 44 Minutes 45 Minutes	2 Hours, 30 Minutes 3 Hours 1 Hour 45 Minutes 45 Minutes 45 Minutes 1 Hour 45 Minutes 1 Hour 45 Minutes 1 Hour 45 Minutes 1 Hour	3 hours, 24 minutes 59 minutes, 18 seconds 17 minutes, 6 seconds 29 minutes, 6 seconds 15 minutes, 5 seconds 45 minutes, 53 seconds 1 minute, 59 seconds 27 minutes, 58 seconds 35 minutes, 11 seconds 34 minutes, 32 seconds 24 minutes, 32 seconds	41 seconds 57 seconds 21 seconds 40 seconds 1 minute, 9 seconds 45 seconds 1 minute, 6 seconds 1 minute, 6 seconds 1 minute, 19 seconds 1 seconds 1 seconds 1 seconds 1 seconds
LIXXIO1 - Pipes and Filters LIXXIO1 - Setting Up a Firewall With UFW and Firewalld or thought and the network in an in this lab, you will will be a set of the set of the network in an in this lab students the windows opera confligure systems to the windows opera confligure systems. Log Correlation & Analysis to Identify Potential IOC When defending no mechanisms set in which splanks to be determined if an attain the windows opera confligure systems to the windows opera confligure systems. The windows opera confligure systems in the windows opera confligure systems to the windows opera confligure systems. Log Correlation & Analysis to Identify Potential IOC When defending no mechanisms set in which should be a subject to the windows opera confligure systems in the windows opera confligure systems. The windows opera confligure systems in the windows o	learn how to chain multiple commands together to achieve more learn how to sue two common firewall management tools called UTW freewall and firewall. Learn how to use tehest, an insecure protocol that sends its data over memorypate from . I will have the opportunity to review various log files associated with atting system. Upon completing this exercise, the will be able to to log events and analyze system events. I will have the opportunity to review various log files associated with atting system. Upon completing this exercise, the will be able to to log events and analyze system events. I will have the opportunity to review various log files associated with atting system. Upon completing this exercise, the will be able to to log events and analyze system events. I will have the opportunity to review various log files associated with an advanced of the complete special special special properties of the complete special special properties and public to increase and special special special correlate server logs, system logs, and application logs to order to acker was successful, and if so what happened and how they got in cheworked digital systems, attention must be paid to the logging place to detect suspicious behavior. In this lab, students will work correlate server logs, system logs, and application logs to order to acker was successful, and if so what happened and thow they got in tacker was successful, and if so what happened an the server logs, system logs, and application logs to order to acker was successful, and if so what happened and the server logs and aphysical access log to determine if a went has occurred, and if so, who may be behind it.	CYBRScore Labs CYBRScore Labs CYBRScore Labs CYBRScore Scored Labs CYBRScore Scored Labs CYBRScore Scored Labs CYBRScore Scored Labs CYBRScore Labs CYBRScore Labs CYBRScore Labs CYBRScore Capstones CYBRScore Labs	Linux System Administration (LSA), Topics: 2, 3, 4, 6, Linux System Administration (LSA), Topics: 2, 3, 4, 6, Linux System Administration (LSA), Topics: 2, 3, 4, 6, Host Forensics (NOF), Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (NOF), Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (NOF), Topics: 1, 5, 6, 7, 8, 9, 10 Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a	Hyper-V	2 Hours 3 Hours 1 Hour 45 Minutes 45 Minutes 49 Minutes 49 Minutes 49 Minutes 40 Minutes 41 Minutes 42 Minutes 43 Minutes 44 Minutes 45 Minutes	2 Hours, 30 Minutes 3 Hours 1 Hour 45 Minutes 45 Minutes 45 Minutes 1 Hour 1 Hour 45 Minutes 1 Hour 45 Minutes	3 hours, 24 minutes 59 minutes, 18 seconds 17 minutes, 6 seconds 29 minutes, 46 seconds 15 minutes, 5 seconds 45 minutes, 53 seconds 1 minute, 59 seconds 27 minutes, 58 seconds 35 minutes, 11 seconds 34 minutes, 32 seconds	41 seconds 57 seconds 21 seconds 40 seconds 1 minute, 9 seconds 45 seconds 1 minute, 6 seconds 1 minute, 6 seconds
LNXIO1 - Pipes and Filters LNXIO1 - Setting Up a Firewall With UFW and Firewalld or Uncomplete Reports LNXIO1 - Setting Up a Firewall With UFW and Firewalld or Uncomplete Reports LNXIO1 - Telnet vs. SSH LnxIO1 - Telne	learn how to chain multiple commands together to achieve more learn how to use two common firewall management tools called UTW freewall and firewall. He common firewall management tools called UTW freewall and firewall. He common the common to the common to the common tool tools to use tehest, an insecure protocol that sends its data over memorytate form. It was not to the common to the common to the way to the common to tool go events and analyze system events. We will be able to to log events and analyze system events. We will be able to to log events and analyze system events. It will have the opportunity to review various log files associated with atting system. Upon completing this exercise, the will be able to to log events and analyze system events. Upon the common to the common to log events and analyze system events. Upon the common to log the log the	CYBRScore Labs CYBRScore Labs CYBRScore Scored Labs CYBRScore Scored Labs CYBRScore Scored Labs CYBRScore Scored Labs CYBRScore Labs	Linux System Administration (LSA), Topics: 2, 3, 4, 6, Linux System Administration (LSA), Topics: 2, 3, 4, 6, Linux System Administration (LSA), Topics: 2, 3, 4, 6, Host Forensics (NOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (NOF); Topics: 1, 5, 6, 7, 8, 9, 10 Network Defense (NOF); Topics: 1, 5, 6, 7, 8, 9, 10 Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a	Hyper-V	2 Hours 3 Hours 1 Hour 45 Minutes 45 Minutes 30 Minutes 49 Minutes 49 Minutes 41 Minutes 42 Minutes 43 Minutes 44 Minutes 45 Minutes 46 Minutes 47 Minutes 48 Minutes 49 Minutes 49 Minutes 40 Minutes 40 Minutes 41 Hour	2 Hours, 30 Minutes 3 Hours 1 Hour 45 Minutes 45 Minutes 45 Minutes 1 Hour 45 Minutes 1 Hour 45 Minutes 1 Hour 45 Minutes 1 Hour	3 hours, 24 minutes 59 minutes, 18 seconds 17 minutes, 6 seconds 29 minutes, 6 seconds 15 minutes, 5 seconds 45 minutes, 53 seconds 1 minute, 59 seconds 27 minutes, 58 seconds 35 minutes, 11 seconds 34 minutes, 32 seconds 24 minutes, 32 seconds	41 seconds 57 seconds 21 seconds 40 seconds 1 minute, 9 seconds 45 seconds 1 minute, 6 seconds 1 minute, 6 seconds 1 minute, 19 seconds 1 seconds 1 seconds 1 seconds 1 seconds
LIXX101 - Pipes and Filters LIXX101 - Setting Up a Firewall With UFW and Firewalld or Uncomplicate Roads. LIXX101 - Setting Up a Firewall With UFW and Firewalld or Uncomplicated In the lab, you will be not the Complex Roads. LIXX101 - Telnet vs. SSH In this lab students the Windows opera configure systems to the Windows oper	learn how to chain multiple commands together to achieve more learn how to use two common firevall management tools called UTW firevall and firevall. learn how to use teheet, an insecure protocol that sends its data over unemcrypted form. set will have the opportunity to review various log files associated with atting system. Upon completing this exerctic, the will be able to to log events and analyze system events. will have the opportunity to review various log files associated with atting system. Upon completing this exerctic, the will be able to to log events and analyze system events. plank to ingest server logs and a physical access log to determine if a went has occurred, and if so, who may be behind it. etworked digital systems, attention must be paid to the logging place to detect suspicious behavior. In this lab, students will work correlate server logs, system logs, and application logs in order to acker was successful, and if so what happened and how they got in. correlate server logs, system logs, and application logs to determine in the server logs, short logs, and application logs to order to acker was successful, and if so what happened and how they got in. It as even't logs, short logs, and application logs to order to acker was successful, and if so what happened and how they got in. the server logs, short logs, and application logs to determine in a term than occurred, and if so, who may be behind it. Server logs to create a report. In is als to become familiar with locations of data on a MAC Image.	CYBRScore Labs	Linux System Administration (LSA), Topics: 2, 3, 4, 6, Linux System Administration (LSA), Topics: 2, 3, 4, 6, Linux System Administration (LSA), Topics: 2, 3, 4, 6, Host Forensics (NOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (NOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (NOF); Topics: 1, 5, 6, 7, 8, 9, 10 Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a Host Forensics (NOF), Topics: 1a, 1c, 1d, 2a, 2b, 4a Host Forensics (NOF), Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (NOF), Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (NOF), Topics: 1, 5, 6, 7, 8, 9, 10	Hyper-V	2 Hours 3 Hours 1 Hour 45 Minutes 45 Minutes 30 Minutes 49 Minutes 30 Minutes 49 Minutes 11 Hour 11 Hour 11 Hour	2 Hours, 30 Minutes 3 Hours 1 Hour 45 Minutes 45 Minutes 45 Minutes 1 Hour 45 Minutes 1 Hour 45 Minutes 1 Hour 45 Minutes 1 Hour 46 Minutes 1 Hour 47 Minutes 1 Hour 48 Minutes 1 Hour As Minutes 2 Hours, 30 Minutes 2 Hours	3 hours, 24 minutes 59 minutes, 18 seconds 17 minutes, 6 seconds 29 minutes, 6 seconds 15 minutes, 5 seconds 45 minutes, 53 seconds 1 minutes, 59 seconds 27 minutes, 58 seconds 35 minutes, 11 seconds 34 minutes, 32 seconds 22 minutes, 23 seconds 24 minutes, 25 seconds 25 minutes, 27 seconds 26 minutes, 27 seconds 27 minutes, 28 seconds 28 minutes, 29 seconds 29 minutes, 29 seconds 40 seconds	41 seconds 57 seconds 21 seconds 40 seconds 1 minute, 9 seconds 45 seconds 1 minute, 6 seconds 1 minute, 6 seconds 1 minute, 7 seconds 1 seconds 1 seconds 22 seconds 23 seconds 23 seconds 24 seconds 25 seconds 26 seconds

Manual Vulnerability Assessment	As part of the defense in depth model it is vitally important to keep tabs on the events occurring on individual developystems. In this lab, students will see many be conduct a manual enrice scan to discover any networked devices as well as the services those devices are running. Next, they will log in the services of the devices are running. Next, they will log in the Next Next Next Section to the services and the neable the intra Next Next Next Section to the services and then enable the	CYBRScore Labs	Operating Systems Hardening (OSH), Topics: 11; IT Systems Components (ISC), Topics: 13	Hyper-V	1 Hour	1 Hour	33 minutes, 33 seconds	34 seconds
	auditing of attempts (successes/failures) to use a specific program (Splunk). Finally, the students will validate that the new audit objects are successfully working by reviewing the Event Log for the Windows workstation host.							
	As part of the defense in depth model it is vitally important to keep tabs on the events occurring on individual devices/systems.							
Manual Vulnerability Assessment	In this lab, students will use mage to conduct a manual service scan to discover any networked devices as well as the services those devices are running. Rext, they will log into a Windows workstation to set up auditing for system services, and then enable the auditing of attempts (successes/failure) to use a specific program (Splunk). Finally, the students will willdate that the new audit objects are successfully working by reviewing the Event Ligo for the Windows workstation host.	CYBRScore Scored Labs	Operating Systems Hardening (OSH), Topics: 11; IT Systems Components (ISC), Topics: 13	Hyper-V	1 Hour	1 Hour	36 minutes, 3 seconds	1 minute, 16 seconds
Manually Analyze Malicious PDF Documents	Several company employees have received unsolicited emails with suspicious pdf attachments. The CIO has asked you to look at the attachments and see if they are malicious.	CYBRScore Labs	Software Security Analysis (SSA); Topics: 1, 2, 3, 4, 5	Hyper-V	1 Hour	1 Hour	33 minutes, 38 seconds	19 seconds
Manually Analyze Malicious PDF Documents	Several company employees have received unsolicited emails with suspicious pdf attachments. The CIO has asked you to look at the attachments and see if they are malicious	CYBRScore Scored Labs	Software Security Analysis (SSA); Topics: 1, 2, 3, 4, 5	Hyper-V	1 Hour	1 Hour	35 minutes, 35 seconds	1 minute, 16 seconds
Manually Analyze Malicious PDF Documents 2	Several company employees have received unsolicited emails with suspicious pdf attachments. The CIO has asked you to look at the attachments and see if they are malicious.	CYBRScore Labs	Software Security Analysis (SSA); Topics: 1, 2, 3, 4, 5	Hyper-V	1 Hour, 30 Minutes	1 Hour, 30 Minutes		
Manually Analyze Malicious PDF Documents 2	Several company employees have received unsolicited emails with suspicious pdf attachments. The CIO has asked you to look at the attachments and see if they are malicious.	CYBRScore Scored Labs	Software Security Analysis (SSA); Topics: 1, 2, 3, 4, 5	Hyper-V	1 Hour, 30 Minutes	1 Hour, 30 Minutes	38 minutes, 48 seconds	1 minute, 5 seconds
Manually Creating a Baseline with MD5Deep	Students will create a baseline on a documents folder using md5deep. Students will ther modify the folder and observe the changes made to that folder.		Operating Systems Hardening (OSH); Topics: 1, 2, 3, 4, 5, 6, 7, 8, 10, 11	Hyper-V	1 Hour	1 Hour	19 minutes, 53 seconds	25 seconds
Manually Creating a Baseline with MD5Deep	Students will create a baseline on a documents folder using md5deep. Students will ther modify the folder and observe the changes made to that folder.		Operating Systems Hardening (OSH); Topics: 1, 2, 3, 4, 5, 6, 7, 8, 10, 11	Hyper-V	1 Hour	1 Hour	8 minutes, 32 seconds	1 minute, 16 seconds
Memory Extraction and Analysis	This is one of the labs for the Advanced Digital Media Forensics class.	CYBRScore Labs	Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10	Hyper-V	3 Hours, 40 Minutes	7 Hours, 20 Minutes		1 minute, 29 seconds
Memory Extraction and Analysis Metadata Extraction Lab	This is one of the labs for the Advanced Digital Media Forensics class. In this lab, students will understand what Metadata is and learn a tool to use to identify	CYBRScore Scored Labs	Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10 Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10	Hyper-V Hyper-V	45 Minutes 1 Hour	1 Hour 1 Hour, 30 Minutes	35 minutes, 50 seconds	1 minute, 25 seconds
	it.					,		
Metadata Extraction Lab	it	CYBRScore Labs	Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10	Hyper-V	1 Hour	1 Hour, 30 Minutes	21 minutes, 20 seconds	1 minute, 40 seconds
Metadata Extraction Lab	In this lab, students will understand what Metadata is and learn a tool to use to identify it.	CYBRScore Scored Labs	Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10	Hyper-V	1 Hour	1 Hour, 30 Minutes	6 minutes, 21 seconds	1 minute
Microsoft Baseline Security Analyzer	In this lab you will use Microsoft Baseline Security Analyzer (MBSA) to perform scans of individual host computers and of groups of computers. You will also learn how to perform the most common scans using command line tools. Once completed, you will have learned how to use MBSA to perform a comprehensive security analysis of your network environment.	CYBRScore Labs	Software Security Analysis (SSA); Topics: 1, 2, 3, 4, 5	Hyper-V	1 Hour	1 Hour	35 minutes, 6 seconds	20 seconds
Microsoft Baseline Security Analyzer	In this lab you will use Microsoft Baseline Security Analyzer (MBSA) to perform scans of individual host computers and of groups of computers. You will also learn how to perform the most common scans using command line tools. Once completed, you will have learned how to use MBSA to perform a comprehensive security analysis of your network environment.	CYBRScore Scored Labs	Software Security Analysis (SSA); Topics: 1, 2, 3, 4, 5	Hyper-V	1 Hour	1 Hour	27 minutes, 5 seconds	1 minute, 17 seconds
Monitoring and Verifying Management Systems	Students will analyze a MBSA Baseline report and compare it to current system configurations. Students will then make necessary system changes to machines and validate baseline using MBSA. Students will finally compare hash values to determine if	CYBRScore Labs	Operating Systems Hardening (OSH); Topics: 1, 2, 3, 4, 5, 6, 7, 8, 10, 11	Hyper-V	1 Hour	1 Hour	11 minutes, 53 seconds	26 seconds
·	any changes have been made to a system.							
