LNX200 - Fundamentals of Linux Security

Course Overview

Fundamentals of Linux Security for System Administrators teaches students basic Linux command line usage and filesystem structure, how to configure, evaluate and troubleshoot common management services used on today's Linux systems, and well as how to configure and test a Linux-based firewall. Linux System Administrators are often responsible for managing systems containing critical or sensitive data and infrastructure. The ability to securely and effectively manage Linux systems is paramount to the System Administrator job role. Completion of this module will prepare students to handle the basic requisite tasks associated with configuring, managing and troubleshooting Linux management tools, services and firewalls.

Estimated Course Length: 12 hours

In order for system administrators to effectively design secure systems, they must have a solid understanding of the Linux command line and file system, and how processes such as authorization, authentication, encryption, and service hardening work across a variety of operating systems. In addition, system administrators should have a strong understanding of common Linux ports, services, and how to control access to ports and services via firewalls.

Prerequisite Knowledge

Before completing this lesson, students should:

- Have familiarity with basic Linux commands
- Have a basic understanding of the Linux directory structure

Objectives

After completing this module, students will be able to:

- Perform basic command line usage and syntax
- Perform package management on Linux
- Identify basic file system structure
- Identify and describe common management services on Linux, and the use case for each
- Configure and troubleshoot various common management services on Linux
- Evaluate the strengths and weaknesses of various service configurations
- Perform service hardening on common Linux management services
- Configure Linux-based firewall

Essential Questions

- How do basic authorization methods prevent users from gaining access to data they are not intended to access?
- How can the lack of proper authentication affect privilege separation?
- How does a strong understanding of encryption enable system administrators to effectively select and implement appropriate encryption schemas?
- How can a lack of service hardening affect operating system and service security?
- What are the potential effects of an unsecured firewall on systems and services?

Activities & Supporting Material

I. Topics
- Linux Command Line
- Linux File System Structure
- Telnet
- SSH
- VNC and SSH tunneling
- Fail2Ban
- Firewalls w/UFW, firewalld

II. Lab Activities
- Lab 1: Basic Linux Command Line Usage
- Lab 2: Basic Linux Filesystem Structure
- Lab 3: Telnet Traffic Capture
- Lab 4: Installing OpenSSH server, configuring sshd
- Lab 5: SSH Keypairs, SSH Keypair Passphrases, and exporting SSH public keys to remote machine
- Lab 6: Fail2Ban Setup and Analysis
- Lab 7: Setting up a firewall with UFW and firewalld

III. Supporting Material
- Video 1: Telnet Vulnerability Demo via Wireshark Capture
- Video 2: SSH Passphrase Strength cracking

Resources

I. Hardware
- Internet-connected laptop running a modern web browser

II. Software
- Telnet
- SSH
- VNC
- Fail2Ban
- UFW
- firewalld
- Guacamole

Assessment

I. Formative
- Multiple choice (or other format) questions in the video that will verify the learning for each submodule.

II. Summative
- Capstone Lab:
- Student's will exploit a novel application that has several vulnerabilities that have various levels of filtering and difficulty in exploiting

Comtech
cyberstronger.com | comtechtel.com
275 West Street, Annapolis, MD 21401