Monitoring and Verifying Management Systems	any changes have been made to a system. Students will analyze a MBSA Baseline report and compare it to current system configurations. Students will then make necessary system changes to machines and validate baseline using MBSA. Students will finally compare hash values to determine if any changes have been made to a system.	CYBRScore Scored Labs	Operating Systems Hardening (OSH); Topics: 1, 2, 3, 4, 5, 6, 7, 8, 10, 11	Hyper-V	1 Hour	1 Hour	13 minutes, 9 seconds	1 minute, 25 seconds
	any changes have been made to a system. Students will analyze a MSA Baseline report and compare it to current system configurations. Students will then make necessary system changes to machines and validate baseline using MSAS. Students will finally compare hash values to determine if any changes have been made to a system. In this lab we will map a drive to a share on the network and then copy resources from a file senere.	CYBRScore Labs	Operating Systems Hardening (OSH); Topics: 1, 2, 3, 4, 5, 6, 7, 8, 10, 11 Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a	Hyper-V	1 Hour	1 Hour	13 minutes, 9 seconds 16 minutes, 23 seconds	1 minute, 25 seconds 32 seconds
Monitoring and Verifying Management Systems	any changes have been made to a system. Students will analyze a MSSA Baseline report and compare it to current system confligurations. Students will analyze a MSSA Baseline report and compare to concept the conflict and will dark baseline using MSSA. Students will finally compare hash values to determine if any changes have been made to a system. In this lab we will map a drive to a share on the network and then copy resources from a file server. In this lab we will map a drive to a share on the network and then copy resources from a file server.	CYBRScore Labs						
Monitoring and Verifying Management Systems Monitoring for False Positives	any changes have been made to a system. Students will analyze a MSSA Baseline report and compare it to current system confligurations. Students will analyze a MSSA Baseline report and compare it to current system confligurations. Students will then make necessary system changes to machines and validate baseline using MSSAS. Students will finally compare hash values to determine if any changes have been made to a system. In this is able well map a drive to a share on the network and then copy resources from a file server. In this is able well imap a drive to a share on the network and then copy resources from a file server.	CYBRScore Labs CYBRScore Labs	Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a	Hyper-V	1 Hour	1 Hour	16 minutes, 23 seconds	32 seconds
Monitoring and Verifying Management Systems Monitoring for False Positives Monitoring for False Positives	any changes have been made to a system. Students will analyze a MSSA Baseline report and compare it to current system configurations. Students will then make necessary system changes to machines and validate baseline using MSSA. Students will finally compare hash values to determine if any changes have been made to a system. In this lab we will map a drive to a share on the network and then copy resources from a lin this dib we will map a drive to a share on the network and then copy resources from a list ship we will map a drive to a share on the network and then copy resources from a list ship we will map a drive to a share on the network and then copy resources from a list ship we will map a drive to a share on the network and then copy resources from a list server.	CYBRScore Labs CYBRScore Labs	Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a	Hyper-V Hyper-V	1 Hour	1 Hour	16 minutes, 23 seconds 48 seconds	32 seconds 23 seconds
Monitoring and Verifying Management Systems Monitoring for False Positives Monitoring for False Positives Monitoring for False Positives Monitoring for False Positives	any changes have been made to a system. Students will analyze a MBSA Baseline report and compare it to current system confligurations. Students will analyze a MBSA Baseline report and compare has have been made to a system. In this lab we will map a drive to a share on the network and then copy resources from a file server. In this lab we will map a drive to a share on the network and then copy resources from a file server. In this lab we will map a drive to a share on the network and then copy resources from a file server. In this lab we will map a drive to a share on the network and then copy resources from a file server. In this lab we will map a drive to a share on the network and then copy resources from a file server. In this lab we will map a drive to a share on the network and then copy resources from a file server. In this lab we will replicate potentially malicious scans from the Internet against a corporate asset. Scans from the Internet are very common. An analyst should know how doeffility file activity by artifacts that are present in the file sew lide in the file them.	CYBRScore Labs CYBRScore Labs CYBRScore Scored Labs	Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a	Hyper-V Hyper-V Hyper-V	1 Hour 1 Hour 1 Hour	1 Hour 1 Hour 1 Hour	16 minutes, 23 seconds 48 seconds 14 minutes, 42 seconds	32 seconds 23 seconds 1 minute, 28 seconds
Monitoring and Verifying Management Systems Monitoring for False Positives Monitoring for False Positives Monitoring for False Positives Monitoring for False Positives Monitoring Network Traffic	any changes have been made to a system. Students will analyze a MISSA Baseline report and compare it to current system configurations. Students will maligine a MISSA Baseline report and compare it to current system configurations. Students will finally compare have found to determine if any changes have been made to a system. In this lab we will map a drive to a share on the network and then copy resources from a file server. In this lab we will map a drive to a share on the network and then copy resources from a file server. In this lab we will map a drive to a share on the network and then copy resources from a file server. In this lab we will replicate potentially malicious scans from the internet against a corporate asset. Scans from the internet are very common, the analyst should know how to defently this activity by artifacts that are present in the ISS a well as entries in the wall form that the student is a second to the secon	CYBRScore Labs CYBRScore Labs CYBRScore Scored Labs CYBRScore Network Forensics	Network Defense (NDF), Topica: 1a, 1c, 1d, 2a, 2b, 4a Network Defense (NDF), Topica: 1a, 1c, 1d, 2a, 2b, 4a Network Defense (NDF), Topica: 1a, 1c, 1d, 2a, 2b, 4a Network Defense (NDF), Topica: 1a, 1c, 1d, 2a, 2b, 4a	Hyper-V Hyper-V Hyper-V	1 Hour 1 Hour 1 Hour 1 Hour	1 Hour 1 Hour 1 Hour 1 Hour	16 minutes, 23 seconds 48 seconds 14 minutes, 42 seconds 26 minutes, 40 seconds	32 seconds 23 seconds 1 minute, 28 seconds 1 minute, 35 seconds
Monitoring and Verifying Management Systems Monitoring for False Positives Monitoring for False Positives Monitoring for False Positives Monitoring for False Positives Monitoring Network Traffic Monitoring Network Traffic	any changes have been made to a system. Students will analyze a MISSA Baseline report and compare it to current system configurations. Students will malize a MISSA Baseline report and compare it to current system configurations. Students will finally compare have found to determine if any changes have been made to a system. In this lab we will map a drive to a share on the network and then copy resources from a file server. In this lab we will map a drive to a share on the network and then copy resources from a file server. In this lab we will map a drive to a share on the network and then copy resources from a file server. In this lab we will replicate potentially malicious scans from the internet against a corporate asset. Scans from the internet are very common, ha malpst should know how to identify this activity by artifacts that are present in the ISs avel as entiries in the well loss. In this lab we will replicate potentially malicious scans from the internet against a mission of the server of the	CYBRScore Labs CYBRScore Labs CYBRScore Network Forensics CYBRScore Network Forensics CYBRScore Labs CYBRScore Labs	Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a	Hyper-V Hyper-V Hyper-V Hyper-V	1 Hour 1 Hour 1 Hour 1 Hour	1 Hour 1 Hour 1 Hour 1 Hour	16 minutes, 23 seconds 48 seconds 14 minutes, 42 seconds 26 minutes, 40 seconds 40 minutes, 10 seconds	32 seconds 23 seconds 2 minute, 28 seconds 2 minute, 35 seconds 33 seconds
Monitoring and Verifying Management Systems Monitoring for False Positives Monitoring for False Positives Monitoring for False Positives Monitoring Network Traffic Monitoring Network Traffic Monitoring Network Traffic	any changes have been made to a system. Students will analyze a MISSA Baseline report and compare it to current system configurations. Students will majeve a MISSA Baseline report and compare it to current system configurations. Students will finally compare have have been made to a system. In this lab we will map a drive to a share on the network and then copy resources from a file server. In this lab we will map a drive to a share on the network and then copy resources from a file server. In this lab we will map a drive to a share on the network and then copy resources from a file server. In this lab we will map a drive to a share on the network and then copy resources from a file server. In this lab we will replicate potentially malicious scans from the internet against a corporate asset. Scans from the internet are very common. An analyst should know how to identify this activity by artifacts that are present in the ISs a well as entries in the web loss. In this lab we will replicate potentially malicious scans from the internet against a corporate asset. Scans from the internet are very common. An analyst should know how to learnify this activity by artifacts that are present in the ISs a well as entries in the web loss. In this lab we will replicate potentially malicious scans from the internet against a corporate asset. Scans from the internet are very common. An analyst should know how to defirify this activity by artifacts that are present in the ISS as well as entries in the web logs. In this lab we will replicate potentially malicious scans from the internet against a corporate asset. Scans from the internet are very common, an analyst should know how to identify this activity by artifacts that are present in the ISS as well as entries in the web logs.	CYBRScore Labs CYBRScore Labs CYBRScore Network Forensics CYBRScore Network Forensics CYBRScore Labs CYBRScore Labs	Network Defense (NDF), Topica: 1a, 1c, 1d, 2a, 2b, 4a Network Defense (NDF), Topica: 1a, 1c, 1d, 2a, 2b, 4a Network Defense (NDF), Topica: 1a, 1c, 1d, 2a, 2b, 4a Network Defense (NDF), Topica: 1a, 1c, 1d, 2a, 2b, 4a Network Defense (NDF), Topica: 1a, 1c, 1d, 2a, 2b, 4a Network Defense (NDF), Topica: 1a, 1c, 1d, 2a, 2b, 4a	Hyper-V Hyper-V Hyper-V Hyper-V Hyper-V	1 Hour 1 Hour 1 Hour 1 Hour 1 Hour	1 Hour 1 Hour 1 Hour 1 Hour 1 Hour	16 minutes, 23 seconds 48 seconds 14 minutes, 42 seconds 26 minutes, 40 seconds 40 minutes, 10 seconds	32 seconds 23 seconds 2 minute, 28 seconds 2 minute, 35 seconds 33 seconds
Monitoring and Verifying Management Systems Monitoring for False Positives Monitoring for False Positives Monitoring for False Positives Monitoring Network Traffic	any changes have been made to a system. Students will analyze a MISSA Baseline report and compare it to current system configurations. Students will insighe a MISSA Baseline report and compare it to current system configurations. Students will finally compare hash values to determine if any changes have been made to a system. In this lab we will map a drive to a share on the network and then copy resources from a line share will be a share on the network and then copy resources from a line server. In this lab we will map a drive to a share on the network and then copy resources from a line server. In this lab we will map a drive to a share on the network and then copy resources from a line server. In this lab we will replicate potentially malicious scans from the internet against a corporate asset. Scans from the internet are very common. An analyst should know how to identify this activity by artifacts that are present in the IDS as well as entries in the well loss. In this lab we will replicate potentially malicious scans from the internet against a corporate asset. Scans from the internet are very common. An analyst should know how to identify this activity by artifacts that are present in the IDS as well as entries in the well loss. Well loss. In this lab we will replicate potentially malicious scans from the internet against a corporate asset. Scans from the internet are very common. An analyst should know how to identify this activity by artifacts that are present in the IDS as well as entries in the well loss. In this lab we will replicate potentially malicious scans from the internet against a corporate asset. Scans from the internet are very common, and an analyst should know how to identify this activity by artifacts that are present in the IDS as well as entries in the well loss. In this lab we will replicate potentially malicious scans from the internet against a corporate asset. Scans from the internet are very common, and an analyst should know how to identify this activity by artifacts t	CYBRScore Labs CYBRScore Labs CYBRScore Network Forensics CYBRScore Network Forensics CYBRScore Labs CYBRScore Labs CYBRScore Scored Labs	Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a	Hyper-V Hyper-V Hyper-V Hyper-V Hyper-V Hyper-V	1 Hour 1 Hour 1 Hour 1 Hour 1 Hour	1 Hour 1 Hour 1 Hour 1 Hour 1 Hour 1 Hour	16 minutes, 23 seconds 48 seconds 14 minutes, 42 seconds 26 minutes, 40 seconds 40 minutes, 10 seconds 36 minutes, 30 seconds	23 seconds 23 seconds 1 minute, 28 seconds 1 minute, 35 seconds 33 seconds 53 seconds
Monitoring and Verifying Management Systems Monitoring for False Positives Monitoring for False Positives Monitoring for False Positives Monitoring Network Traffic Monitoring Network Traffic Monitoring Network Traffic Monitoring Network Traffic Monitoring Network Traffic (Troubleshooting)	any changes have been made to a system. Students will analyze a MISSA Baseline report and compare it to current system configurations. Students will make a MISSA Baseline report and compare it to current system configurations. Students will will have been made to a system. In this lab we will map a drive to a share on the network and then copy resources from a line in the lab was shared to a system. In this lab we will map a drive to a share on the network and then copy resources from a life server. In this lab we will map a drive to a share on the network and then copy resources from a life server. In this lab we will map a drive to a share on the network and then copy resources from a life server. In this lab we will map a drive to a share on the network and then copy resources from a life server. In this lab we will replicate potentially malicious scans from the internet against a corporate asset. Scans from the internet are very common. An analyst should know how to identify this activity by artifacts that are present in the IDS as well as entries in the well loss. In this lab we will replicate potentially malicious scans from the internet against a corporate asset. Scans from the internet are very common. An analyst should know how to identify this activity by artifacts that are present in the IDS as well as entries in the well loss. In this lab we will replicate potentially malicious scans from the internet against a corporate asset. Scans from the internet are very common. An analyst should know how to identify this activity by artifacts that are present in the IDS as well as entries in the well loss. In this lab we will replicate potentially malicious scans from the internet against a corporate asset. Scans from the internet are very common, and an analyst should know how to identify this activity by artifacts that are present in the IDS as well as entries in the well loss. In this lab we will replicate potentially malicious scans from the internet against a corporate asset. Scans from the inte	CYBRScore Labs CYBRScore Labs CYBRScore Network Forensics CYBRScore Network Forensics CYBRScore Labs CYBRScore Scored Labs CYBRScore Scored Labs CYBRScore Scored Labs	Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a	Hyper-V Hyper-V Hyper-V Hyper-V Hyper-V Hyper-V Hyper-V	1 Hour 1 Hour 1 Hour 1 Hour 1 Hour 1 Hour	1 Hour	16 minutes, 23 seconds 48 seconds 14 minutes, 42 seconds 26 minutes, 40 seconds 40 minutes, 10 seconds 36 minutes, 30 seconds	23 seconds 23 seconds 2 minute, 28 seconds 1 minute, 25 seconds 3 seconds 33 seconds 53 seconds 1 minute, 27 seconds
Monitoring and Verifying Management Systems Monitoring for False Positives Monitoring for False Positives Monitoring Network Traffic Monitoring Network Traffic Monitoring Network Traffic Monitoring Network Traffic (Troubleshooting) Monitoring Network Traffic (Troubleshooting)	any changes have been made to a system. Students will analyze a MISSA Baseline report and compare it to current system configurations. Students will malize a MISSA Baseline report and compare it to current system configurations. Students will finally compare hash values to determine if any changes have been made to a system. In this lab we will map a drive to a share on the network and then copy resources from a file server. In this lab we will map a drive to a share on the network and then copy resources from a file server. In this lab we will map a drive to a share on the network and then copy resources from a file server. In this lab we will map a drive to a share on the network and then copy resources from a file server. In this lab we will replicate potentially malicious scans from the internet against a corporate asset. Scans from the internet are very common, an analyst should know how to dentify this activity by artifacts that are present in the IDS as well as entries in the web loss. In this lab we will replicate potentially malicious scans from the internet against a corporate asset. Scans from the internet are very common. An analyst should know how to dentify this activity by artifacts that are present in the IDS as well as entries in the web loss. In this lab we will replicate potentially malicious scans from the internet against a corporate asset. Scans from the internet are very common, An analyst should know how to identify this activity by artifacts that are present in the IDS as well as entries in the web logs. In this lab we will replicate potentially malicious scans from the internet against a corporate asset. Scans from the internet are very common, and an analyst should know how to identify this activity by artifacts that are present in the IDS as well as entries in the web logs. In this lab we will replicate potentially malicious scans from the internet against a corporate asset. Scans from the internet are very common, and an analyst should know how to identify this activity by	CYBRScore Labs CYBRScore Labs CYBRScore Network Forensics CYBRScore Scored Labs CYBRScore Scored Labs	Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a	Hyper-V Hyper-V Hyper-V Hyper-V Hyper-V Hyper-V Hyper-V Hyper-V	1 Hour 1 Hour 1 Hour 1 Hour 1 Hour 1 Hour	1 Hour	16 minutes, 23 seconds 48 seconds 14 minutes, 42 seconds 26 minutes, 40 seconds 40 minutes, 10 seconds 36 minutes, 30 seconds 47 minutes, 36 seconds	23 seconds 23 seconds 1 minute, 28 seconds 1 minute, 35 seconds 33 seconds 33 seconds 1 minute, 27 seconds

Part									
Manufactions	Nessus Scanning and Reporting	Vulnerability Scanner. Trainees will modify scan settings to perform different types of scans and to learn about the different functionalities Nessus provides. Trainees will the compare the results of a Nessus scan against the results of a NMAP scan against the samt target and discuss the differences and similarities between the two tools. Lastly, trainees	e cronocore cuos	Operating Systems Hardening (OSH), Topics: 11; IT Systems Components (ISC), Topics: 13	Hyper-V	3 Hours	4 Hours	40 minutes, 36 seconds	41 seconds
Note Proceedings Note Procedure	Nessus Setup and Config	This exercise will familiarize trainees with the Nessus Vulnerability Scanning tool. Trainees will be able to install and configure Nessus after completing this exercise.	CYBRScore Labs	Operating Systems Hardening (OSH), Topics: 11; IT Systems Components (ISC), Topics: 13	Hyper-V	3 Hours	4 Hours	24 minutes, 51 seconds	40 seconds
State Stat	Network Discovery		CYBRScore Labs	Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a	Hyper-V	1 Hour, 30 Minutes	1 Hour, 30 Minutes	19 minutes, 13 seconds	59 seconds
March Marc	Network Discovery		CYBRScore Scored Labs	Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a	Hyper-V	1 Hour, 30 Minutes	1 Hour, 30 Minutes	30 minutes, 11 seconds	46 seconds
March Marc	Network Forensics Lab Book Environment	Students will develop an understanding of the Network Forensics through a series of	CYBRScore Network Forensics	Network Forensics; Topics: 1, 2, 6	Hyper-V	40 Hours	40 Hours	2 hours, 21 minutes	34 seconds
March Marc	Network Forensics Lab Book Environment	Students will develop an understanding of the Network Forensics through a series of	CYBRScore Labs	Network Forensics; Topics: 1, 2, 6	Hyper-V	40 Hours	40 Hours	12 minutes, 49 seconds	43 seconds
Part	Network Miner	This lab exercise is designed to allow the trainee to become familiar with using Network	CYBRScore Labs	Network Defense (NDE) Tonics: 1a 1c 1d 2a 2b 4a	vSphere	1 Hour	1 Hour		
Company Comp	Notwork Minor	This lab exercise is designed to allow the trainee to become familiar with using Network	CVPRScore Scored Labo		uSahara	20 Minutes	1 Hour	20 minutes 18 coconds	20 cocondo
March Marc		Miner.						20 minutes, 10 seconds	zo seconos
March Marc		Miner.							
March Marc	Network Segmentation (FW/DMZ/WAN/LAN)	access to the appropriate IP address.	CYBRScore Labs	Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a	Hyper-V	1 Hour	1 Hour, 30 Minutes	34 minutes, 26 seconds	59 seconds
Comment Comm	Network Segmentation (FW/DMZ/WAN/LAN)	Create three distinct areas for this network, route traffic accordingly and lock down VPN access to the appropriate IP address.			Hyper-V				,
Part	Network Topology Generation	Students will utilize Zenmap to generate a visual network topology.		Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a					
March Control Contro									
Manual Column Manual Colum	Network ropology deneration	In this lab the student will kill some processes and close down some shares in processes	CT PROCOSE OCOSEG LADS	Network Deterise (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a	nyper-V	1 HOUI	1 mout	40 minutes, 8 seconds	1 minute, 19 seconds
para medical from the Windows 2 processed of the particular and marked and the particular and marked and particular and particular and marked and pa	Open and Close Ports on Windows 7	to a suspected threat. Student will then determine the potential adverse effects to the network based on service requirements.	CYBRScore Labs	Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a	Hyper-V	1 Hour	1 Hour	23 minutes, 47 seconds	22 seconds
service Column by the service Column by the service of the column by the s	Open and Close Ports on Windows 7	to a suspected threat. Student will then determine the potential adverse effects to the	CYBRScore Scored Labs	Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a	Hyper-V	1 Hour	1 Hour	23 minutes, 17 seconds	21 seconds
see found found for the found of the found o	Open Source Collection	functionality of Google, default webpages used for web-servers, and the specifics of Google Hacking database. This allows the students to understand how open source	CYBRScore Labs	Network Defense (NDF), Topics: 1a, 1c, 1d, 2b, 4a	Hyper-V	2 Hours	2 Hours	48 minutes, 10 seconds	38 seconds
Section of Parlice of Carding Section of the law and the law payer and can see that the support and can see that the support and can see the law to approximate the payer and can see the law to approximate the payer and can see the law to approximate the payer and can see the law to approximate the payer and can see the law to approximate the payer and can see the law to approximate the law to the law to the law to approximate the law to t	Open Source Collection	functionality of Google, default webpages used for web-servers, and the specifics of Google Hacking database. This allows the students to understand how open source	CYBRScore Scored Labs	Network Defense (NDF). Topics: 1a, 1c, 1d, 2b, 4a	Hyper-V	2 Hours	2 Hours	24 minutes, 39 seconds	1 minute, 10 seconds
Part County Cou	Open Source Password Cracking	Students will use John the Ripper and Cain and Abel to crack password protected files	CYBRScore Digital Media Forensics	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10	Hyper-V	2 Hours	4 Hours	42 seconds	18 seconds
March Section Sectio	Open Source Password Cracking	Students will use John the Ripper and Cain and Abel to crack password protected files	CYBRScore Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10	Hyper-V	2 Hours	4 Hours	38 minutes, 17 seconds	34 seconds
where the finance of tables of tenders of tables of tabl	Open Source Password Cracking	Students will use John the Ripper and Cain and Abel to crack password protected files	CYBRScore Scored Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10	Hyper-V	1 Hour	2 Hours	29 minutes, 35 seconds	1 minute, 6 seconds
where the finance of tables of tenders of tables of tabl	•	Students will become familiarized with data visualization using Kihana - one of the 3 toology		3. , , , , , , , , , , , , , , , , , , ,					
Make the make the count of fetherwish Table and the count of precision of the count	Overview of Kibana	included in Elastic's ELK stack, a trio of open-source applications that work together in order to meet a myriad of different monitoring and analytics needs.	CYBRScore Labs	Network Security Administration (NSA); Topics: 2, 5, 7, 8, 9, 10	Hyper-V	1 Hour	1 Hour	53 minutes, 58 seconds	1 minute, 19 seconds
Atter and Windows Frame and Wi	PAM Lab	SSH to create a user account and assign the user account permissions on the virtual machine.		Operating Systems Administration (OSA); Topics: 2, 4, 5, 6, 9, 11	vSphere	1 Hour	1 Hour	10 minutes, 25 seconds	30 seconds
This Date has been facilities with the feed of the Network Traffic This Date has been facilities from record buttering from the Network Traffic This Date has been facilities from record buttering from the Network Traffic The Confidence of Traffic The Confidenc	Parse Files Out of Network Traffic		CYBRScore Network Forensics	Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a	Hyper-V	1 Hour	1 Hour	18 minutes, 20 seconds	24 seconds
This list best his businesh bow to careful widnesh businesh bow to a careful widnesh businesh bow to a careful widnesh businesh b	Parse Files Out of Network Traffic		CYBRScore Labs	Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a	Hyper-V	1 Hour	1 Hour	26 minutes, 32 seconds	19 seconds
State and Wine-bis. State and	Parse Files Out of Network Traffic	This lab teach students how to extract various files from network traffic using Network	CYBRScore Scored Labs	Network Defence (NDE) Tonics: 1a 1c 1d 2a 2h 4a	Hyner-V	1 Hour	1 Hour	24 minutes 4 seconds	1 minute 9 seconds
Suderity will participate in attack analysis Using Trusted Tool Set determination, clearly interesting explositive process and methods used determination, to desting historicalise specified viscority participate and cornelize system of the process of the proce	Participate in Attack Analysis Using Trusted Tool Set	Students will participate in attack analysis/incident response, including root cause determination, to identify vulnerabilities exploited, vector/source and methods used (e.g., malware, denial of service). Students will then investigate and correlate system logs to identify missing patches, level of access obtained, unauthorized processes or	CYBRScore Labs	Network Security Administration (NSA); Topics: 2, 5, 7, 8, 9, 10	Hyper-V	38 Minutes	1 Hour	1 minute, 19 seconds	18 seconds
Session of Lacking with PRTK In this lab, Students will almost our seckes Data's Password Recovery Toolkit (PRTS) to crack various types of passwords. In this lab, Students will almost our seckes Data's Password Recovery Toolkit (PRTS) to crack various types of passwords. In this lab, Students will almost our seckes Data's Password Recovery Toolkit (PRTS) to crack various types of passwords. In this lab, Students will almost our seckes Data's Password Recovery Toolkit (PRTS) to crack various types of passwords. Students will installation and Validation Testing Students will installation and Validation Testing Students will installation and Validation Testing Students will installate the where ability, in necessary. In this lab, the student will pass that year or noning Windows Systems and then nove to remediate the whereability, in necessary. In this lab, the student will pass that year or noning Windows XP. The student will install almost a service Pass 2 exploits. This password Canceling With WSUS Students will have access to a Windows 2012 Sever running Windows XP. The student will install a service Pass 2 exploits. They will be students will installate the whereability, in necessary. They will see that the password that the students of the password Recovery Toolkit will be a service Pass 2 exploits. This password Canceling With WSUS Students will have access to a Windows 2012 Sever running Windows XP. The student will install a service Pass 2 exploits. They will be a service Pass 2 exploits. They will see that the password that the sect and approve pathies received for Windows Y expert running with will be used Mincrosoft Baseline Security Analyzer (MISA) and the Open Vulnerability Assessment System (Open VAIS.) and use it to select and approve pathies receive (PSUS), and use it to select and approve pathies receive for System Administration (WSA), Topics: 12 Windows System Administration (WSA), Topics: 5: Opensing System Hardening (OSH), Topics: 12 Windows System Administration (WSA), Topics: 5: Opensing	Participate in Attack Analysis Using Trusted Tool Set	Students will participate in attack analysis/incident response, including root cause determination, to identify vulnerabilities exploited, vector/source and methods used (e.g., malware, denial of service). Students will then investigate and correlate system logs to identify missing patches, level of access obtained, unauthorized processes or programs.	CYBRScore Scored Labs	Network Security Administration (NSA): Topics: 2, 5, 7, 8, 9, 10	Hyper-V	30 Minutes	1 Hour	7 minutes, 22 seconds	1 minute, 23 seconds
In this labs, butdents will learn how to use Access Data's Password Recovery Toolk? PRTS to crack visuously spee of passwords. In this labs, butdents will learn how to use Access Data's Password Recovery Toolk? PRTS to crack visuously spee of passwords. PRTS to crack visuously speed of passwords. PRTS to crack visuously	Password Cracking with PRTK	In this lab, students will learn how to use Access Data's Password Recovery ToolKit (PRTK) to crack various types of passwords.	CYBRScore Digital Media Forensics	Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10	Hyper-V	1 Hour, 30 Minutes	2 Hours		
In this labs, students will learn how to use Access Data's Password Recovery Toolkit (PRT) to crack kinding types of password by the password	Password Cracking with PRTK	In this lab, students will learn how to use Access Data's Password Recovery ToolKit	CYBRScore Labs	Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10	Hyper-V	1 Hour, 30 Minutes	2 Hours	18 minutes, 56 seconds	1 minute, 15 seconds
### PRTS to cance various types of passwords. PRTS to cance various types of passwords. PRTS to cance various types of passwords. Sudents will identify if a valuerability is present on two Windows systems and then move to remediate the valuerability. If a valuerability is present on two Windows systems and then move to remediate the valuerability. If a valuerability is present on two Windows systems and then move to remediate the valuerability. If a valuerability is present on two Windows systems and then move to remediate the valuerability. If a valuerability is present on two Windows systems and then move to remediate the valuerability. If a valuerability is present on two Windows systems and then move to remediate the valuerability. If necessary.	Password Cracking with PRTK	In this lab, students will learn how to use Access Data's Password Recovery ToolKit	CYBRScore Scored Labs	Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10	Hyper-V	1 Hour, 30 Minutes	2 Hours	37 minutes, 21 seconds	1 minute, 13 seconds
Students will flame access to a Windows XP Service Pack 3 It is no longer vulnerability. Appreciate and Updates atching With WSUS Students will have access to a Windows XP Service Pack 3 It is no longer vulnerability. Appreciate and updates To Systems Components (ISC), Topics: 12, Windows System Administration (WSA), Topics: 5: Operating System Hardening (OSH), Topics: 9: Whyper-V To Windows XP Service Pack 3 It is no longer vulnerability. Appreciate and approve patches and updates To Systems Components (ISC), Topics: 12, Windows System Administration (WSA), Topics: 5: Operating System Hardening (OSH), Topics: 9: Whyper-V To Windows XP Service Pack 3 It is no longer vulnerability as precise and approve patches because on express provided on reports provided and provided access to a Windows 2012 Server running the Windows Server Update Service (WSUS), and use it to select and approve patches needed for a Windows 2012 Server running the Windows Server Update Service (WSUS), and use it to select and approve patches needed for a Windows 2012 Server running the Windows Server Update Service (WSUS), and use it to select and approve patches needed for a Windows 2012 Server running the Windows Server Update Service (WSUS), and use it to select and approve patches needed for a Windows 2012 Server running the Windows Server Update Service (WSUS), and use it to select and approve patches needed for a Windows 2012 Server running the Windows Server Update Service (WSUS), and use it to select and approve patc	Patch Installation and Validation Testing	Students will identify if a vulnerability is present on two Windows systems and then	CYBRScore Labs	IT Systems Components (ISC), Topics: 12; Windows System Administration (WSA), Topics: 5;	Hyper-V	1 Hour, 30 Minutes	1 Hour, 30 Minutes	1 minute, 43 seconds	23 seconds
move to remediate the vulnerability, if necessary. In this lab, the student will patch a system running Windows XP. The student will install sevice Patch 2 exploits. Students will have access to a Windows 22 Service Patch 2 exploits. Students will have access to a Windows 22 Service Patch 2 exploits. Students will have access to a Windows 22 Service Patch 2 exploits. Students will have access to a Windows 22 Service Patch 2 exploits. Students will have access to a Windows 22 Service Patch 2 exploits. They will select the required pottless based on reports provided not negrots provided and reports provided reports provided and provide scenning activity performed with the use of Microsoft Baseline Security Analyzer (MBSA) and the Operating System Hardening (OSH), Topics: 12 Windows System Administration (WSA), Topics: 5: Operating System Hardening (OSH), Topics: 9 ###PEFV I Hour, 30 Minutes 1 Hour 2 Diminutes, 5 seconds 22 seconds 23 seconds VRBSCore Labs Operating System Hardening (OSH), Topics: 12 Windows System Administration (WSA), Topics: 5: Operating System Hardening (OSH), Topics: 9 ####PEFV I Hour, 30 Minutes 1 Hour 2 Diminutes, 42 minutes, 42 minutes, 42 minutes, 43 seconds 30 seconds Operating System Hardening (OSH), Topics: 12 Windows System Administration (WSA), Topics: 5: Operating System Hardening (OSH), Topics: 12 Windows System Administration (WSA), Topics: 5: Operating System Hardening (OSH), Topics: 12 Windows System Administration (WSA), Topics: 5: Operating System Hardening (OSH), Topics: 12 Windows System Administration (WSA), Topics: 5: Operating System Hardening (OSH), Topics: 12 Windows System Administration (WSA), Topics: 5: Operating System Hardening (OSH), Topics: 12 Windows System Administration (WSA), Topics: 5: Operating System Hardening OSH), Topics: 12 Windows System Administration (WSA), Topics: 5: Operating System Hardening OSH), Topics: 12 Windows System Administration (WSA), Topics: 5: Operating System Hardening OSH), Topics: 12 Windows System Admin				IT Systems Components (ISC), Topics: 12; Windows System Administration (WSA), Topics: 5;					
Service Pack 3 it is no longer vulnerable to Windows XP Service Pack 2 exploits. VRBS.core Labs Operating System Hardening (OSH), Topics: 9 Students will have access to a Windows 2012 Server unning the Windows Service Pack 2 exploits. They will select the required patches based on reports provided by previous scanning activity performed with the use of Microsoft Baseline Security Analyzer (MBSA) and the Operating System Hardening (OSH), Topics: 9 Students will have access to a Windows 2012 Server unning the Windows Service Pack 2 exploits. They will select the required patches based on reports provided by previous scanning activity performed with the use of Microsoft Baseline Security Analyzer (MBSA) and the Operating System Hardening (OSH), Topics: 9 Students will have access to a Windows 2012 Server unning the Windows Server Update Service (WSSS), and use it to select and approve patchs needed for a Windows Cerver Update Service (WSSS), and use it to select and approve patchs needed for a Windows Cerver Update Service (WSSS), and use it to select and approve patchs needed for a Windows Cerver Update Service (WSSS), and use it to select and approve patchs needed for a Windows Cerver Update Service (WSSS), and use it to select and approve patchs needed for a Windows Cerver Update Service (WSSS), and use it to select and approve patchs needed for a Windows Cerver Update Service (WSSS), and use it to select and approve patch needed for a Windows Cerver Update Service (WSSS), and use it to select and approve patch needed for a Windows Cerver Update Service (WSSS), and use it to select and approve patch needed for a Windows Cerver Update Service (WSSS), and use it to select and approve patch needed for a Windows Cerver Update Service (WSSS), and use it to select and approve patch needed for a Windows Service (WSSS), and use it to select and approve patch needed for a Windows Service (WSSS), and use it to select and patch needed for a Windows Service (WSSS), and use it to select and approve patch needed for a	ratin installation and validation Testing	move to remediate the vulnerability, if necessary.	CTBRSCORE SCORED LADS	Operating System Hardening (OSH), Topics: 9	nyper-v	1 nour, 30 Minutes	1 mour, 30 Minutes	42 minutes, / seconds	1 minute, 31 seconds
Service (MSSS), and use it to select and approve patches needed for a Windows 7 elect. They will select the required patches based on reports provided assemble System (MBSA) and the Operating System Hardening (OSH), Topics: 9 Students will have access to a Windows 2012 Server running the Windows Server Update Service (MSSS), and use it to select and approve patches needed for a Windows Server Update Service (MSSS), and use it to select and approve patches needed for a Windows Server Update Service (MSSS), and use it to select and approve patches needed for a Windows Server Update Service (MSSS), and use it to select and approve patches needed for a Windows Server Update Service (MSSS), and use it to select and approve patches needed for a Windows Server Update Service (MSSS), and use it to select and approve patches needed for a Windows Server Update Service (MSSS), and use it to select and approve patches needed for a Windows Server Update Service (MSSS), and use it to select and approve patches needed for a Windows Server Update Service (MSSS), and use it to select and approve patches needed for a Windows Server Update Service (MSSS), and use it to select and approve patches needed for a Windows Server Update Service (MSSS), and use it to select and approve patches needed for a Windows Server Update Service (MSSS), and use it to select and approve patches needed for a Windows Server Update Service (MSSS), and use it to select and approve patches needed for a Windows Server Update Service (MSSS), and use it to select and approve patches needed for a Windows Service (MSSS), and use it to select and approve patches needed for a Windows Service (MSSS), and use it to select and approve patches needed for a Windows Serv	Patches and Updates		CYBRScore Labs	IT Systems Components (ISC), Topics: 12; Windows System Administration (WSA), Topics: 5; Operating System Hardening (OSH), Topics: 9	Hyper-V	30 Minutes	1 Hour	20 minutes, 5 seconds	22 seconds
Service (WSUS), and use it to select and approve patches needed for a Windows 7 client. They will select the required patches based on reports provided by previous scanning activity performed with the use of Microsoft Baseline Security Analyzer (MBSA) and the Open Van). Open Vulnerability Assessment System (OpenVAS). IT Systems Components (ISC), Topics: 12: Windows System Administration (WSA), Topics: 5: Operating OSH), Topics: 9 It hour, 30 Minutes 2 Hours 1 Hour, 30 Minutes 2 Hours 2 Hours 2 Hours 3 Minutes, 49 seconds 1 minute, 37 seconds	Patching With WSUS	Service (WSUS), and use it to select and approve patches needed for a Windows 7 client. They will select the required patches based on reports provided by previous scanning activity performed with the use of Microsoft Baseline Security Analyzer (MBSA) and the	CYBRScore Labs		Hyper-V	30 Minutes	45 Minutes	9 minutes, 43 seconds	30 seconds
enetration Tester (CYBRScore Challenge) Hack the Network and Deface the Web Server CryBRScore Captiones Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10 Vsphere Hours Is minutes, 58 seconds S4 seconds	Patching With WSUS	Service (WSUS), and use it to select and approve patches needed for a Windows 7 client. They will select the required patches based on reports provided by previous scanning activity performed with the use of Microsoft Baseline Security Analyzer (MBSA) and the	CYBRScore Scored Labs	IT Systems Components (ISC), Topics: 12; Windows System Administration (WSA), Topics: 5; Operating System Hardening (OSH), Topics: 9	Hyper-V	1 Hour, 30 Minutes	2 Hours	26 minutes, 49 seconds	1 minute, 37 seconds
	Penetration Tester (CYBRScore Challenge)	Hack the Network and Deface the Web Server	CYBRScore Capstones	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10	vSphere	4 Hours	8 Hours	15 minutes, 58 seconds	54 seconds

Penetration Tester Challenge	Hack the Network and Deface the Web Server	CYBRScore Scored Labs	Penetration Testing (PTT), Topics; 3, 4, 5, 6, 8, 9, 10	vSphere	1 Hour	1 Hour	39 minutes, 13 seconds	1 minute, 21 seconds
Penetration Tester Challenge Capstone	Hack the Network and Deface the Web Server Hack the Network and Deface the Web Server	CYBRScore Scored Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10 Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10	vSphere	3 Hours	5 Hours	25 minutes, 44 seconds	
Pentesting & Network Exploitation - Assessment	Hack the Network and Deface the Web Server	CYBRScore Scored Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10	vSphere	3 Hours	5 Hours	1 hour, 39 minutes	58 seconds
Pentesting & Network Exploitation - LAN Exploitation Labs	Pentesting & Network Exploitation exposes students to all manner of reconnaissance, scinning, enumeration, exploitation and pillaging for 802.3 networks. The Lab topics expose students to a variety of recon, discovery, scanning, enumeration, exploitation, post-exploitation, pillaging, covering your tracks and persistence.	CYBRScore Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10	vSphere	20 Hours	40 Hours		
Pentesting & Network Exploitation - Linux Target Analysis Capstone v2	The Art of Exploitation: Pentesting & Network Exploitation capstone tests personnel on their understanding of and capability in performing reconnaissance scanning, enumeration, exploitation and data harvesting against physical networks.	CYBRScore Capstones	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10	vSphere	3 Hours	3 Hours, 30 Minutes	6 minutes, 45 seconds	1 minute
Pentesting & Network Exploitation - Linux Target Analysis Labs	Pentesting & Network Exploitation exposes students to all manner of reconnaissance, scanning, enumeration, exploitation and pillaging for 802.3 networks. The Lab topics expose students to a variety of recon, discovery, scanning, enumeration, exploitation, post-exploitation, pillaging, covering your tracks and persistence.	CYBRScore Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10	vSphere	20 Hours	40 Hours	2 minutes, 8 seconds	31 seconds
Pentesting & Network Exploitation - Linux Target Analysis Labs (4)	Art of Exploitation: Pentesting & Network Exploitation exposes students to all manner of reconnaissance, scanning, enumeration, exploitation and pilliaging for 802.3 networks. The Lab topics expose students to a variety of recon, discovery, scanning, enumeration, exploitation, post-exploitation, pilliaging, covering your tracks and persistence.	CYBRScore Scored Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10	vSphere	3 Hours, 57 Minutes	6 Hours, 40 Minutes	1 hour, 32 minutes	37 seconds
Pentesting & Network Exploitation - WAN/DMZ Exploitation & Pivoting Lal	Art of Exploitation: Pentesting & Network Exploitation exposes students to all manner of recomassance, scanning, enumeration, exploitation and pillaging for 802.3 networks. The Lab topics expose students to a variety of recon, discovery, scanning, enumeration, exploitation, post-exploitation, pillaging, covering your tracks and persistence.	CYBRScore Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10	vSphere	20 Hours	40 Hours	53 minutes, 58 seconds	51 seconds
Pentesting & Network Exploitation - Windows Target Analysis Labs	Pentesting & Network Exploitation exposes students to all manner of reconnaissance, scenning, enumeration, exploitation and pillaging for 80.2 in networks. The Lab topics expose students to a variety of recon, discovery, scanning, enumeration, exploitation, post-exploitation, pillaging, covering your tracks and persistence.	CYBRScore Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10	vSphere	20 Hours	40 Hours	18 minutes, 13 seconds	26 seconds
Pentesting & Network Exploitation: All Labs	Art of Exploitation: Pentesting & Network Exploitation exposes students to all manner of reconnaissance, scanning, enumeration, exploitation and pillaging for 802.3 networks. The Lab topics expose students to a variety of recon, discovery, scanning, enumeration, exploitation, post-exploitation, pillaging, covering your tracks and persistence.	CYBRScore Scored Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10	vSphere	3 Hours	4 Hours	2 hours, 4 minutes	2 minutes, 34 seconds
Pentesting & Network Exploitation: DMZ Exploitation	Art of Exploitation: Pentesting & Network Exploitation exposes students to all manner of reconnaissance, scanning, enumeration, exploitation and pilliaging for 802.3 networks. The Lab topics expose students to a variety of recon, discovery, scanning, enumeration, exploitation, post-exploitation, pilliaging, covering your tracks and persistence.	CYBRScore Scored Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10	vSphere	5 Hours	5 Hours, 10 Minutes	2 hours, 16 minutes	2 minutes, 42 seconds
Pentesting & Network Exploitation: DMZ Exploitation Capstone	Art of Exploitation: Pentesting & Network Exploitation exposes students to all manner of reconnaissance, scanning, enumeration, exploitation and pilliaging for 802.3 networks. The Lab topics expose students to a variety of recon, discovery, scanning, enumeration, exploitation, post-exploitation, pilliaging, covering your tracks and persistence.	CYBRScore Capstones	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10	vSphere	3 Hours	4 Hours	2 hours, 9 minutes	2 minutes, 35 seconds
Pentesting & Network Exploitation: DMZ Exploitation Capstone v2	The Art of Exploitation: Pentesting & Network Exploitation capstone tests personnel on their understanding of and capability in performing reconnaissance scanning, enumeration, exploitation and data harvesting against physical networks.	CYBRScore Capstones	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10	vSphere	3 Hours	4 Hours	10 minutes, 17 seconds	2 minutes, 34 seconds
Pentesting & Network Exploitation: LAN Exploitation	Art of Exploitation: Pentesting & Network Exploitation exposes students to all manner of reconnaissance, scanning, enumeration, exploitation and pillaging for 802.3 networks. The Lab topics expose students to a variety of recon, discovery, scanning, enumeration, exploitation, post-exploitation, pillaging, covering your tracks and persistence.	CYBRScore Scored Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10	vSphere	3 Hours	4 Hours	2 hours, 53 minutes	2 minutes, 39 seconds
Pentesting & Network Exploitation: LAN Exploitation Capstone	Art of Exploitation: Pentesting & Network Exploitation exposes students to all manner of reconnaissance, scanning, enumeration, exploitation and pilliaging for 802.3 networks. The Lab topics expose students to a variety of recon, discovery, scanning, enumeration, exploitation, post-exploitation, pilliaging, covering your tracks and persistence.	CYBRScore Capstones	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10	vSphere	3 Hours	4 Hours	14 minutes, 41 seconds	2 minutes, 38 seconds
Pentesting & Network Exploitation: LAN Exploitation Capstone v2	The Art of Exploitation: Pentesting & Network Exploitation capstone tests personnel on their understanding of and capability in performing reconnaissance scanning, enumeration, exploitation and data harvesting against physical networks.	CYBRScore Capstones	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10	vSphere	3 Hours	4 Hours	2 hours, 13 minutes	1 minute, 30 seconds
Pentesting & Network Exploitation: Windows Target Analysis Capstone v2	The Art of Exploitation: Pentesting & Network Exploitation capstone tests personnel on their understanding of and capability in performing reconnaissance scanning, enumeration, exploitation and data harvesting against physical networks.	CYBRScore Capstones	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10	vSphere	1 Hour	1 Hour	19 minutes, 46 seconds	1 minute, 30 seconds
Pentesting & Network Exploitation: Windows Target Analysis Labs	Art of Exploitation: Pentesting & Network Exploitation exposes students to all manner of reconnaissance, scanning, enumeration, exploitation and pilliaging for 802.3 networks. The Lab topics expose students to a variety of recon, discovery, scanning, enumeration, exploitation, post-exploitation, pilliaging, covering your tracks and persistence.	CYBRScore Scored Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10	vSphere	3 Hours	4 Hours	57 minutes, 25 seconds	2 minutes, 25 seconds
Performing an Initial Attack Analysis	Students will use perform incident response on a compromised machine.	CYBRScore Labs	Network Security Administration (NSA); Topics: 2, 5, 7, 8, 9, 10	Hyper-V	1 Hour	1 Hour		31 seconds
Performing an Initial Attack Analysis Performing an Initial Attack Analysis Capstone - Skills Passport	Students will use perform incident response on a compromised machine.	CYBRScore Scored Labs CYBRScore Capstones	Network Security Administration (NSA); Topics: 2, 5, 7, 8, 9, 10	Hyper-V	1 Hour	1 Hour	25 minutes, 53 seconds	1 minute, 31 seconds
	Students will use perform incident response on a compromised machine. This next lab walks students through identifying a security incident, as well as handling		Network Security Administration (NSA); Topics: 2, 5, 7, 8, 9, 10	Hyper-V				
Performing Incident Response in a Windows Environment	and then responding to the incident.	CYBRScore Labs	Network Security Administration (NSA); Topics: 2, 5, 7, 8, 9, 10	Hyper-V	45 Minutes	1 Hour	17 minutes, 14 seconds	35 seconds
Performing Incident Response in a Windows Environment	This next lab walks students through identifying a security incident, as well as handling and then responding to the incident.	CYBRScore Scored Labs	Network Security Administration (NSA); Topics: 2, 5, 7, 8, 9, 10	Hyper-V	45 Minutes	1 Hour	39 minutes, 33 seconds	1 minute, 15 seconds

			1				
This lab walks students through identifying a security incident, as well as handling and then responding to the incident.	CYBRScore Capstones	Network Security Administration (NSA); Topics: 2, 5, 7, 8, 9, 10	Hyper-V	1 Hour	2 Hours	1 hour, 6 minutes	48 seconds
Anti-virus [AV] programs are software designed to detect and quarantine programs that are deemed malicious. These applications were originally designed to renove malware from inflected computers. Over time, AV products evolved no protect against other threats such as keyloggers, worms, and malicious websites, in this lab you will install, configure and use ratin-virus to help derind your system.	CYBRScore Labs	Operating Systems Hardening (OSH); Topics: 1, 2, 3, 4, 5, 6, 7, 8, 10, 11	Hyper-V	45 Minutes	45 Minutes	30 minutes, 43 seconds	13 seconds
Anti-virus (AV) programs are software designed to detect and quarantine programs that are deemed malicious. These applications were originally designed to renove malware from infected computers. Over time, AV products evolved to protect against other threats such as keyloggers, worms, and malicious vebsites: in this lab you will install, configure and use arti-virus to help defen your system.	CYBRScore Scored Labs	Operating Systems Hardening (QSH); Topics: 1, 2, 3, 4, 5, 6, 7, 8, 10, 11	Hyper-V	1 Hour	1 Hour	19 minutes, 11 seconds	1 minute, 14 seconds
Students will send a phishing email using the Social Engineering Toolkit. Students will then impersonate a user clicking on the attachment to observe how dangerous they can be and generate a phishing awareness email to educate users of the dangers of clicking unknown links.	CYBRScore Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10	Hyper-V	1 Hour	2 Hours	24 minutes, 22 seconds	30 seconds
be and generate a phishing awareness email to educate users of the dangers of clicking unknown links.	CYBRScore Scored Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10	Hyper-V	1 Hour	2 Hours	30 minutes, 10 seconds	1 minute, 21 seconds
In this lab you will simulate an attack involving physical access to a workstation. Physical security is important because if an attacker, or you as a penetration tester, have physical access to a machine, it is very difficult to stop a determined effort to gain access to that machine.	CYBRScore Scored Labs	Security Program Management (SPM); Topics: 6, 8	Hyper-V	1 Hour	1 Hour	43 minutes, 2 seconds	41 seconds
machine.		Security Program Management (SPM); Topics: 6, 8	Hyper-V	1 Hour	1 Hour	37 minutes, 38 seconds	1 minute, 43 seconds
In this lab, we expand on our initial coverage of Metasploit and we will look at what to do	CYBRScore Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10	Hyper-V	2 Hours	2 Hours, 30 Minutes	1 hour, 12 minutes	1 minute, 18 seconds
In this lab, as part of the recovery process, the student will restore services to a host in a post-incident environment. Startup services, and firewall settings, will both need to be addressed.		Network Security Administration (NSA); Topics: 2, 5, 7, 8, 9, 10	Hyper-V	1 Hour	1 Hour	1 minute, 13 seconds	18 seconds
Students will go through a practice forensic analysis using a given image and the available	CYBRScore Digital Media Forensics	Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10	Hyper-V	2 Hours	4 Hours		
Students will go through a practice forensic analysis using a given image and the available	CYBRScore Capstones	Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10	Hyper-V	2 Hours	4 Hours		
Students will utilize Nmap, a network discovery and mapping tool, to identify the systems on a network of responsibility. Using the tool, students will identify other devices on the laboratory network, to include computers and network infrastructure devices, such as		Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10	Hyper-V	1 Hour	1 Hour	22 minutes, 47 seconds	42 seconds
Students will utilize Nmap, a network discovery and mapping tool, to identify the systems on a network of responsibility. Using the tool, students will identify other devices on the laboratory network, to include computers and network infrastructure devices, such as	CYBRScore Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10	Hyper-V	1 Hour	1 Hour	22 minutes, 14 seconds	38 seconds
Students will utilize Nmap, a network discovery and mapping tool, to identify the systems on a network of responsibility. Using the tool, students will identify other devices on the laboratory network, to include computers and network infrastructure devices, such as routers.	CYBRScore Scored Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10	Hyper-V	1 Hour	1 Hour	23 minutes, 44 seconds	1 minute, 20 seconds
In this lab, students will prepare target media for imaging using dc3dd and Disk Wipe.	CYBRScore Digital Media Forensics	Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10	Hyper-V	45 Minutes	1 Hour		
In this lab, students will prepare target media for imaging using dc3dd and Disk Wipe.	CYBRScore Labs	Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10	Hyper-V	45 Minutes	1 Hour	23 minutes, 6 seconds	1 minute, 15 seconds
	CYBRScore Scored Labs	Host Forensirs (HOF): Tonics: 1 5 6 7 8 9 10	Hyner-V	45 Minutes	1 Hour	9 minutes 37 seconds	50 seconds
Students will take a PCAP indicating the presence of a beacon on the network and analyze it. The analysis will determine if there's activity that we can mitigate mitigation and then implement a Firewall block with logging to prevent future beaconing.	CYBRScore Network Forensics	Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a	Hyper-V	1 Hour	1 Hour	16 minutes, 4 seconds	45 seconds
Students will take a PCAP indicating the presence of a beacon on the network and analyze it. The analysis will determine if there's activity that we can mitigate mitigation and then implement a Firewall block with logging to prevent future beaconing.	CYBRScore Scored Labs	Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a	Hyper-V	45 Minutes	45 Minutes	18 minutes	1 minute, 34 seconds
Students will take a PCAP indicating the presence of a beacon on the network and analyze it. The analysis will determine if there's activity that we can mitigate mitigation and then implement a Firewall block with logging to prevent future beaconing.	CYBRScore Labs	Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a	Hyper-V	1 Hour	1 Hour	24 minutes, 5 seconds	26 seconds
The Python Tool Building lab is divided into two parts: Python Fundamentals and Python Tool Building. If you're new to Python, or have limited experience, please complete the exercises found in part one. The exercises will provide you with a primer on important Python fundamentals. If you have experience with Python, you may want to skip the first section, or simply refer to it during the labs. In part two, you will build several scanning/enumeration and exploitation scripts. These scripts will demonstrate the power and usefulness of Python when performing penetration tests and red team exercises. The scripts are ment to be fairly straightforward proof-of-concepts to get your stratest. You are highly encouraged to customer and execut the scripts to whe keyord the scenarios provided.	CYBRScore Labs	to code in this bookcamp-like setting	Hyper-V	2 Hours	4 Hours	58 minutes, 48 seconds	33 seconds
In Development	CYBRScore Labs	Network Defense (NDF), Topics: 1a, 1c, 1d, 2b, 4a	Hyper-V	4 Hours	4 Hours		
				58 Hours, 20 Minutes	58 Hours, 20 Minutes		
In Development In Development	CYBRScore Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10 Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10	Hyper-V		58 Hours, 20 Minutes		
In Development	CYBRScore Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10	Hyper-V	58 Hours, 20 Minutes	58 Hours, 20 Minutes		
In this lab, you will exploit a very simple SQL injection vulnerability, as an authenticated	CYBRScore Labs		Hyper-V	2 Hours	4 Hours		
ports. While you will often be able to use tools such as netcat or telnet to perform banner grabs, it is useful to know how to write a quick script that you can deploy on an engagement should your traditional tool set be unavailable.			Hyper-V	2 Hours	4 Hours		
In this lab, students are given a compromised machine on which they will place an agent. This agent will need to beacon out for instructions, execute commands, and push the data to a remote server.	CYBRScore Labs		Hyper-V	2 Hours	4 Hours		
	Then responding to the incident. Anti-virus IAV programs are software designed to detect and quarantine programs that are deemed malicious. These applications were originally designed to remove malware from infected computers. Over time, Ary products evolved no protect against other threats such as keyloggers, worms, and malicious websites. In this lab you will install, configure and use arti-virus to help demoly our system. Anti-virus (AV) programs are software designed to detect and quarantine programs that are deemed malicious. These applications were originally designed to remove malware from infected computers. Over time, Ary products evolved to protect against other threats such as keyloggers, worms, and malicious websites. In this lab you will install, configure and use arti-virus to help defined your system. Students will send a phishing email using the Social Engineering Toolkit. Students will be imperiously a survivision to help defined your system. Students will send a phishing email using the Social Engineering Toolkit. Students will control will be a surviving to the product of the surviving to help and the survivinia of the products every of the dangers of clicking malicious milks. Students will send a phishing email using the Social Engineering Toolkit. Students will be interested to the survivinia of t	Then responding to the incident: are deemed malicious. These applications were originally designed to remove malware from infected computers. Over time, Any products sevolved to protest against other threats such as keyloggers, women, and malicious webloties. In this lab you will incital, configure and our anti-wirns to high defined your system. Anti-virus (AN) programs are software designed to detect and quarantine programs that are deemed malicious. Three applications were originally designed to remove malware from infected computers. Dever time, AN products evolved to protest against other threats such as keyloggers, women, and malicious webloties. In this lab you will install, configure and our anti-virus to help defend your system. Anti-virus (AN) programs are software designed to detect and quarantine programs that are deemed malicious. Three applications were originally designed to remove malware from infected computers. Dever time, AV products evolved to protest against other threats such as level publing great and the second protest of the body will install, configure and our anti-virus to help defend your system. Students will send a planking email using the Social Engineering Toolist. Students will be the impersonate a user clicking on the attachment to observe how dangerous they can be an expensive to the application of the dangers of clicking authority in install, and the protest of the dangers of clicking authority in important because if an attacker, or you as a penetration tester, here phylical access to a machine. It is very difficult to store phylical access to a workstation. Phylical access to a workstation in Phylical access to a workstation in Phylical access to a workstation. Phylical security is important because if an attacker, or you as a penetration tester, here phylical access to a workstation in Phylical security is important because if an attacker, or you as a penetration tester, here phylical access to a workstation in Phylical security is important because if an attacker, or y	Section Section 1. Sec	The extra production are all whose is departed to detect and expansion programs and form which companies to determine a programs and an extra production and the prod	March 1997 Mar	Company Comp	Comment Comm

Python Tool Building - Local File Inclusion		CYBRScore Labs		Hyper-V	2 Hours	4 Hours		
Ransomware	availability of files outside of the web root. Students will learn what ransomware is, observe how it works, and implement mitigation	CYBRScore Labs	Vulnerability Analysis (VLA): Topics: 1. 3. 4. 5. 6. 7. 8. 10	Hyper-V	30 Minutes	45 Minutes	27 minutes, 52 seconds	1 minute. 15 seconds
Recover from Browser-based Heap Spray Attack	strategies to recover from a ransomware attack. After identifying a browser-based heap spray attack used against a corporate asset, students will learn about EMET and the role it plays in recovery from a variety of attack		Vulnerability Analysis (VLA); Topics: 1, 3, 4, 5, 6, 7, 8, 10	Hyper-V	1 Hour, 17 Minutes	2 Hours	18 minutes, 58 seconds	
Recover from Illegal Bitcoin Mining Incident	vectors. Students will conduct recovery activities using indicators of Compromise found on the victors computes and other explicitly related splifters. Students will also conduct recovery	CYBRScore Labs	Vulnerability Analysis (VLA); Topics: 1, 3, 4, 5, 6, 7, 8, 10	Hyper-V	45 Minutes	1 Hour		
Recover from Illegal Bitcoin Mining Incident	Students will conduct recovery activities using Indicators of Compromise found on the victim computer and other network-nelated artifacts. Students will also conduct recovery operations by looking for evidence of reinfection, malicious network activity, and checking pacts livels and hotflies applied to the victim computer.	CYBRScore Scored Labs	Vulnerability Analysis (VLA); Topics: 1, 3, 4, 5, 6, 7, 8, 10	Hyper-V	45 Minutes	1 Hour	21 minutes, 35 seconds	1 minute, 9 seconds
Recover from Incident	This lab covers a variety of concepts, and exercises static and dynamic analysis skills related to malware identification and eradication. After identifying and analyzing a malicious executable in a test environment, use the information gained to recover from an incident, and remove the malicious file from the victim's computer.	CYBRScore Labs	Vulnerability Analysis (VLA); Topics: 1, 3, 4, 5, 6, 7, 8, 10	Hyper-V	2 Hours	4 Hours	39 minutes, 14 seconds	23 seconds
Recover from Incident	This lab covers a variety of concepts, and exercises static and dynamic analysis skills related to malware identification and eradication. After identifying and analyzing a malicious executable in a test environment, use the information gained to recover from an incident, and remove the malicious file from the victim's computer.	CYBRScore Scored Labs	Vulnerability Analysis (VLA); Topics: 1, 3, 4, 5, 6, 7, 8, 10	Hyper-V	2 Hours	4 Hours	5 minutes	31 seconds
Recover from SQL Injection Attack	After identifying a SQL Injection attack, students will learn about parameterized queries in back-end web servers to minimize future SQLI attacks.	CYBRScore Labs	Vulnerability Analysis (VLA); Topics: 1, 3, 4, 5, 6, 7, 8, 10	Hyper-V	1 Hour, 6 Minutes	2 Hours	41 minutes, 12 seconds	26 seconds
Recover from SQL Injection Attack	After identifying a SQL Injection attack, students will learn about parameterized queries in back-end web servers to minimize future SQLi attacks.	CYBRScore Scored Labs	Vulnerability Analysis (VLA); Topics: 1, 3, 4, 5, 6, 7, 8, 10	Hyper-V	1 Hour, 6 Minutes	2 Hours	7 minutes, 18 seconds	1 minute, 11 seconds
Recover from Web-Based Flashpack Incident	analysis to determine infection vector and payload delivery mechanisms as well as system-specific recovery procedures to restore the system to its original functionality.	CYBRScore Labs	Vulnerability Analysis (VLA); Topics: 1, 3, 4, 5, 6, 7, 8, 10	Hyper-V	1 Hour, 19 Minutes	2 Hours	7 minutes, 5 seconds	31 seconds
Recovering Data and Data Integrity Checks	In this lab, the student will establish a baseline of two pre-defined files, delete those files, and subsequently restore them. After restoration, the student will perform an integrity validation on the recovered files.		Vulnerability Analysis (VLA); Topics: 1, 3, 4, 5, 6, 7, 8, 10	Hyper-V	1 Hour	1 Hour	39 minutes, 59 seconds	42 seconds
Recovery From Inadequate Patching	Students will become familiar with procedures used backing up data, patching the system after a reported attack, checking the system for new vulnerabilities and then performing a roilback.	CYBRScore Labs	Vulnerability Analysis (VLA); Topics: 1, 3, 4, 5, 6, 7, 8, 10	Hyper-V	2 Hours	2 Hours	1 hour, 6 minutes	1 minute, 18 seconds
Registry Analysis	Windows Registry as well as where to find the information.	CYBRScore Digital Media Forensics	Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10	Hyper-V	3 Hours	4 Hours		
Registry Analysis	In this lab, students will understand what type of information is contained within the Windows Registry as well as where to find the information.	CYBRScore Labs	Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10	Hyper-V	3 Hours	4 Hours	42 minutes, 33 seconds	1 minute, 5 seconds
Registry Analysis	In this lab, students will understand what type of information is contained within the Windows Registry as well as where to find the information.	CYBRScore Scored Labs	Host Forensics (HOF); Topics: 1, 5, 6, 7, 8, 9, 10	Hyper-V	1 Hour	2 Hours	41 minutes, 4 seconds	1 minute, 19 seconds
Remove Trojan		CYBRScore Labs	Operating Systems Hardening (OSH); Topics: 1, 2, 3, 4, 5, 6, 7, 8, 10, 11	Hyper-V	1 Hour	1 Hour	39 minutes, 42 seconds	17 seconds
Report Comparison and Evaluation	Students will generate reports from Core Impact and from OpenVAS and compare the discrepancies between the two. Students will also identify the positive and negative	CYBRScore Labs	Network Security Administration (NSA); Topics: 2, 5, 7, 8, 9, 10	Hyper-V	1 Hour	1 Hour, 30 Minutes	13 minutes, 15 seconds	27 seconds
Report Comparison and Evaluation		CYBRScore Scored Labs	Network Security Administration (NSA); Topics: 2, 5, 7, 8, 9, 10	Hyper-V	1 Hour	1 Hour, 30 Minutes		
Report Writing for Presentation to Management	qualities for both report types. In an easifier lab, industed sanalyzed a suspected exploit (FlashPack Exploit Kt) on a corporate machine. In this lab they will find evidence of another FlashPack infection in using previously captured network traffic. In this scenario they will determine the details about how this stack was successful and will fill out a report with their findings. This report will been be used to before the Management Team, as well as note the incident for future tracking purposes.	CYBRScore Labs	Cybersecurity Planning and Management (CPM); Topics: 2, 4, 5, 6, 8, 9	Hyper-V	1 Hour	1 Hour, 30 Minutes	32 minutes, 32 seconds	22 seconds
Report Writing for Presentation to Management	in an earlier lab, students analyzed a suspected exploit (FlashPack Exploit Kit) on a corporate machine. In this lab they will find evidence of another FlashPack infection in using previously explured network traffic. In this scenario flew will determine the details about how this attack was successful and will fill out a report with their findings. This report will then be used to brief the Management Team, as well as note the incident for future tracking purposes.		Cybersecurity Planning and Management (CPM); Topics: 2, 4, 5, 6, 8, 9	Hyper-V	1 Hour	1 Hour, 30 Minutes	35 minutes, 49 seconds	47 seconds
Respond to and Validate Alerts from Antivirus Software	Students will respond to and validate alerts from Antivirus software.	CYBRScore Labs	Software Security Analysis (SSA); Topics: 1, 2, 3, 4, 5	Hyper-V	30 Minutes	1 Hour	10 minutes, 13 seconds	16 seconds
Reverse Engineering Malware	MAL500 builds upon our Fundamentals of Malware Analysis course and exposes students to the theoretical knowledge and hands on techniques used to analyze malware of greater complexity. In Reverse Engineering Malware, students will learn how to reverse and dissect malicious Windows programs, ethel guser-mode and kernel-mode malware, as well as identify common malware functionality and hiding techniques. This course is for malware or spiring-malware analysis who have already laker CMRSCore's Modo (fundamentals of Malware Analysis) course, or for those who have encountered malware analysis as part of incident response, research, or secure development, and want to improve upon their knowledge and skills.	CYBRScore Labs	Software Security Analysis (SSA); Topics: 1, 2, 3, 4, 5	vSphere	40 Hours	41 Hours, 40 Minutes	4 minutes, 35 seconds	11 seconds
Rogue Device Identification and Blocking	Students will scan a network and identify rogue devices. Students will then customize the firewall rules to ensure that any rogue devices are blocked from communicating with other systems on the network.	CYBRScore Labs	Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a	Hyper-V	1 Hour	1 Hour	24 minutes, 46 seconds	36 seconds
Rogue Device Identification and Blocking	Students will scan a network and identify rogue devices. Students will then customize the firewall rules to ensure that any rogue devices are blocked from communicating with other systems on the network.	CYBRScore Network Forensics	Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a	Hyper-V	1 Hour	1 Hour	28 minutes, 38 seconds	2 minutes, 10 seconds
Rogue Device Identification and Blocking	Students will scan a network and identify rogue devices. Students will then customize the firewall rules to ensure that any rogue devices are blocked from communicating with other systems on the network.		Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a	Hyper-V	1 Hour	1 Hour	41 minutes, 13 seconds	1 minute, 16 seconds
RootKit	This lab is designed to introduce the student to a Windows rootkit and to some tools and techniques used in discovery and removal of the rootkit. This experience should provide them with a basic understanding of rootkits and the challenges they pose during the removal process.	CYBRScore Labs	Operating Systems Hardening (OSH); Topics: 1, 2, 3, 4, 5, 6, 7, 8, 10, 11	vSphere	1 Hour	1 Hour	1 minute, 32 seconds	11 seconds
Scanning and Enumeration	In this lab, you will practice scanning and enumeration using several popular tools, and learn how they can be used together to create a thorough and efficient workflow during the enumeration phase.	CYBRScore Scored Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10	Hyper-V	3 Hours	4 Hours	54 minutes, 39 seconds	1 minute, 2 seconds
Scanning and Enumeration (Scored)	in this lab, you will practice scanning and enumeration using several popular tools, and learn how they can be used together to create a thorough and efficient workflow during the enumeration phase.	CYBRScore Scored Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10	Hyper-V	3 Hours	4 Hours	26 minutes, 46 seconds	1 minute, 23 seconds

Scanning and Mapping Networks	Students will use Zenmap to scan a network segment in order to create an updated network map and detail findings on the systems discovered. They will use the material they generated to help them discover if there have been any changes to the network after they compare it to a previously generated network map/scan.	CYBRScore Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10	Hyper-V	45 Minutes	1 Hour	20 minutes, 41 seconds	46 seconds
Scanning and Mapping Networks	Students will use Zenmap to scan a network segment in order to create an updated network map and detail findings on the systems discovered. They will use the material they generated to help them discover if there have been any changes to the network after they compare it to a previously generated network map/scan.	CYBRScore Scored Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10	Hyper-V	3 Hours	4 Hours	34 minutes, 1 second	1 minute, 34 seconds
Scanning From Windows	Students will leverage Scainline, a windows network discovery and mapping tool, to identify the systems on a network of responsibility. Students will utilize non-traditional scans to attempt avoiding an Intrusion Detection System (IDS).	CYBRScore Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10	Hyper-V	45 Minutes	45 Minutes	15 minutes, 4 seconds	36 seconds
Scanning From Windows	Students will leverage Scalnline, a windows network discovery and mapping tool, to identify the systems on a network of responsibility. Students will utilize non-traditional scans to attempt avoiding an Intrusion Detection System (IDS).	CYBRScore Network Forensics	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10	Hyper-V	45 Minutes	45 Minutes	13 minutes, 58 seconds	44 seconds
Scanning with Nmap	In this lab, you will perform several scans but, using Wireshark, you will be able to view the scan traffic to see what the tool is actually doing under the hood.	CYBRScore Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10	Hyper-V	1 Hour	1 Hour	54 minutes, 19 seconds	33 seconds
Searching for Indicators of Compromise	If a company has a vulnerable internet facing application, it can be exploited. An analyst should know how to identify attacks by artifacts that are present in the IDS as well as evidence on the compromised system.	CYBRScore Labs	Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a	Hyper-V	1 Hour	1 Hour	34 minutes, 52 seconds	51 seconds
Searching for Indicators of Compromise	If a company has a vulnerable internet facing application, it can be exploited. An analyst should know how to identify attacks by artifacts that are present in the IDS as well as evidence on the compromised system.	CYBRScore Network Forensics	Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a	Hyper-V	1 Hour	1 Hour	34 minutes, 8 seconds	41 seconds
Searching for Indicators of Compromise	If a company has a vulnerable internet facing application, it can be exploited. An analyst should know how to identify attacks by artifacts that are present in the IDS as well as evidence on the compromised system.	CYBRScore Scored Labs	Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a	Hyper-V	1 Hour	1 Hour		
Secure Coding (C++) - Lab 1: Race Conditions	In this lab, we will look at attacks on race conditions and then cover how to fix them.	CYBRScore Labs		Hyper-V	1 Hour			
Secure Coding (C++) - Lab 2: Data Validation	In this lab, we will look at vulnerabilities involving code injection due to improper handling of user input.	CYBRScore Labs		Hyper-V	1 Hour			
Secure Coding (C++) - Lab 3: Authentication	In this lab, we will look at authentication vulnerabilities including verbose error messages, plaintext passwords, and single-factor authentication.	CYBRScore Labs		Hyper-V	1 Hour			
Secure Coding (C++) - Lab 4: Access Control	In this lab, we will look at vulnerabilities with access control - the process by which a system decides whether or not a user is allowed to make use of a resource.	CYBRScore Labs		Hyper-V	1 Hour			
Secure Coding (C++) - Lab 5: Cryptography	There are many issues that can arise with Cryptography, when trying to write secure code. In this lab, we will address three examples.	CYBRScore Labs		Hyper-V	1 Hour			
Secure Coding (C++) - Lab 6: Error Handling	In this lab, we will look at vulnerabilities involving overly verbose error messages and insufficient logging.	CYBRScore Labs		Hyper-V	45 Minutes			
Secure Coding (C++) - Lab 7: Static Analysis	In this lab, we will be looking at a tool called CodeChecker that analyzes code for issues with both security vulnerabilities and coding conventions.	CYBRScore Labs		Hyper-V	30 Minutes			
Secure Coding (C++) - Lab 8: Buffer Overflows	When too much data is placed into a buffer, it can overwrite adjacent memory values leading to remote code execution or system crashes. This lab will explore such vulnerabilities and how to fix them.	CYBRScore Labs		Hyper-V	1 Hour			
Secure Coding (Java) - Lab 1: Race Conditions	In this lab, we will look at attacks on race conditions and then cover how to fix them.	CYBRScore Labs		Hyper-V	1 Hour			
Secure Coding (Java) - Lab 2: Data Validation	In this lab, we will look at vulnerabilities involving code injection due to improper handling of user input.	CYBRScore Labs		Hyper-V	1 Hour			
Secure Coding (Java) - Lab 3: Authentication	In this lab, we will look at authentication vulnerabilities including verbose error messages, plaintext passwords, and single-factor authentication.	CYBRScore Labs		Hyper-V	1 Hour			
Secure Coding (Java) - Lab 4: Access Control	In this lab, we will look at vulnerabilities with access control - the process by which a system decides whether or not a user is allowed to make use of a resource.	CYBRScore Labs		Hyper-V	45 Minutes			
Secure Coding (Java) - Lab 5: Cryptography	There are many issues that can arise with Cryptography, when trying to write secure code. In this lab, we will address three examples.	CYBRScore Labs		Hyper-V	1 Hour			
Secure Coding (Java) - Lab 6: Error Handling	In this lab, we will look at vulnerabilities involving overly verbose error messages and insufficient logging.	CYBRScore Labs		Hyper-V	45 Minutes			
Secure Coding (Java) - Lab 7: Static Analysis	In this lab, we will be looking at a tool called CodeChecker that analyzes code for issues with both security vulnerabilities and coding conventions.	CYBRScore Labs		Hyper-V	30 Minutes			
Secure Coding (Java) - Lab 8: Insecure Deserialization	Many languages use object serialization for communication as it can greatly ease development. However, in some cases, actions can be taken automatically when objects are deserialized, if certain conditions are present. If the serigized object is ever exposed to and end user, that user can tamper with and modify the object, either causing marchitorized danges in variables or, if those conditions are present, execution of unauthorized code. This issue has been the source of several major security breaches. In this lab, we will examine this problem, see how it can be exploited, and demonstrate bes practices for securing your code against these types of attacks.	CYBRScore Labs		Hyper-V	1 Hour			
Secure Coding (Python) - Lab 1: Race Conditions	In this lab, we will look at attacks on race conditions and then cover how to fix them.	CYBRScore Labs	Secure Programming Practices (SPP); Topics: 1, 2, 3, 4 (all), 5a, 6, 7, 8	Hyper-V	1 Hour	2 Hours	1 hour, 6 minutes	32 seconds
Secure Coding (Python) - Lab 2: Data Validation	In this lab, we will look at vulnerabilities involving code injection due to improper handling of user input.	CYBRScore Labs	Secure Programming Practices (SPP); Topics: 1, 2, 3, 4 (all), 5a, 6, 7, 8	Hyper-V	30 Minutes	1 Hour	31 minutes, 2 seconds	21 seconds
Secure Coding (Python) - Lab 3: Authentication	In this lab, we will look at authentication vulnerabilities including verbose error messages, plaintext passwords, and single-factor authentication.	CYBRScore Labs	Secure Programming Practices (SPP); Topics: 1, 2, 3, 4 (all), 5a, 6, 7, 8	Hyper-V	1 Hour, 30 Minutes	2 Hours	1 hour	24 seconds
Secure Coding (Python) - Lab 4: Access Control	In this lab, we will look at vulnerabilities with access control - the process by which a system decides whether or not a user is allowed to make use of a resource.	CYBRScore Labs	Secure Programming Practices (SPP); Topics: 1, 2, 3, 4 (all), 5a, 6, 7, 8	Hyper-V	1 Hour	1 Hour, 30 Minutes	55 minutes, 37 seconds	25 seconds
Secure Coding (Python) - Lab 5: Cryptography	There are many issues that can arise with Cryptography, when trying to write secure code. In this lab, we will address three examples.	CYBRScore Labs	Secure Programming Practices (SPP); Topics: 1, 2, 3, 4 (all), 5a, 6, 7, 8	Hyper-V	1 Hour, 30 Minutes	2 Hours	54 minutes, 25 seconds	31 seconds
Secure Coding (Python) - Lab 6: Error Handling	In this lab, we will look at vulnerabilities involving overly verbose error messages and insufficient logging.	CYBRScore Labs	Secure Programming Practices (SPP); Topics: 1, 2, 3, 4 (all), 5a, 6, 7, 8	Hyper-V	30 Minutes	1 Hour	1 hour, 3 minutes	24 seconds
Secure Coding (Python) - Lab 7: Static Analysis	In this lab, we will be looking at a tool called CodeChecker that analyzes code for issues with both security vulnerabilities and coding conventions.	CYBRScore Labs	Secure Programming Practices (SPP); Topics: 1, 2, 3, 4 (all), 5a, 6, 7, 8	Hyper-V	1 Hour	1 Hour, 30 Minutes	2 hours, 30 minutes	34 seconds
Secure Coding (Python) - Lab 8: Pickles and Imports	In this lab, we will look at Python Pickles and the Python import system. We will be able to fix the issue relating to Pickles, and we will discuss how to mitigate the issues with	CYBRScore Labs	Secure Programming Practices (SPP); Topics: 1, 2, 3, 4 (all), 5a, 6, 7, 8	Hyper-V	45 Minutes	1 Hour	1 hour, 54 minutes	24 seconds
Secure Software Developer - Demo	Imports. Demonstration of assessment environment and capabilities.	CYBRScore	Assessment - Covers dozens of KU	Hyper-V	1 Hour	1 Hour	46 minutes, 3 seconds	2 minutes, 4 seconds

	This lab is designed to familiarize users with the Theater Manager python application. It contains the same vulnerable code used in the Secure Software Developer - Python series of assessments.							
Secure Software Developer - Python Code Review	Use this lab to review functionality and user/data interactions of the application. The	CYBRScore	Assessment - Covers dozens of KU	Hyper-V	1 Hour	1 Hour	59 minutes, 14 seconds	1 minute, 14 seconds
	documentation provided within is the same documentation available in the assessments. This lab is not scored, but time is limited to 1 hour per instance. You can launch this lab as many times as needed.							
Secure Software Developer - Python - Authentication and Access Control	This assessment in the Secure Software Development - Python series focuses on the following security areas: Authentication, Access Control, Cryptography (Access Token Forgery), and SQL Injection	CYBRScore	Assessment - Covers dozens of KU	Hyper-V	1 Hour	1 Hour	25 minutes	1 minute, 43 seconds
Secure Software Developer - Python - Business Logic and Serialization	This assessment in the Secure Software Development - Python series focuses on the following security areas: Access Control and Insecure Data Deserialization	CYBRScore	Assessment - Covers dozens of KU	Hyper-V	1 Hour	1 Hour		
Secure Software Developer - Python - Race Conditions and Data Validation	This assessment in the Secure Software Development - Python series focuses on the following security areas: Race Conditions and Data Validation	CYBRScore	Assessment - Covers dozens of KU	Hyper-V	1 Hour	1 Hour		
Secure Software Developer - Python - Secure Sockets and Error Handling	This assessment in the Secure Software Development - Python series focuses on the following security areas: Error Handling and Logging, Cryptography (Implement SSL), and Static Code Analysis - Identifying False Positives	CYBRScore	Assessment - Covers dazens of KU	Hyper-V	1 Hour	1 Hour		
	This lab is designed to familiarize users with the Theater Manager PHP application. It contains the same vulnerable code used in the Secure Software Developer - PHP series of assessments.							
Secure Software Developer - PHP Code Review	Use this lab to review functionality and user/data interactions of the application. The documentation provided within is the same documentation available in the assessments. This lab is not scored, but time is limited to 1 hour per instance. You can launch this lab	CYBRScore	Assessment - Covers dozens of KU	Hyper-V	1 Hour	1 Hour		
	as many times as needed.							
Secure Software Developer - PHP - Authentication and Access Control	This assessment in the Secure Software Development - PHP series focuses on the following security areas: SQL Injection, Access Control, and Authentication	CYBRScore	Assessment - Covers dozens of KU	Hyper-V	1 Hour	1 Hour		
Secure Software Developer - PHP - Data Handling and Authorization	This assessment in the Secure Software Development - PHP series focuses on the following security areas: Cross-Site Scripting, Data Validation, and Cryptography	CYBRScore	Assessment - Covers dozens of KU	Hyper-V	1 Hour	1 Hour		
Secure Software Developer - PHP - Data Validation and Error Handling	This assessment in the Secure Software Development - Python series focuses on the following security areas: Data Validation, Command Injection, and Error Handling	CYBRScore	Assessment - Covers dozens of KU	Hyper-V	1 Hour	1 Hour		
Secure Software Developer - PHP - Business Logic and Logging	This assessment in the Secure Software Development - PHP series focuses on the following security areas: Access Control and Error Handling	CYBRScore	Assessment - Covers dozens of KU	Hyper-V	1 Hour	1 Hour		
	This lab is designed to familiarize users with the Theater Manager java application. It contains the same vulnerable code used in the Secure Software Developer - Java series of assessments.							
Secure Software Developer - Java Code Review	Use this lab to review functionality and user/data interactions of the application. The documentation provided within is the same documentation available in the assessments. This lab is not scored, but time is limited to 1 hour per instance. You can launch this lab	CYBRScore	Assessment - Covers dozens of KU	Hyper-V	1 Hour	1 Hour		
	as many times as needed. This assessment in the Secure Software Development - Java series focuses on the							
Secure Software Developer - Java - Authentication and Serialization	Inis assessment in the Secure Software Development - Java series focuses on the following security areas: Authentication and Serialization. This assessment in the Secure Software Development - Java series focuses on the	CYBRScore	Assessment - Covers dozens of KU	Hyper-V	1 Hour	1 Hour		
Secure Software Developer - Java - Race Conditions and Authorization	following security areas: Race conditions and Authorization controls. This assessment in the Secure Software Development - Java series focuses on the	CYBRScore	Assessment - Covers dozens of KU	Hyper-V	1 Hour	1 Hour		
Secure Software Developer - Java - SSL and Error Handling	following security areas: SSL and Error handling. This assessment in the Secure Software Development - Java series focuses on the	CYBRScore	Assessment - Covers dozens of KU	Hyper-V	1 Hour	1 Hour		
Secure Software Developer - Java - Access Control and Business Logic	following security areas: Access controls, Business Logic, and Error Handling.	CYBRScore	Assessment - Covers dozens of KU	Hyper-V	1 Hour	1 Hour		
Secure Software Developer - C++ Code Review	This lab is designed to familiative users with the Theater Manager C++ application. It contains the same universible code used in the Secure Software Developer C-++ series assessments. Use this lab to review functionally and user/data interactions of the application. The documentation provided within is the same documentation available in the assessments.	CYBRScore	Assessment - Covers dozens of KU	Hyper-V	1 Hour	1 Hour		
	This lab is not scored, but time is limited to 1 hour per instance. You can launch this lab as many times as needed.							
Secure Software Developer - C++ - Authentication and Buffer Overflows	This assessment in the Secure Software Development - C++ series focuses on the following security areas: SQL Injection, Buffer Overflows, and Authentication.	CYBRScore	Assessment - Covers dozens of KU	Hyper-V	1 Hour	1 Hour		
Secure Software Developer - C++ - Race Conditions and Authorization	This assessment in the Secure Software Development - C++ series focuses on the following security areas: Race Conditions and Cryptography.	CYBRScore	Assessment - Covers dozens of KU	Hyper-V	1 Hour	1 Hour		
Secure Software Developer - C++ - SSL and Error Handling	This assessment in the Secure Software Development - C++ series focuses on the following security areas: Directory Traversal, Verbose Errors, and SSL.	CYBRScore	Assessment - Covers dozens of KU	Hyper-V	1 Hour	1 Hour		
Secure Software Developer - C++ - Access Control and Business Logic	This assessment in the Secure Software Development - C++ series focuses on the following security areas: Access Control, Business Logic, and Error Handling.	CYBRScore	Assessment - Covers dozens of KU	Hyper-V	1 Hour	1 Hour		
	This lab is designed to familiarize users with the Theater Manager CII application. It contains the same vulnerable code used in the Secure Software Developer - CII series of assessments.							
Secure Software Developer - C# - Code Review	Use this lab to review functionality and user/data interactions of the application. The documentation provided within is the same documentation available in the assessments. This lab is not scored, but time is limited to 1 hour per instance. You can launch this lab	CYBRScore	Assessment - Covers dozens of KU	Hyper-V	1 Hour	1 Hour		
	as many times as needed.							
Secure Software Developer - C# - Injection and Hashing	This assessment in the Secure Software Development - C++ series focuses on the following security areas: Authentication, Access Control, and SQL Injection. This assessment in the Secure Software Development - C++ series focuses on the	CYBRScore	Assessment - Covers dozens of KU	Hyper-V	1 Hour	1 Hour		
Secure Software Developer - C# - Access Control	following security areas: Business Logic and Access Control.	CYBRScore	Assessment - Covers dozens of KU	Hyper-V	1 Hour	1 Hour		
Secure Software Developer - C# - Logging and Data Validation	This assessment in the Secure Software Development - C++ series focuses on the following security areas: Directory Traversal and Verbose Error Messages.	CYBRScore	Assessment - Covers dozens of KU Linux System Administration (LSA), Topics: 2, 3, 4, 6, - Operating System Concepts (OSC),	Hyper-V	1 Hour	1 Hour		
Securing Linux - Advanced IPTables Securing Linux - Basic Restrictions	Awaiting Verification	CYBRScore Labs CYBRScore Labs	Topics: 1, 2, 4, 9 - Cybersecurity Principles (CSP), Topics:	Hyper-V Hyper-V	1 Hour	1 Hour	2 hours, 27 minutes 1 hour, 23 minutes	1 minute, 42 seconds 1 minute, 9 seconds
Securing Linux - Basic Restrictions Securing Linux - Capabilities and ACLs	Awaiting Verification Awaiting Verification	CYBRScore Labs	Toolcs: 1, 2, 4, 9 - Cybersecurity Principles (CSP), Toolcs: I	Hyper-V		1 Hour	1 nour, 23 minutes 54 minutes, 38 seconds	1 minute, 9 seconds
Securing Linux - Capabilities and ACLs Securing Linux - Encryption	Awaiting Verification Awaiting Verification	CYBRScore Labs	Linux System Administration (LSA), Topics: 2, 3, 4, 6, - Operating System Concepts (OSC),	Hyper-V	1 Hour	1 Hour	1 hour, 22 minutes	1 minute, 47 seconds
Securing Linux - Firewalls	Awaiting Verification	CYBRScore Labs	Topics: 1, 2, 4, 9 - Cybersecurity Principles (CSP), Topics: 1 Linux System Administration (LSA), Topics: 2, 3, 4, 6, - Operating System Concepts (OSC), Topics: 1, 2, 4, 9, - Cybersecurity Principles (CSP), Topics: 1	Hyper-V	1 Hour	1 Hour	5 hours, 12 minutes	3 minutes, 17 seconds
Securing Linux - Network Intrusion Detection	Awaiting Verification	CYBRScore Labs	Topics: 1, 2, 4, 9 - Cybersecurity Principles (CSP), Topics: Linux System Administration (LSA), Topics: 2, 3, 4, 6, - Operating System Concepts (OSC), Topics: 1, 2, 4, 9 - Cybersecurity Principles (CSP), Topics:	Hyper-V	1 Hour	1 Hour	1 hour, 41 minutes	1 minute, 10 seconds

Securing Linux - Secure Remote Access	Awaiting Verification	CYBRScore Labs	Linux System Administration (LSA), Topics: 2, 3, 4, 6, - Operating System Concepts (OSC),	Hyper-V	2 Hours	2 Hours	2 hours, 16 minutes	1 minute, 23 seconds
	Linux environments are ubiquitous in many different sectors, and securing these		Topics: 1, 2, 4, 9 - Cybersecurity Principles (CSP), Topics:					
Securing Linux for System Administrators	environments is as important as securing Windows environments. This lish walks you through implementing least-privilege and strong security procisics in a Linux environment. Specifically, you will walk through ways to secure your Linux box, look at and fix common areas of privilege is used-plauses, and get introduced to SELinux and how It helps when implementing least-privilege.	CYBRScore Labs	Linux System Administration (LSA), Topics: 2, 3, 4, 6 - Cybensecurity Principles (CSP), Topics: ; Operating System Concepts (OSC), Topics: 1, 9	Hyper-V	45 Minutes	1 Hour	15 minutes, 10 seconds	1 minute, 20 seconds
Securing Linux for System Administrators	Linux environments are ubiquitous in many different sectors, and securing these environments is as important as securing Windows environments. This lab walks you through implementing least-privilege and strong security practices in a Linux environment. Specifically, you will waik through ways to secure your Linux box, look at and fix common areas of privilege sexies/plauses, and get introduced to SELinux and how It helps when implementing least-privilege.	CYBRScore Scored Labs	Linux System Administration (LSA), Topics: 2, 3, 4, 6 - Cybersecurity Principles (CSP), Topics: ; Operating System Concepts (OSC), Topics: 1, 9	Hyper-V	45 Minutes	1 Hour	46 minutes, 22 seconds	1 minute, 11 seconds
Securing Linux for System Administrators Capstone	Linux environments are ubiquitous in many different sectors, and securing these environments is as important as securing Windows environments. This lab walks you through implementing least-privilege and strong security practices in a Linux environment. Specifically, you will walk through ways to secure your Linux box, look at and fix common areas of privilege issue/spluses, and get introduced to SELinux and how It helps when implementing least-privilege.	CYBRScore Capstones	Linux System Administration (LSA), Topics: 2, 3, 4, 6 - Cybersecurity Principles (CSP), Topics: ; Operating System Concepts (OSC), Topics: 1, 9	Hyper-V	45 Minutes	1 Hour	49 minutes, 8 seconds	56 seconds
Sensitive Information Identification	Students will utilize Data Loss Prevention (DLP) software to identify documents potentially containing sensitive information. They will parse through results and delineate false positives from documents containing legitimate sensitive information.	CYBRScore Labs	Operating Systems Hardening (OSH); Topics: 1, 2, 3, 4, 5, 6, 7, 8, 10, 11	Hyper-V	1 Hour	1 Hour	15 minutes, 16 seconds	19 seconds
Setting up Filters and Queries in Kibana	Students will focus on using filters and queries in Kibana to find indicators of compromise within the network.	CYBRScore Labs	Network Security Administration (NSA); Topics: 2, 5, 7, 8, 9, 10	Hyper-V	1 Hour	1 Hour	1 hour	1 minute, 17 seconds
Setting Up SYSLOG Forwarding From a Windows System	Students will learn how to conduct manual scanning against systems using command line tools such as Netcat then they will login to a discovered system and enable object access verify that auditing to the object is enabled.	CYBRScore Labs	Operating System Concepts (OSC), Topics: 2, 4; Windows System Administration (WSA), Topics: 2, 7	Hyper-V	32 Minutes	1 Hour	36 minutes, 39 seconds	31 seconds
Setting Up SYSLOG Forwarding From a Windows System	Students will learn how to conduct manual scanning against systems using command line tools such as Netcat then they will login to a discovered system and enable object access verify that auditing to the object is enabled.	CYBRScore Scored Labs	Operating System Concepts (OSC), Topics: 2, 4; Windows System Administration (WSA), Topics: 2, 7	Hyper-V	30 Minutes	1 Hour	3 minutes, 11 seconds	56 seconds
Setting Up Zones in a Firewall	As part of a good defense in depth strategy, you have to remember to include control mechanisms at the network level. In this lab, students will configure a pfense firewall to create/isolate various network segments. This effort creates pre-set logical barriers which can be used to organize containment around a detected attacker/mail/clous program and limit any movement.	CYBRScore Labs	Basic Networking, Topics: 3; Network Defense (NDF), Topics: 1a, 1c, 1d, 2b, 4a	Hyper-V	1 Hour	1 Hour	14 minutes, 24 seconds	25 seconds
Setting Up Zones in a Firewall	Students will configure a pfSense Firewall to create/isolate various network segments.	CYBRScore Scored Labs	Basic Networking, Topics: 3; Network Defense (NDF), Topics: 1a, 1c, 1d, 2b, 4a	Hyper-V	1 Hour	1 Hour	31 minutes, 24 seconds	52 seconds
SETUID	This lab exercise is designed to build upon the students understanding of user and file permissions by using the setuid flag.	CYBRScore Labs	Operating Systems Administration (OSA); Topics: 2, 4, 5, 6, 9, 11	vSphere	1 Hour	1 Hour	6 minutes, 10 seconds	6 seconds
Sinkholing C2 Traffic	You have a known C2 Domain that has infected your network. You will create a DNS record and sinkhole all requests to this domain. This will allow your analysts to identify which machines are in your environment and also protect your network by redirecting systems that attempt to contact this domain.	CYBRScore Labs	Basic Networking, Topics: 3; Network Defense (NDF), Topics: 1a, 1c, 1d, 2b, 4a	Hyper-V	46 Minutes	1 Hour	2 minutes, 56 seconds	39 seconds
Snap Exploit		CYBRScore Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10	Hyper-V	45 Minutes	1 Hour	18 minutes, 34 seconds	1 minute, 6 seconds
Snorby Setup and Operation	Onion and to configure and install Snort and Snorby.	CYBRScore Labs	Network Defense (NDF), Topics: 1a, 1c, 1d, 2b, 4a	vSphere	1 Hour	1 Hour		
Snorby Setup and Operation Snorby Setup and Operation	Onion and to configure and install Snort and Snorby. This lab exercise is designed to expose trainees to perform an initial setup for Security Onion and to configure and install Snort and Snorby.	CYBRScore Labs CYBRScore Scored Labs	Network Defense (NDF), Topics: 1a, 1c, 1d, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2b, 4a	vSphere	1 Hour 1 Hour	1 Hour 1 Hour	1 minute, 10 seconds	
	Onion and to conflueue and install snort and Snorby. This lab exercise to designed to expose crainees to perform an initial setup for Security Onion and to configure and install Snort and Snorby. This lab will provide the student with experience in manually installing Snort and its support software, sevel as with configuring Snort to behave as a Network intrusion Detection System. Students will create a custom user account and group to run Snort and create/ferst a custom rule.						1 minute, 10 seconds 28 minutes, 32 seconds	13 seconds
Snorby Setup and Operation	Onion and to configure and install snort and Snorby. This lab exercise designed to expose traines to perform an initial setup for Security Onion and to configure and install snort and Snorby. This lab will provide the student with experience in manually installing Snort and its support software, as well as with configuring Snort to behave as a Network intrusion Detection System Students will create a custom sure account and group to run Snort	CYBRScore Scored Labs	Network Defense (NDF), Topics: 1a, 1c, 1d, 2b, 4a			1 Hour		13 seconds
Snorby Setup and Operation SNORT Configuration and Operation Lab	Onion and to configure and install snort and Snorby. This lab exercise be designed to expose trainees to perform an initial setup for Security Onion and to configure and install snort and Snorby. This lab will provide the student with experience in manually installing Snort and its support software, as well as with configuring Snort to behave as a Network intrusion bettection system as Caustine user accurate and group to run Snort and create/test a custom rule accurate a custom sure accurate and group to run Snort and create/test a custom rule. This lab will provide the student with experience in manually installing Snort and its support software, as well as with configuring Snort to behave as a Network intrusion Detection System Suddents will create a custom sure accurate and group to run Snort	CYBRScore Scored Labs CYBRScore Labs	Network Defense (NDF), Topics: 1a, 1c, 1d, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2b, 4a	vSphere vSphere	1 Hour	1 Hour	28 minutes, 32 seconds	
Snorby Setup and Operation SNORT Configuration and Operation Lab SNORT Configuration and Operation Lab	Onion and to conflueue and install snort and Snorby. This lab exercise to designed to expose crainees to perform an initial setup for Security Onion and to configure and install snort and Snorby. This lab will provide the student with seperience in manually installing Snort and its support software, as well as with configuring Snort to behave as a Network intrusion betection System. Students will create a custom user account and group to run Snort and create/rest a custom rule: a custom user account and group to run Snort and create/rest a custom with experience in manually installing Snort and ats support software, as well as with configuring Snort to behave as a Network intrusion Detection System. Students will create a custom user account and group to run Snort and create/fert a custom rule. Often the security analyst will need to update the existing IDS/F9s (Intrusion) Detection) System to Analysis and event feets. This lab will simulate creating a	CVBRScore Scored Labs CVBRScore Labs CVBRScore Scored Labs	Network Defense (NDF), Topics: 1a, 1c, 1d, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2b, 4a	vSphere vSphere vSphere	1 Hour 1 Hour 3 Hours	1 Hour 1 Hour 4 Hours	28 minutes, 32 seconds 1 hour, 1 minute	22 seconds
Snorby Setup and Operation SNORT Configuration and Operation Lab SNORT Configuration and Operation Lab SNORT Configuration and Operation Lab Snort Signatures, IDS Tuning, and Blocking	onion and to configure and install snort and Snorby. This lab exercise to designed to expose channes to perform an initial setup for Security Onion and to configure and install snort and Snorby. This lab writer to designed to expose channes to perform an initial setup for Security Onion and to configure and install snort and Snorby. This lab will provide the student with experience in manually installing Snort and its support software, as well as with configuring Snort to behave as a Network intrusion and create/test a custom rules a custom rules a custom rules a custom such and create/test a custom rules of the specific configuring Snort to behave as a Network intrusion betection Systems. Students will create a custom use a account and group to run Snort and create/test a custom rule. Often the security nailyst will need to update the existing IDS/PS (intrusion betections) Systems (to handle new threats. This lab will simulate creating a reject and drop rule for a specific traffic type and alert the Snoby SERM when they hit. Often the security nailyst will need to update the existing IDS/PS (intrusion betections) Prevention System) to handle new threats. This lab will simulate creating a reject and drop rule for a specific traffic type and alert the Snoby SERM when they hit. Students will leverage Highing 10 assess posts of various devices on the assigned network. Students will utilize non-traditional scans to attempt avoiding an intrusion Detection.	CYBRScore Labs CYBRScore Labs CYBRScore Labs CYBRScore Labs CYBRScore Labs	Network Defense (NDF), Topics: 1a, 1c, 1d, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2b, 4a	vSphere vSphere vSphere	1 Hour 1 Hour 3 Hours 1 Hours	1 Hour 1 Hour 4 Hours	28 minutes, 32 seconds 1 hour, 1 minute 1 minute, 28 seconds	22 seconds 40 seconds
Snorby Setup and Operation SNORT Configuration and Operation Lab SNORT Configuration and Operation Lab SNORT Signatures, IDS Tuning, and Blocking Snort Signatures, IDS Tuning, and Blocking	Onion and to configure and install snort and Snorby. This lab exercise to designed to expose traines to perform an initial setup for Security Onion and to configure and install snort and Snorby. This lab exercise to designed to expose requires the manually installing Snort and its support software, as well as with configuring Snort to behave as a Network Intrusion Detection System. Students will crease a custom user account and group to run Snort and create/test a custom rule. This lab will provide the student with experience in manually installing Snort and its support software, as well as with configuring Snort to behave as a Network Intrusion Detection System. Students will crease a custom user account and group to run Snort and create/test a custom rule account software, as well as with configuring Snort to behave as a Network Intrusion Detection System Students will crease a custom user account and group to run Snort and create/test a custom rule. Often the security analyst will need to update the existing IDS/IPS (Intrusion Detection)Prevention System) to handle new threats. This lab will simulate creating a reject and drop rule for a specific traffic type and alert the Snothy SEM When they hit. Often the security analyst will need to update the existing IDS/IPS (Intrusion Detection)Prevention System) to handle new threats. This lab will simulate creating a reject and drop rule for a specific traffic type and alert the Snothy SEM When they hit. Students will leverage Hejring 1 to assess ports of various devices on the assigned network. Students will valide everage Hejring 2 to assess ports of various devices on the assigned network. Students will valide everage Hejring 2 to assess ports of various devices on the assigned network.	CYBRScore Scored Labs CYBRScore Labs CYBRScore Scored Labs CYBRScore Scored Labs CYBRScore Labs CYBRScore Labs	Network Defense (NDF), Topics: 1a, 1c, 1d, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2b, 4a	vSphere vSphere vSphere	1 Hour 1 Hour 3 Hours 1 Hour, 9 Minutes 3 Hours	1 Hour 1 Hours 4 Hours 1 Hour	28 minutes, 32 seconds 1 hour, 1 minute 1 minute, 28 seconds 1 hour, 1 minute	22 seconds 40 seconds 1 minute, 27 seconds
Snorby Setup and Operation SNORT Configuration and Operation Lab SNORT Configuration and Operation Lab Snort Signatures, IDS Tuning, and Blocking Snort Signatures, IDS Tuning, and Blocking Specialized Linux Port Scans	Onion and to configure and install snort and Snorby. This lab exercise to designed to expose trainees to perform an initial setup for Security Onion and to configure and install snort and Snorby. This lab exercise to designed to expose crainees to perform an initial setup for Security Onion and to configure and install snort and snorby. This lab will provide the student with experience in manually installing Snort and its support software, as well as with configuring Snort to behave as a Network Intrusion Detection System Caustom rule. This lab will provide the student with experience in manually installing Snort and its support software, as well as with configuring Snort to behave as a Network intrusion Detection System Students will create a custom user accurate and group to run Snort and createfeat a custom rule. Configuring Snort to behave as a Network intrusion Detection System Students will create a custom user accurate and group to run Snort and createfeat a custom rule. Often the security analyst will need to update the existing IDS/IPS (Intrusion Detection)/Prevention System) to handle new threats. This lab will simulate creating a reject and drop united for a specific traffic year and after the Snoty-SEM when they hit. Often the security analyst will need to update the existing IDS/IPS (Intrusion Detection) System (IDS). Students will everage Hignig 3 to assess ports of various devices on the assigned network. Students will cillier non-traditional scans to attempt avoiding an Intrusion Detection System (IDS). In this lab you will put your skills using Squert to the test by performing analysis during a least access cannot be an attack roll to the actual Scannoth.	CYBRScore Labs CYBRScore Labs CYBRScore Labs CYBRScore Labs CYBRScore Labs CYBRScore Scored Labs	Network Defense (NDF), Topics: 1a, 1c, 1d, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2b, 4a Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10	vSphere vSphere vSphere Hyper-V Hyper-V	1 Hour 1 Hour 3 Hours 1 Hour, 9 Minutes 3 Hours 45 Minutes	1 Hour 1 Hours 4 Hours 1 Hour 4 Hours 4 Hours 4 Hours	28 minutes, 32 seconds 1 hour, 1 minute 1 minute, 28 seconds 1 hour, 1 minute 49 minutes, 54 seconds 7 minutes, 34 seconds	22 seconds 40 seconds 1 minute, 27 seconds
Snorby Setup and Operation SNORT Configuration and Operation Lab SNORT Configuration and Operation Lab Snort Signatures, IDS Tuning, and Blocking Snort Signatures, IDS Tuning, and Blocking Specialized Linux Port Scans Specialized Linux Port Scans	Onion and to configure and install snort and Snorby. This lab exercise to designed to expose trainees to perform an initial setup for Security Onion and to configure and install snort and Snorby. This lab exercise to designed to expose crainees to perform an initial setup for Security Onion and to configure and install snort and snorby. This lab will provide the student with experience in manually installing Snort and its support software, as well as with configuring Snort to behave as a Network Intrusion Detection System. Students will crease a custom user account and group to run Snort and creately test a custom rule. This lab will provide the student with experience in manually installing Snort and its support software, as well as with configuring Snort to behave as a Network intrusion Detection System Students will crease extorm user account and group to run Snort and createffers at austion rule. Often the security analyst will need to update the existing IDS/IPS (Intrusion Detection)Prevention System) to handle new threats. This lab will simulate creating a reject and drop rule for a specific traffic year and after the Snoby SEM when they hit. Often the security analyst will need to update the existing IDS/IPS (Intrusion Detection)Prevention System) to handle new threats. This lab will simulate creating a reject and drop rule on randomization store that the substitute of the substitute of the specific traffic year and after the Snoby SEM when they hit. Students will leverage Highing 10 assess ports of various devices on the assigned network. Students will calle enon-traditional scans to attempt avoiding an Intrusion Detection System (IDS). In this lab you will put your skills using Squert to the test by performing analysis during a low attack scansing or the labs to aller your understanding of the infrastructure, not to the labs to aller your understanding of the infrastructure, and to	CYBRScore Scored Labs CYBRScore Labs CYBRScore Scored Labs CYBRScore Labs CYBRScore Labs CYBRScore Scored Labs CYBRScore Scored Labs CYBRScore Network Forensics	Network Defense (NDF), Topics: 1a, 1c, 1d, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2b, 4a Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10 Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10	vSphere vSphere vSphere vSphere Hyper-V Hyper-V Hyper-V	1 Hour 1 Hour 3 Hours 1 Hour, 9 Minutes 3 Hours 45 Minutes 45 Minutes	1 Hour 1 Hours 4 Hours 1 Hour 4 Hours 4 Hours 4 Hours 45 Minutes	28 minutes, 32 seconds 1 hour, 1 minute 1 minute, 28 seconds 1 hour, 1 minute 49 minutes, 54 seconds 7 minutes, 34 seconds	22 seconds 40 seconds 1 minute, 27 seconds 26 seconds 39 seconds
Snorby Setup and Operation SNORT Configuration and Operation Lab SNORT Configuration and Operation Lab Snort Signatures, IDS Tuning, and Blocking Snort Signatures, IDS Tuning, and Blocking Specialized Linux Port Scans Specialized Linux Port Scans Squert Capstone	Online and to configure and install snort and Snorby. This lab exercise is designed to expose traines to perform an initial setup for Security Online and to configure and install snort and Snorby. This lab exercise designed to expose requested in the support of the support	CYBRScore Labs CYBRScore Labs CYBRScore Scored Labs CYBRScore Labs CYBRScore Labs CYBRScore Labs CYBRScore Labs CYBRScore Labs CYBRScore Labs	Network Defense (NDF), Topics: 1a, 1c, 1d, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2b, 4a Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10 Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10 Network Security Administration (NSA); Topics: 2, 5, 7, 8, 9, 10	vSphere vSphere vSphere hyper-V hyper-V hyper-V hyper-V hyper-V	1 Hour 3 Hours 1 Hour, 9 Minutes 3 Hours 45 Minutes 45 Minutes	1 Hour 4 Hours 1 Hour 4 Hours	28 minutes, 32 seconds 1 hour, 1 minute 1 minute, 28 seconds 1 hour, 1 minute 49 minutes, 54 seconds 7 minutes, 34 seconds	22 seconds 40 seconds 1 minute, 27 seconds 26 seconds 39 seconds
Snorby Setup and Operation SNORT Configuration and Operation Lab SNORT Configuration and Operation Lab Snort Signatures, IDS Tuning, and Blocking Snort Signatures, IDS Tuning, and Blocking Snort Signatures, IDS Tuning, and Blocking Specialized Linux Port Scans Specialized Linux Port Scans Specialized Linux Port Scans System Administrator Capstone (Auditing and Log Collection)	Onion and to configure and install snort and Snorby. This lab exercise designed to expose traines to perform an initial setup for Security Onion and to configure and install snort and Snorby. This lab exercise designed to expose craines to perform an initial setup for Security Onion and to configure and install snort and snorty. This lab will provide the student with experience in manually installing Snort and its support software, as well as with configuring Snort to behave as a Network Intrusion Detection System. Students will crease a custom user account and group to run Snort and create/rest a custom rule. This lab will provide the student with experience in manually installing Snort and its support software, as well as with configuring Snort to behave as a Network Intrusion Detection System. Students will crease a custom user account and group to run Snort and create/rest a custom rule. Often the security analyst will need to update the existing IDS/IPS (Intrusion Detection). The special and drop rule or a specific traffic type and alert the Snoty SEM When they little regist and drop rule for a specific traffic type and alert the Snoty SEM When they hit. Often the security analyst will need to update the existing IDS/IPS (Intrusion Detection). Prevention System) to handle new threats. This lab will simulate creating a regist and drop rule for a specific traffic type and alert the Snoty SEM When they hit. Students will leverage Hignig 10 assess ports of various devices on the assigned network. Students will clille on craditional scans to attempt avoiding an intrusion Detection System (IDS). In this lab you will grut your skills using Squert for IDS and in intrusion Detection System (IDS). Students will expect the contraditional scans to attempt avoiding an intrusion Detection System (IDS). A number of technologies exist that work together to protect systems and networks. The real value of your networks and systems rests in the data than retworks carry and reside nystems, also known as hardening, s	CYBRScore Scored Labs CYBRScore Labs CYBRScore Scored Labs CYBRScore Capstones	Network Defense (NDF), Topics: 1a, 1c, 1d, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2b, 4a Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10 Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10 Network Security Administration (NSA); Topics: 2, 5, 7, 8, 9, 10 Operating System Concepts (OSC), Topics: 2, 4, Windows System Administration (WSA), Topics: 2, 7, 8, 9, 10 Operating System Concepts (OSC), Topics: 2, 4, 8, Windows System Administration (WSA), Topics: 2, 4, 8	vSphere vSphere vSphere hyperv hyperv hyperv hyperv hyperv hyperv hyperv	1 Hour 1 Hour 3 Hours 1 Hour, 9 Minutes 3 Hours 45 Minutes 45 Minutes 1 Hour 1 Hour, 30 Minutes	1 Hour 1 Hour 4 Hours 1 Hour 4 Hours 4 Hours 4 Hours 4 Hours 4 Minutes 45 Minutes 1 Hour, 30 Minutes	28 minutes, 32 seconds 1 hour, 1 minute 1 minute, 28 seconds 1 hour, 1 minute 49 minutes, 54 seconds 7 minutes, 43 seconds 37 minutes, 37 seconds	22 seconds 40 seconds 1 minute, 27 seconds 26 seconds 39 seconds 2 minutes, 12 seconds
Snorby Setup and Operation SNORT Configuration and Operation Lab SNORT Configuration and Operation Lab Snort Signatures, IDS Tuning, and Blocking Snort Signatures, IDS Tuning, and Blocking Specialized Linux Port Scans Specialized Linux Port Scans Squert Capstone System Administrator Capstone (Auditing and Log Collection) System Hardening	Onion and to configure and install snort and Snorby. This lab exercise designed to expose traines to perform an initial setup for Security Onion and to configure and install snort and Snorby. This lab exercise designed to expose traines to perform an initial setup for Security Onion and to configure and install snort and snorby. This lab will provide the student with experience in manually installing Snort and its support software, as well as with configuring Snort to behave as a Network Intrusion Detection System. Students will crease a custom user account and group to run Snort and create/rest a custom rule. This lab will provide the student with experience in manually installing Snort and its support software, as well as with configuring Snort to behave as a Network intrusion Detection System Students will crease a custom user account and group to run Snort and create/fest a custom rule. This lab will provide analyst will need to update the existing IDS/IPS (Intrusion Detection). Prevention System) to handle new threats. This lab will simulate creating a reject and drop under to a specific traility by and alert the Soloy SEM when they hit. Often the security analyst will need to update the existing IDS/IPS (Intrusion Detection). Prevention System) to handle new threats. This lab will simulate creating a reject and drop under a specific traility to handle new threats. This lab will simulate creating a reject and drop under a specific traility by and alert the Soloy SEM when they hit. Students will leverage Highing 10 assess ports of various devices on the assigned network. Students will critice non-traditional scans to attempt avoiding an Intrusion Detection System (IDS). In this lab you will put your skills using Squert to the test by performing analysis during a live attack scenario. You are tasked with monitoring Squert for IDS alerts as an attack rolls no your infrastructure. You have been provided with a simple network map in the real value of your releasts and attacks. A number of technologies	CYBRScore Labs CYBRScore Labs CYBRScore Scored Labs CYBRScore Labs	Network Defense (NDF), Topics: 1a, 1c, 1d, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2b, 4a Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10 Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10 Network Security Administration (NSA); Topics: 2, 5, 7, 8, 9, 10 Operating System Concepts (OSC), Topics: 2, 4; Windows System Administration (WSA), Topics: 5, 10, 13 Operating Systems Hardening (OSH), Topics: 2, 4, 8; Windows System Administration (WSA), Operating Systems Hardening (OSH), Topics: 2, 4, 8; Windows System Administration (WSA), Operating Systems Hardening (OSH), Topics: 2, 4, 8; Windows System Administration (WSA), Operating Systems Hardening (OSH), Topics: 2, 4, 8; Windows System Administration (WSA), Operating Systems Hardening (OSH), Topics: 2, 4, 8; Windows System Administration (WSA), Operating Systems Hardening (OSH), Topics: 2, 4, 8; Windows System Administration (WSA),	vSphere vSphere vSphere vSphere Hyper-V Hyper-V Hyper-V Hyper-V Hyper-V Hyper-V Hyper-V Hyper-V	1 Hour 3 Hours 1 Hour, 9 Minutes 3 Hours 45 Minutes 45 Minutes 1 Hour 1 Hour, 30 Minutes	1 Hour 1 Hours 1 Hours 1 Hours 4 Hours 4 Hours 45 Minutes 45 Minutes 24 Hour, 30 Minutes 1 Hour, 30 Minutes	28 minutes, 32 seconds 1 hour, 1 minute 1 minute, 28 seconds 1 hour, 1 minute 49 minutes, 54 seconds 7 minutes, 53 seconds 37 minutes, 37 seconds	22 seconds 40 seconds 1 minute, 27 seconds 26 seconds 27 seconds 28 seconds 29 seconds 2 minutes, 12 seconds
Snorby Setup and Operation SNORT Configuration and Operation Lab SNORT Configuration and Operation Lab SNORT Configuration and Operation Lab Snort Signatures, IDS Tuning, and Blocking Snort Signatures, IDS Tuning, and Blocking Specialized Linux Port Scans Specialized Linux Port Scans Squert Capstone System Administrator Capstone (Auditing and Log Collection) System Hardening System Hardening	Onion and to configure and install snort and Snorby. This lab exercise designed to expose traines to perform an initial setup for Security Onion and to configure and install snort and Snorby. This lab exercise designed to expose requested to prevent and to configure and install snort and Snorby. This lab will provide the student with experience in manually installing Snort and its support software, as well as with configuring Snort to behave as a Network Intrusion Detection System. Students will create a custom user account and group to run Snort and create/fest a custom rule. This lab will provide the student will happerine so in manually installing Snort and its support so the student will be apperine so in manually installing Snort and its lab will sometime to the student will be a support to the student will be a support to run Snort and create/fest a custom rule. Often the security snalyst will need to update the existing IDS/IPS (Intrusion Detection/Prevention System) to handle new theats. This lab will simulate creating a erget and drop rule for a specific traffic type and alert the Snody SEM when they hit. Often the security analyst will need to update the existing IDS/IPS (Intrusion Detection/Prevention System) to handle new threats. This lab will simulate creating a reject and drop rule for a specific traffic type and alert the Snody SEM when they hit. Students will everage Heigral 3 to assess ports of various devices on the assigned network. Students will everage Heigral 3 to assess ports of various devices on the assigned network. Students will everage Heigral 3 to assess ports of various devices on the assigned network. Students will everage Heigral 3 to assess ports of various devices on the assigned network. Students will everage Heigral 3 to assess ports of various devices on the assigned network Students will everage Heigral 3 to assess ports of various devices on the assigned network Students will everage Heigral 3 to assess ports of various devices on the assigned network Students will	CYBRScore Scored Labs CYBRScore Labs	Network Defense (NDF), Topics: 1a, 1c, 1d, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2b, 4a Network Defense (NDF), Topics: 1a, 1c, 1d, 2b, 4a Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10 Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10 Network Security Administration (NSA); Topics: 2, 5, 7, 8, 9, 10 Operating Systems Concepts (OSC), Topics: 2, 4, 8; Windows System Administration (WSA), Topics: 5, 10, 13 Operating Systems Hardening (OSH), Topics: 2, 4, 8; Windows System Administration (WSA), Topics: 5, 10, 13	vSphere vSphere vSphere vSphere hyper-v hyper-v hyper-v hyper-v hyper-v hyper-v hyper-v vSphere	1 Hour 1 Hours 1 Hour, 9 Minutes 1 Hour, 9 Minutes 45 Minutes 45 Minutes 1 Hour 1 Hour 1 Hour	1 Hour 4 Hours 1 Hour 4 Hours 4 Hours 4 Hours 45 Minutes 45 Minutes 1 Hour, 30 Minutes 1 Hour	28 minutes, 32 seconds 1 hour, 1 minute 1 minute, 28 seconds 1 hour, 1 minute 49 minutes, 54 seconds 7 minutes, 37 seconds 37 minutes, 37 seconds	22 seconds 40 seconds 1 minute, 27 seconds 26 seconds 39 seconds 2 minutes, 12 seconds 1 minute, 24 seconds

Threat Designation	Students will conduct scans against a web server, a file share, a printer and a user's host device. The student will identify specific threats posed to the system. Students will then an a network and identify potential points of ingress (open ports, etc) that could cause compromise to the system.	CYBRScore Labs	Operating Systems Hardening (OSH); Topics: 1, 2, 3, 4, 5, 6, 7, 8, 10, 11	Hyper-V	1 Hour	1 Hour	16 minutes, 57 seconds	35 seconds
Threat Designation	Students will conduct scans against a web server, a file share, a printer and a user's host device. The student will identify specific threats posed to the system. Students will then an a network and identify potential points of ingress (open ports, etc) that could cause compromise to the system.	CYBRScore Scored Labs	Network Security Administration (NSA); Topics: 2, 5, 7, 8, 9, 10	Hyper-V	1 Hour	1 Hour	25 minutes, 29 seconds	51 seconds
Tweaking Firewall Rules for Detection	Students will use organizational firewall for monitoring, detecting and auditing traffic on the network. Students will then configure log traffic of interest forwarded to a syslog server.	CYBRScore Labs	Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a	Hyper-V	3 Hours	4 Hours	27 minutes, 55 seconds	31 seconds
Use pfTop to Analyze Network Traffic	Students will use pTrop, a network traffic monitoring/statistics julipin used in pSense, to analyze and monitor network traffic. They will walk through the steps of performing a detailed investigation to determine what type of traffic is occurring across the exercise network. Fanility, with the use of visualization tools they will be able to Interher analyze network traffic statistics and learn how visuals can quickly aid in the incident response process.	CYBRScore Labs	Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a	Hyper-V	40 Minutes	1 Hour	46 seconds	29 seconds
Use pfTop to Analyze Network Traffic	Students will use pfTop, a network traffic monitoring/statistics plugin used in pfSense, to analyze and monitor network traffic. They will walk through the steps of performing a detailed investigation to determine what type of traffic is occurring across the exercise network. Finally, with the use of use visualization tools they will be able to further analyze network traffic statistics and learn how visuals can quickly aide in the incident response process.	CYBRScore Network Forensics	Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a	Hyper-V	40 Minutes	1 Hour	18 minutes, 33 seconds	1 minute, 11 seconds
Use pfTop to Analyze Network Traffic	Students will use pfTop, a network traffic monitoring/statistics plugin used in pfSense, to analyze and monitor network traffic. They will walk through the steps of performing a detailed investigation to determine what type of traffic is cocurring across the secretice network. Finally, with the use of use visualization tools they will be able to further analyze network traffic statistics and learn how visuals can quickly alde in the incident response process.	CYBRScore Scored Labs	Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a	Hyper-V	40 Minutes	1 Hour	27 minutes, 52 seconds	49 seconds
Use pfTop to Analyze Network Traffic Capstone	Students will use pfTop, a network traffic monitoring/statistics plugin used in pfSense, to analyze and monitor network traffic. They will walk through the steps of performing a detailed investigation to determine what type of traffic is occurring across the secretic network. Finally, with the use of use visualization tools they will be able to further analyze network traffic statistics and learn how visuals can quickly aide in the incident response process.	CYBRScore Capstones	Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a	Hyper-V	40 Minutes	1 Hour	15 minutes, 47 seconds	2 minutes, 6 seconds
Using PowerShell to Analyze a System	Students will be using Power Shell to search for running processes, users and tasks on local and remote systems in the user environment.	CYBRScore Labs	Operating Systems Hardening (OSH); Topics: 1, 2, 3, 4, 5, 6, 7, 8, 10, 11	Hyper-V	1 Hour	1 Hour	26 minutes, 36 seconds	19 seconds
Using Snort and Wireshark to Analyze Traffic	In this lab, we will replicate the actions involved in simple network traffic analysis in order to detect suspicious activity. Students will be exposed to Wireshark and Snort.	CYBRScore Labs	Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a	Hyper-V	1 Hour	1 Hour	12 minutes, 26 seconds	36 seconds
Using Snort and Wireshark to Analyze Traffic	In this lab we will replicate the need for Analysts to be able to analyze network traffic an detect suspicious activity. Tools like Wireshark and Snort can be utilized to read, capture and analyze traffic.		Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a	Hyper-V	1 Hour	1 Hour	25 minutes, 39 seconds	1 minute, 25 seconds
Using Snort and Wireshark to Analyze Traffic	In this lab we will replicate the need for Analysts to be able to analyze network traffic an detect suspicious activity. Tools like Wireshark and Snort can be utilized to read, capture and analyze traffic.	d , CYBRScore Scored Labs	Network Defense (NDF), Topics: 1a, 1c, 1d, 2a, 2b, 4a	Hyper-V	45 Minutes	1 Hour, 30 Minutes	29 minutes, 19 seconds	1 minute, 22 seconds
Validate Indications of Compromise: Analysis of PE File	Malware authors frequently use certain functions, symbols and other tools as a way of building and obfuscating the true nature of their executables. As part of the Detect phase you should be able to detect evidence of and determine if an executable is mallicious, and be able to provide information that can be used to create signatures to detect it in the future.	CYBRScore Labs	Software Security Analysis (SSA); Topics: 1, 2, 3, 4, 5	Hyper-V	30 Minutes	30 Minutes	12 minutes, 13 seconds	35 seconds
Verify Attributes of Identified SilentBanker Intrusion	Students will verify attributes of the identified intrusion with existing internal and external intrusion, pattern and malware databases.	CYBRScore Labs	Software Security Analysis (SSA); Topics: 1, 2, 3, 4, 5	Hyper-V	1 Hour	1 Hour	2 minutes, 6 seconds	18 seconds
Verify Attributes of Identified SilentBanker Intrusion	Students will verify attributes of the identified intrusion with existing internal and external intrusion, pattern and malware databases.	CYBRScore Scored Labs	Software Security Analysis (SSA); Topics: 1, 2, 3, 4, 5	Hyper-V	1 Hour	1 Hour	32 minutes, 37 seconds	1 minute, 16 seconds
Verify Attributes of Intrusion Through Additional Analysis	Students will validate potential intrusions identified by monitoring systems and perform	CYBRScore Labs	Operating Systems Hardening (OSH); Topics: 1, 2, 3, 4, 5, 6, 7, 8, 10, 11	Hyper-V	30 Minutes	1 Hour	38 minutes, 55 seconds	25 seconds
Verifying Hotfixes	additional analysis. Software patches repair bugs or vulnerabilities found in software programs. Patches are simply updates that fix a problem or vulnerability within a program. Sometimes, instead of just releasing a patch, vendors will release an upgrade version of their software, although they may refer to the upgrade as a patch. In this lab, you will learn how to identify currently installed patches, manually install a hotfix and configure a work around.	CYBRScore Labs	Operating Systems Hardening (OSH); Topics: 1, 2, 3, 4, 5, 6, 7, 8, 10, 11	Hyper-V	1 Hour	1 Hour	5 minutes, 54 seconds	20 seconds
Virtualization	This lab is designed to provide students with the experience of creating a simple virtual machine (VM) using VMware Player.	CYBRScore Labs	Operating Systems Hardening (OSH); Topics: 1, 2, 3, 4, 5, 6, 7, 8, 10, 11	vSphere	1 Hour	1 Hour		
Vulnerability Analysis/Protection	Students will use OpenVAS to do a vulnerability analysis. Students will then identify applicable vulnerabilities and protect their system(s) against them.	CYBRScore Labs	Operating Systems Hardening (OSH), Topics: 11; IT Systems Components (ISC), Topics: 13	Hyper-V	1 Hour, 30 Minutes	1 Hour, 30 Minutes	55 minutes, 57 seconds	32 seconds
Vulnerability Analysis/Protection	applicable volinerabilities and protect their system(s) against tiern. Students will use Open/AS to do a vulnerabilities analysis. Students will then identify applicable vulnerabilities and protect their system(s) against them.	CYBRScore Scored Labs	Operating Systems Hardening (OSH), Topics: 11; IT Systems Components (ISC), Topics: 13	Hyper-V	3 Hours	4 Hours	35 minutes, 55 seconds	1 minute, 20 seconds
Vulnerability Analyst Capstone	Students will identify if a vulnerability is present in the systems and remediate the	CYBRScore Scored Labs	Operating Systems Hardening (OSH), Topics: 11; IT Systems Components (ISC), Topics: 13	Hyper-V	1 Hour, 7 Minutes	2 Hours	36 minutes, 25 seconds	54 seconds
Vulnerability Assessment Analyst - Blue Team	vulnerability if necessary. This assessment is one of three, and is focused specifically on items related to Blue Team	1 CYBRScore	Assessment - Covers dozens of KU	Hyper-V	45 Minutes	1 Hour	24 minutes, 54 seconds	2 minutes, 23 seconds
Vulnerability Assessment Analyst - Intelligence Gathering	operations. This assessment is one of three and is focused specifically on items related to vulnerability assessments. In this assessment, you will focus on using scanning and enumeration techniques to gather information to be used in your analysis.	CYBRScore	Assessment - Covers dozens of KU	Hyper-V	45 Minutes	1 Hour	22 minutes, 53 seconds	2 minutes, 7 seconds
Vulnerability Assessment Analyst - Intelligence Gathering (Renet)	This assessment is one of three and is focused specifically on items related to vulnerability assessments. In this assessment, you will focus on using scanning and enumeration techniques to gather information to be used in your analysis.	CYBRScore	Assessment - Covers dozens of KU	Hyper-V	45 Minutes	1 Hour	2 minutes, 22 seconds	2 minutes, 3 seconds
Vulnerability Assessment Analyst - Red Team	This assessment is one of three, and is focused specifically on items related to Red Team operations.	CYBRScore	Assessment - Covers dozens of KU	Hyper-V	45 Minutes	1 Hour	34 minutes, 16 seconds	2 minutes, 22 seconds
Vulnerability Identification and Remediation	Learners will use Nmap and Open/AS/Greenbone Vulnerability Scanner to confirm old vulnerable systems and to also discover new ones. They will perform a risk analysis of the findings and determine steps to be taken to miligate the issues discovered. Finally, armed with a previously completed audit report as an example, they will fill out the necessary audit documentation to provide details on their findings and to add any suggested miligations.	CYBRScore Labs	Operating Systems Hardening (OSH), Topics: 11; IT Systems Components (ISC), Topics: 13	Hyper-V	1 Hour	1 Hour, 30 Minutes	5 minutes, 56 seconds	Z8 seconds
Vulnerability Identification and Remediation	Learners will use Nimap and Open/AS/Greenbone Vulnerability Scanner to confirm old vulnerable systems and to also discover new ones. They will perform a risk analysis of the findings and determine steps to be taken to militigate the Issues discovered. Finally, armed with a previously completed audit report as an example, they will fill out the necessary audit documentation to provide details on their findings and to add any suggested militigations.	CYBRScore Scored Labs	Operating Systems Hardening (OSH), Topics: 11; IT Systems Components (ISC), Topics: 13	Hyper-V	1 Hour	1 Hour, 30 Minutes	58 minutes, 14 seconds	1 minute, 24 seconds
Vulnerability Proof of Concept and Remediation	Students will identify if a vulnerability is present in the systems and remediate the vulnerability if necessary.	CYBRScore Scored Labs	Operating Systems Hardening (OSH), Topics: 11; IT Systems Components (ISC), Topics: 13	Hyper-V	1 Hour, 7 Minutes	2 Hours	42 minutes, 11 seconds	42 seconds
	vulneraumity in necessary.							

Vulnerability Scan Analysis	Students will run a Core Impact or Nessus Scan and identify vulnerabilities. Students will then view the report and prioritize vulnerabilities according to risk.	CYBRScore Labs	Operating Systems Hardening (OSH), Topics: 11; IT Systems Components (ISC), Topics: 13	Hyper-V	2 Hours	2 Hours	23 minutes, 59 seconds	38 seconds
Vulnerability Scan Analysis	Students will run a Core Impact or Nessus Scan and identify vulnerabilities. Students will then view the report and prioritize vulnerabilities according to risk.	CYBRScore Scored Labs	Operating Systems Hardening (OSH), Topics: 11; IT Systems Components (ISC), Topics: 13	Hyper-V	3 Hours	4 Hours	22 minutes, 30 seconds	1 minute, 29 seconds
Vulnerability Scanner Set-up and Configuration	Students will setup and configure Core Impact in preparation of a vulnerability scan against an internal network.	CYBRScore Labs	Operating Systems Hardening (OSH), Topics: 11; IT Systems Components (ISC), Topics: 13	Hyper-V	1 Hour	1 Hour	11 minutes, 44 seconds	1 minute, 12 seconds
Vulnerability Scanner Set-up and Configuration	Students will setup and configure Core Impact in preparation of a vulnerability scan against an internal network.	CYBRScore Scored Labs	Operating Systems Hardening (OSH), Topics: 11; IT Systems Components (ISC), Topics: 13	Hyper-V	1 Hour	1 Hour	22 minutes, 30 seconds	1 minute, 31 seconds
Vulnerability Scanner Set-up and Configuration, Pt. 2	Students will utilize OpenVAS to identify hosts on a network and assess their vulnerabilities.	CYBRScore Labs	Operating Systems Hardening (OSH), Topics: 11; IT Systems Components (ISC), Topics: 13	Hyper-V	1 Hour	1 Hour	21 minutes, 4 seconds	29 seconds
Web 201 - Capstone	In this lab, you will be faced with a set of unknown web applications that have a number	CYBRScore Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10 - Web Application Security - all topics	Hyper-V	8 Hours	10 Hours	12 minutes, 18 seconds	38 seconds
Web 201 - Lab 1: Recon Tools	knowing what the application consists of. These tools will help to give a more complete picture of this at the beginning.	CYBRScore Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10 - Web Application Security - all topics	Hyper-V	1 Hour	1 Hour	20 minutes, 13 seconds	17 seconds
Web 201 - Lab 2.1: Detecting and Exploiting Hard to Find SQL injections	In this lab, we will look at a few different examples of how our input could be processed or blocked. We will explore several different evasion techniques to achieve our goals.	CYBRScore Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10 - Web Application Security - all topics	Hyper-V	1 Hour	1 Hour	18 minutes, 39 seconds	26 seconds
Web 201 - Lab 2.2: Advanced Sqlmap	In this lab we will explore some more advanced features of the SQL injection tool sqimap, that will enable us to use it to exploit more difficult SQL injection vulnerabilities. Cases in which the default usage of the tool will not be able to find or exploit the vulnerabilities.	CYBRScore Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10 - Web Application Security - all topics	Hyper-V	1 Hour, 30 Minutes	1 Hour, 30 Minutes	8 minutes, 53 seconds	22 seconds
Web 201 - Lab 2.3: Manual Blind SQL Injection	In this lab, we will cover how to exploit Blind SQL Injections manually. Typically, if you come across a Blind SQL Injection, you would use spimap to exilirate the data. However, smeetimes you cannot get samples to find the injection point, or you don't have it available on the system you are using, or perhaps it would be caught by an intrusion Detection System and you need to be sealthy. In these cases, it is important to know how to exploit these issues manually.	CYBRScore Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10 - Web Application Security - all topics	Hyper-V	1 Hour, 30 Minutes	1 Hour, 30 Minutes	1 minute, 14 seconds	18 seconds
Web 201 - Lab 2.4: NoSQL Injection	In this lab, we will explore a few aspects of NoSQL injections. We will be using a Node.js application as an example, with a MongoDB backend.	CYBRScore Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10 - Web Application Security - all topics	Hyper-V	30 Minutes	30 Minutes	33 seconds	18 seconds
Web 201 - Lab 3.1: Cross Site Scripting Filter Evasion	In this lab, we will explore a few different filters and how to evade them to display an alert box. We will then finish by implementing a cookie stealer in a place where filters are in place.	CYBRScore Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10 - Web Application Security - all topics	Hyper-V	1 Hour	1 Hour	10 minutes, 37 seconds	20 seconds
Web 201 - Lab 3.2: Exploiting Misconfigured CORS	In this lab we will compare and constrast default operation, secure configuration of CORS, and misconfigured CORS.	CYBRScore Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10 - Web Application Security - all topics	Hyper-V	30 Minutes	30 Minutes	1 minute, 22 seconds	29 seconds
Web 201 - Lab 4: Advanced OS Command Injection	in the first part of this lab, we will explore some methods of evading the filters and still accomplishing the goal. In the second part of the lab, we will make the exploit even more difficult by leaving the filters in place as well as removing the output, making it a blind OS Command Injection.		Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10 - Web Application Security - all topics	Hyper-V	1 Hour	1 Hour	47 seconds	18 seconds
Web 201 - Lab 5: Advanced Local File Inclusion	As an attacker, the two main goals in exploiting LT are typically to expose secret or sensitive information or to cause attribut ools to be executed, giving them remote command execution. For the former goal, you may want the source code for the application, which is made difficult in that the code is interpreted and executed and not directly displayed. For the latter goal, one of the main hurdles is getting your own code onto the sever itself in order to be included by the application.	CYBRScore Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10 - Web Application Security - all topics	Hyper-V	1 Hour	1 Hour	27 minutes, 34 seconds	25 seconds
Web 201 - Lab 6: Advanced CSRF	Cross Site Request Forgery (CSRF) is when an attacker can induce a victim to make a nequest to a site they are already authenticated to and cause them to make changes that they otherwise would's want to do. For example, an attacker could cause the victim to change their password or their contact email without their knowledge. The best modern defence against CSRF is the ant-CSRF token, a random token generated per session that must be submitted with each request in order to ensure that the legitimate client is the course of the request. Since the attacker han own yor knowing this token, the attacker cannot cause the victim to submit it along with the change request. Nowever, there is at least one case where that sin't true. That is, is the CSRF protected site alon has a Cross Site Scripting vulnerability on a page that contains the token. An attacker may be able to leverage the XSS to leak the CSRF token, at which point the CSRF attack can be carried out. That is what we will explore in this lab.	CYBRScore Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10 - Web Application Security - all topics	Hyper-V	1 Hour	1 Hour	9 minutes, 21 seconds	18 seconds
Web 201 - Lab 7.1: XXE to Obtain Arbitrary Files	In this lab, we will explore the basic limitations of XXE and techniques that can be used in a PHP web application to overcome them.	CYBRScore Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10 - Web Application Security - all topics	Hyper-V	30 Minutes	30 Minutes		
Web 201 - Lab 7.2: Out of Band XXE Attacks	Sometimes there is an XML External Entity vulnerability, but exploiting it doesn't send any data back within the web application. If this is the case, it not only may be hard to detect that the issue exists, but it will also be difficult to exploit the issue.	CYBRScore Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10 - Web Application Security - all topics	Hyper-V	45 Minutes	45 Minutes	41 seconds	18 seconds
Web 201 - Lab 8: Server Side Request Forgery	In this example we will be faced with a web application that will simply open whatever resource you specify, with increasingly strict restrictions. However, in a real application that his issue will likely be a bit harder of lond. It might surface in an application that is acting as a proxy for some resource or it might simply be retrieving resources from a private retwork. In any case, some of the restrictions that we will explore may be natural restrictions based on how the application is implemented, or may be steps taken to secure the functionality.	CYBRScore Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10 - Web Application Security - all topics	Hyper-V	45 Minutes	45 Minutes		
Web 201 - Lab 9: Insecure Deserialization in Python and Java	Insecure Describilation occurs when the web application takes a serialized object, that has been exposed to the user and possibly tampered with, and converts it back into an object of the property of the pr		Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10 - Web Application Security - all topics	Hyper-V	1 Hour	1 Hour	15 minutes, 7 seconds	20 seconds
WEB241 Environment Setup	the WEB241 Labs.	CYBRScore Labs	Web Application Security (WAS) - all topics - Secure Programming Practices (SSP) (all)	Hyper-V	100 Hours	100 Hours		
WEB241: Hardening PHP Web Apps - Broken Access Control	This lab teaches methods to deploy basic access control in a web application written in PHP.	CYBRScore Labs	Web Application Security (WAS) - all topics - Secure Programming Practices (SSP) (all)	Hyper-V	45 Minutes	45 Minutes		
WEB241: Hardening PHP Web Apps - Broken Access Control	This lab teaches methods to deploy basic access control in a web application written in PHP.	CYBRScore Scored Labs	Web Application Security (WAS) - all topics - Secure Programming Practices (SSP) (all)	Hyper-V	45 Minutes	45 Minutes	17 minutes, 1 second	1 minute, 6 seconds

WEB241: Hardening PHP Web Apps - Broken Authentication	This lab teaches methods to secure the authentication methods in a web application written in PHP.	CYBRScore Labs	Web Application Security (WAS) - all topics - Secure Programming Practices (SSP) (all)	Hyper-V	1 Hour	1 Hour		
WEB241: Hardening PHP Web Apps - Broken Authentication	This lab teaches methods to secure the authentication methods in a web application written in PHP.	CYBRScore Scored Labs	Web Application Security (WAS) - all topics - Secure Programming Practices (SSP) (all)	Hyper-V	1 Hour	1 Hour	7 minutes, 38 seconds	1 minute, 3 seconds
WEB241: Hardening PHP Web Apps - Capstone	This lab is a capstone event for the Web 241 labs. It incorporates many vulnerabilities and will walk the student through which ones to fix.	CYBRScore Labs	Web Application Security (WAS) - all topics - Secure Programming Practices (SSP) (all)	Hyper-V	2 Hours	2 Hours		
WEB241: Hardening PHP Web Apps - Cross Site Scripting	This lab teaches methods to secure web applications written in PHP against XSS attacks.	CYBRScore Labs	Web Application Security (WAS) - all topics - Secure Programming Practices (SSP) (all)	Hyper-V	45 Minutes	1 Hour	16 minutes, 15 seconds	26 seconds
WEB241: Hardening PHP Web Apps - CSRF	This lab teaches methods to secure web applications written in PHP against Cross Site Request Forgery attacks.	CYBRScore Labs	Web Application Security (WAS) - all topics - Secure Programming Practices (SSP) (all)	Hyper-V	30 Minutes	45 Minutes		
WEB241: Hardening PHP Web Apps - CSRF	This lab teaches methods to secure web applications written in PHP against Cross Site Request Forgery attacks.	CYBRScore Scored Labs	Web Application Security (WAS) - all topics - Secure Programming Practices (SSP) (all)	Hyper-V	30 Minutes	45 Minutes	5 minutes, 28 seconds	43 seconds
WEB241: Hardening PHP Web Apps - File Uploads	This lab teaches methods to secure web applications written in PHP with respect to file upload capabilities.	CYBRScore Labs	Web Application Security (WAS) - all topics - Secure Programming Practices (SSP) (all)	Hyper-V	45 Minutes	1 Hour		
WEB241: Hardening PHP Web Apps - OS Command Injection	This lab teaches methods to secure a web application written in PHP against OS Command Injection attacks.	CYBRScore Labs	Web Application Security (WAS) - all topics - Secure Programming Practices (SSP) (all)	Hyper-V	30 Minutes	30 Minutes		
WEB241: Hardening PHP Web Apps - OS Command Injection	This lab teaches methods to secure a web application written in PHP against OS Command Injection attacks.	CYBRScore Scored Labs	Web Application Security (WAS) - all topics - Secure Programming Practices (SSP) (all)	Hyper-V	30 Minutes	30 Minutes	20 minutes, 57 seconds	1 minute, 2 seconds
WEB241: Hardening PHP Web Apps - Password Hashing	This lab teaches how to properly use password hashing in a PHP web application.	CYBRScore Labs	Web Application Security (WAS) - all topics - Secure Programming Practices (SSP) (all)	Hyper-V	30 Minutes	30 Minutes		
WEB241: Hardening PHP Web Apps - Password Hashing	This lab teaches how to properly use password hashing in a PHP web application.	CYBRScore Scored Labs	Web Application Security (WAS) - all topics - Secure Programming Practices (SSP) (all)	Hyper-V	30 Minutes	30 Minutes	7 minutes, 34 seconds	53 seconds
WEB241: Hardening PHP Web Apps - Path Traversal and LFI	This lab teaches methods to prevent Path Traversal and Local File Inclusion in a web application written in PHP.	CYBRScore Labs	Web Application Security (WAS) - all topics - Secure Programming Practices (SSP) (all)	Hyper-V	30 Minutes	30 Minutes		
WEB241: Hardening PHP Web Apps - Path Traversal and LFI	This lab teaches methods to prevent Path Traversal and Local File Inclusion in a web application written in PHP.	CYBRScore Scored Labs	Web Application Security (WAS) - all topics - Secure Programming Practices (SSP) (all)	Hyper-V	30 Minutes	30 Minutes	15 minutes, 40 seconds	54 seconds
WEB241: Hardening PHP Web Apps - PHP Configuration	This lab teaches methods to secure the PHP configuration for web applications written in PHP.	CYBRScore Labs	Web Application Security (WAS) - all topics - Secure Programming Practices (SSP) (all)	Hyper-V	30 Minutes	30 Minutes		
WEB241: Hardening PHP Web Apps - Secure Deserialization	This lab teaches methods to secure web applications written in PHP against insecure Deserialization attacks.	CYBRScore Labs	Web Application Security (WAS) - all topics - Secure Programming Practices (SSP) (all)	Hyper-V	30 Minutes	45 Minutes		
WEB241: Hardening PHP Web Apps - Sensitive Data Exposure		CYBRScore Labs	Web Application Security (WAS) - all topics - Secure Programming Practices (SSP) (all)	Hyper-V	30 Minutes	30 Minutes	25 minutes, 1 second	26 seconds
WEB241: Hardening PHP Web Apps - SQL Injection	Injection attacks.	CYBRScore Labs	Web Application Security (WAS) - all topics - Secure Programming Practices (SSP) (all)	Hyper-V	45 Minutes	45 Minutes	6 minutes, 24 seconds	21 seconds
WEB241: Hardening PHP Web Apps - Two Factor Authentication	This lab teaches how to deploy Google Authenticator in a PHP web application in order to deploy Two Factor Authentication.	CYBRScore Labs	Web Application Security (WAS) - all topics - Secure Programming Practices (SSP) (all)	Hyper-V	30 Minutes	30 Minutes		
WEB241: Hardening PHP Web Apps - XXE	This lab teaches methods to secure a web application written in PHP against XXE attacks.	CYBRScore Labs	Web Application Security (WAS) - all topics - Secure Programming Practices (SSP) (all)	Hyper-V	30 Minutes	30 Minutes	11 minutes, 46 seconds	28 seconds
WebApp Attack PCAP Analysis	In this lab you will analyze a capture file of a web application attack in order to identify the attack vector and deduce the vulnerability the attack exploited.	CYBRScore Labs	Vulnerability Analysis (VLA); Topics: 1, 3, 4, 5, 6, 7, 8, 10	Hyper-V	1 Hour, 14 Minutes	45 Minutes		
WebApp Attack PCAP Analysis	In this lab you will analyze a capture file of a web application attack in order to identify the attack vector and deduce the vulnerability the attack exploited.	CYBRScore Scored Labs	Vulnerability Analysis (VLA); Topics: 1, 3, 4, 5, 6, 7, 8, 10	Hyper-V	30 Minutes	45 Minutes	51 minutes, 53 seconds	1 minute, 31 seconds
Web Recon and SQLi - Capstone	In this lab, you will be faced with a web applications that has a number of vulnerabilities. Your job will be to exploit each of these in turn to achieve the end objective.	CYBRScore Labs		Hyper-V	1 Hour	1 Hour 30 Minutes		
Whitelist Comparison	Students are provided a whitelist of applications allowed for installation on a system. Students will compare the list against multiple hosts and remove the installed applications which are not on the list.	CYBRScore Labs	Operating Systems Hardening (OSH); Topics: 1, 2, 3, 4, 5, 6, 7, 8, 10, 11	Hyper-V	1 Hour	1 Hour	3 minutes, 8 seconds	31 seconds
Whitelist IP Address from IDS Alerts	Students will whitelist the approved scanning device so that no security alerts are generated from the host.	CYBRScore Labs	Operating Systems Hardening (OSH); Topics: 1, 2, 3, 4, 5, 6, 7, 8, 10, 11	Hyper-V	1 Hour	1 Hour	24 minutes, 6 seconds	28 seconds
Whitelisting & Suspicious File Verification	Students will become familiar with procedures used in the validation of suspicious files. During the course of the lab the student will generate a system-level baseline using a command line file hash tool, followed by checking new/unknown files against whitelists and online tools.	CYBRScore Labs	Operating Systems Hardening (OSH); Topics: 1, 2, 3, 4, 5, 6, 7, 8, 10, 11	Hyper-V	2 Hours	2 Hours	53 minutes, 32 seconds	22 seconds
Whitelisting & Suspicious File Verification Capstone	Students will become familiar with procedures used in the validation of suspicious files. During the course of the lab the student will generate a system-level baseline using a command line file hash tool, followed by checking new/unknown files against whitelists and online tools.	CYBRScore Scored Labs	Operating Systems Hardening (OSH); Topics: 1, 2, 3, 4, 5, 6, 7, 8, 10, 11	Hyper-V	2 Hours	2 Hours	8 minutes, 28 seconds	52 seconds
White-linking & Countries on File Venific V	Students will become familiar with procedures used in the validation of suspicious files.							
Whitelisting & Suspicious File Verification Capstone	During the course of the lab the student will generate a system-level baseline using a command line file hash tool, followed by checking new/unknown files against whitelists and online tools.	CYBRScore Capstones	Operating Systems Hardening (OSH); Topics: 1, 2, 3, 4, 5, 6, 7, 8, 10, 11	Hyper-V	2 Hours	2 Hours	2 minutes, 22 seconds	24 seconds
Whitelisting & Suspicious File Verification Capstone Windows Deployment Services	command line file hash tool, followed by checking new/unknown files against whitelists	CYBRScore Capstones CYBRScore Labs	Operating Systems Hardening (OSH); Topics: 1, 2, 3, 4, 5, 6, 7, 8, 10, 11 Operating Systems Hardening (OSH); Topics: 1, 2, 3, 4, 5, 6, 7, 8, 10, 11	Hyper-V Hyper-V		2 Hours, 30 Minutes	2 minutes, 22 seconds 1 hour, 17 minutes	24 seconds 21 seconds
	command line file hash bod, followed by checking new/unknown files against whitelists and online tools. As an indient responder, it's important to understand how to create baseline Windows templates. You will learn how Window Deployment Service(WDS) may be used to create a baseline Windows 7 image. You'll also learn how to deploy a PXE boot image using WDS. As an indient responder, it's important to understand how to create baseline Windows templates. You will learn how Windows Deployment Service(WDS) may be used to create as baseline Windows 7 image. You'll also learn how to deploy a PXE boot image using WDS.	CYBRScore Labs CYBRScore Scored Labs			1 Hour, 15 Minutes		1 hour, 17 minutes	
Windows Deployment Services	command line file hash book, followed by checking new/unknown files against whitelists and online tools. As an indient responder, it's important to understand how to create baseline Windows templates. You will like man bow Window Deployment Service (WOS) may be used to create a baseline Windows 7 image. You'll also learn how to deploy a PXE boot image using WIS. As an indient responder, it's important to understand how to create baseline Windows templates. You will like man how Windows Deployment Service (WOS) may be used to create a baseline Windows 7 image. You'll also learn how to deploy a PXE boot image using WIS. It is this shay out will use Windows Event Viewer to view and filter the security event log on a Mindows 7 image. You'll also learn how to deploy a PXE boot image using WIS.	CYBRScore Labs CYBRScore Scored Labs CYBRScore Labs	Operating Systems Hardening (OSH); Topics: 1, 2, 3, 4, 5, 6, 7, 8, 10, 11	Hyper-V	1 Hour, 15 Minutes 1 Hour, 15 Minutes	2 Hours, 30 Minutes	1 hour, 17 minutes	21 seconds
Windows Deployment Services Windows Deployment Services	command line file hash boo, followed by checking new/unknown files against whitelists and online tools and online tools. As an incident responder, it's important to understand how to create baseline Windows templates. You will learn how Windows Deployment Services(WDS) may be used to create a baseline Windows Timage. It also learn how to deploy a PTE boot image using wIDS. As an incident responder, it's important to understand how to create baseline Windows As an incident septiment of the properties of the properties will be used to the properties will be used to the properties will be used with the properties will be used to the properties and the properties will be used to the properties and the properties will be used to the properties and the properties will be used to the properties and the properties will be used to the properties and the properties will be used to the properties and the properties will be used to the properties and the properties will be used to the properties and the properties will be used to the properties and the properties will be used to the properties and the properties and the properties and the properties and the properties are the properties and the properties and the properties are the properties are the properties and the properties are the properties and the properties are the properties and the properties are the propert	CYBRScore Labs CYBRScore Scored Labs CYBRScore Labs	Operating Systems Hardening (OSH); Topics: 1, 2, 3, 4, 5, 6, 7, 8, 10, 11 Operating Systems Hardening (OSH); Topics: 1, 2, 3, 4, 5, 6, 7, 8, 10, 11	Hyper-V Hyper-V	1 Hour, 15 Minutes 1 Hour, 15 Minutes	2 Hours, 30 Minutes 2 Hours, 30 Minutes	1 hour, 17 minutes 13 minutes, 29 seconds 8 minutes, 50 seconds	21 seconds 6 minutes, 6 seconds
Windows Deployment Services Windows Deployment Services Windows Event Ug Manipulation via Windows Event Viewer	command line file hash book, followed by checking new/unknown files against whitelists and online tools. As an indient responder, it's important to understand how to create baseline Windows templates. You will like man bow Window Deployment Service (WOS) may be used to create a baseline Windows 7 image. You'll also learn how to deploy a PXE boot image using WIS. As an indient responder, it's important to understand how to create baseline Windows templates. You will like man how Windows Deployment Service (WOS) may be used to create a baseline Windows 7 image. You'll also learn how to deploy a PXE boot image using WIS. It is this shay out will use Windows Event Viewer to view and filter the security event log on a Mindows 7 image. You'll also learn how to deploy a PXE boot image using WIS.	CYBRScore Labs CYBRScore Scored Labs CYBRScore Labs	Operating Systems Hardening (OSH); Topks: 1, 2, 3, 4, 5, 6, 7, 8, 10, 11 Operating Systems Hardening (OSH); Topks: 1, 2, 3, 4, 5, 6, 7, 8, 10, 11 Operating Systems Hardening (OSH); Topks: 1, 2, 3, 4, 5, 6, 7, 8, 10, 11	Hyper-V Hyper-V	1 Hour, 15 Minutes 1 Hour, 15 Minutes	2 Hours, 30 Minutes 2 Hours, 30 Minutes	1 hour, 17 minutes 13 minutes, 29 seconds 8 minutes, 50 seconds	21 seconds 6 minutes, 6 seconds 23 seconds
Windows Deployment Services Windows Deployment Services Windows Event Log Manipulation via Windows Event Viewer Windows Event Log Manipulation via Windows Event Viewer	command line file hash book, followed by checking new/unknown files against whitelists and online tools. As an indient responder, it's important to understand how to create baseline Windows templates, You will learn how Window Deployment Service(WDS) may be used to create a baseline Windows Timage. You'll also learn how to deploy a PXE boot image using WDS. As an incident responder, it's important to understand how to create baseline Windows Templates. You will learn how Windows Deployment Service(WDS) may be used to create a baseline Windows Timage. You'll also learn how to deploy a PXE boot image using WDS. In this lab you will use Windows Event Viewer to view and filter the security event log on a Windows 7 clien computer specifically for account logon. In this lab you will use Windows Event Viewer to view and filter the security event log on a Windows 7 clien computer specifically for account logon. In this lab, you will learn techniques necessary to scan Windows machines for vulnerabilities and exploit a wulnerability to gain control of the victim machine. Note that this lab is highly guided step by step; in a real world penetration test, each of	CYBRScore Labs CYBRScore Scored Labs CYBRScore Labs CYBRScore Labs CYBRScore Network Forensics	Operating Systems Hardening (OSH); Topks: 1, 2, 3, 4, 5, 6, 7, 8, 10, 11 Operating Systems Hardening (OSH); Topks: 1, 2, 3, 4, 5, 6, 7, 8, 10, 11 Operating Systems Hardening (OSH); Topks: 1, 2, 3, 4, 5, 6, 7, 8, 10, 11 Operating Systems Hardening (OSH); Topks: 1, 2, 3, 4, 5, 6, 7, 8, 10, 11	Hyper-V Hyper-V Hyper-V	1 Hour, 15 Minutes 1 Hour, 15 Minutes 1 Hour 1 Hour 3 Hour	2 Hours, 30 Minutes 2 Hours, 30 Minutes 1 Hour 1 Hour	1 hour, 17 minutes 13 minutes, 29 seconds 8 minutes, 50 seconds 9 minutes, 51 seconds	21 seconds 6 minutes, 6 seconds 23 seconds 20 seconds

In this lab, we will use the Pywin32 extensions and the Deviare library to hook into functions and interact with the internal data structures. The Deviar library is a bit limited in terms of tapabilities as a rootify, mainly since that is not what it was designed to do. However, it will be enough for our purposes and will enable us to more simply create a rootify that ourse a cover channel to editine table.	CYBRScore Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10	Hyper-V	2 Hours	2 Hours	10 minutes, 15 seconds	1 minute, 7 seconds
A number of technologies exist that work together to protect systems and networks. The real value of your networks and systems rests in the data that networks carry and reside in systems. In this laby out iff locus onso ways you can seleguard the data that resides on systems and when data is sent across the network. Securing an operating system, also known as hardening, strives to reduce vulnerabilities in order to protect a system against threats and attacks.	CYBRScore Labs	Operating Systems Hardening (OSH), Topics: 2, 4, 8; Windows System Administration (WSA), Topics: 5, 10, 13	Hyper-V	1 Hour	1 Hour	27 minutes, 51 seconds	25 seconds
A number of technologies exist that work together to protect systems and networks. The real value of your networks and systems rests in the data that networks carry and reside in systems. In this laby out iff locus onso ways you can seleguard the data that resides on systems and when data is sent across the network. Securing an operating system, also known as hardening, strives to reduce vulnerabilities in order to protect a system against threats and attacks.	CYBRScore Scored Labs	Operating Systems Hardening (OSH), Topics: 2, 4, 8; Windows System Administration (WSA), Topics: 5, 10, 13	Hyper-V	1 Hour	1 Hour	36 minutes, 34 seconds	1 minute, 12 seconds
A number of technologies exist that work together to protect systems and networks. The real value of your networks and systems rests in the data that networks carry and reside in systems. In this laby out iff locus on some ways you can seleguard the data that resides on systems and when data is sent across the network. Securing an operating system, also known as hardering, strives to reduce vulnerabilities in order to protect a system against threats and attacks.	CYBRScore Capstones	Operating Systems Hardening (OSH), Topics: 2, 4, 8; Windows System Administration (WSA), Topics: 5, 10, 13	Hyper-V	1 Hour	1 Hour	1 minute, 4 seconds	18 seconds
This lab exercise is designed to allow the trainee become familiar with the use of Wireshark.	CYBRScore Scored Labs	Network Defense (NDF), Topics: 1a, 1c, 1d, 2b, 4a	vSphere	1 Hour	1 Hour	27 minutes, 18 seconds	1 minute, 29 seconds
This lab exercise is designed to allow the trainee become familiar with the use of Wireshark.	CYBRScore Labs	Network Defense (NDF), Topics: 1a, 1c, 1d, 2b, 4a	vSphere	1 Hour	1 Hour	16 minutes, 47 seconds	12 seconds
In this lab, students will write their own vulnerable program in C, debug the program while performing a buffer overflow, and control execution flow to jump to a function in the code that is not normally called.	CYBRScore Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10	Hyper-V	3 Hours	3 Hours, 40 Minutes	51 minutes, 47 seconds	1 minute, 31 seconds
In this lab, students will explore fuzzing, shellcode generation, and analyzing output for bad characters. The students will then exploit vulnserver and Free MP3 Ripper 2.6	CYBRScore Labs	Penetration Testing (PTT), Topics: 3, 4, 5, 6, 8, 9, 10	Hyper-V	3 Hours	3 Hours, 40 Minutes	1 hour, 5 minutes	1 minute, 14 seconds
In this lab, students will explore fuzzing, shellcode generation, and analyzing output for bad characters. The students will then exploit vulnserver and Free MP3 Ripper 2.6	CYBRScore Labs		Hyper-V	3 Hours	3 Hours, 40 Minutes		
	functions and interact with the internal data structures. The Deviare library is a bit limited in terms of tapabilities as notific, mainly since that is not what it was designed to do. However, it will be enough for our purposes and will enable us to more simply create a notificial to discount of the data that networks. The real value of your networks and systems rests in the data that networks carry and reside in systems. In this lab, you will focus on some ways you can safeguard the data that resides on systems and when data is sent across the network. Securing an operating system, also known as hardening, strives to reduce vulnerabilities in order to protect a systems and sense and that data size of the control of	functions and interact with the internal data structures. The Deviare library is a bit limited in terms of it capabilities as a motility and interest of the control of the property of the control of th	functions and interact with the internal data structures. The Deviate library is a bit limited in terms of tapabilities as notable, making since this internal training of the property of the	Intendition and interact with the internal data structures. The Deviare Bloay is a bit limited in terms of tapabilities as notificially as a possible of the Common of the	Intentions and interact with the internal data structures. The Deviare Bibory is a Dit Intendia Internal Cipabilities as notification in Cipabilities as notificity and intendiated intendiated and intendiate	functions and interact with the intermed data structures. The Deviate Bibary is a bit immedial intermed (a trapabilities are notes) making and intermed intermed (a trapabilities are notes) making and intermediate and support and analysing order and protect a systems, also known as hardening, strikes or order or portect a systems and when data is sent scross the networks carry and reside residence of your networks and attacks. A number of technologies exist that work together to protect systems and networks. The real value of your networks and attacks. A number of technologies exist that work together to protect systems and networks. The real value of your networks and attacks. A number of technologies exist that work together to protect systems and networks. The real value of your networks and attacks. A number of technologies exist that work together to protect systems and networks. The real value of your networks and stacks. A number of technologies exist that work together to protect systems and networks. The real value of your networks and stacks. A number of technologies exist that work together to protect systems and networks. The real value of your networks and stacks. A number of technologies exist that work together to protect a systems, also known as way your can still your will focus on some way you can still great the data that resides on yatems and when data is sent across the network. Securing an operating system, also known as hardening, strikes or orduce vulnerabilities in order to protect a system, also known as hardening, strikes or orduce vulnerabilities in order to protect a system, also known as hardening, strikes or orduce vulnerabilities in order to protect a system, also known as hardening, strikes or orduce vulnerabilities in order to protect a system, also known as hardening, strikes or orduce vulnerabilities in order to protect a system, also known as hardening, strikes or ordu	functions and interact with the internal data structures. The Deviate library is a bit limited in terms of I capabilities as a rooff, many since that is not what it was designed to do. However, it will be enough for our purposes and will enable us to more simply create a notification that work tragether to protect pristens and enteroists. The enables will enable us to more simply create a notification that work tragether to protect significant and will enable us to more simply created a notification that work tragether to protect significant and will enable us to more simply created a notification that work tragether to protect any systems, and when data is seen terms the reduction & control enables will be a provided on the protect and systems, and when data is seen terms the reduction & control enables will be a provided on the protect and systems, and when data is seen terms the reduction & control enables will be a provided on the protect and structures. A number of technologies exist that work tragether to protect a systems, and when data is seen terms that work tragether to protect a systems, and when data is seen terms that death and enables that work tragether to protect a system, and when data is seen terms that death and enables that work tragether to protect a system, and when data is seen terms that death and enables that work tragether to protect a system, and when data is seen terms that each and when data is seen terms that death and enables that work tragether to protect a system, and when data is seen terms that each and when data is seen term that and when data is seen terms that each and when data is seen terms that each and when data is seen term that and when data is seen terms that death and when data is seen terms that each an