Vulnerability Assessment Management Labs

Course: **00114**
Filter: **Beginner**
Duration: **20 hours**
Category:: **Cyber Security**
Price: **2800,00 €**

About Course

Learn the security techniques used by the Internet’s most skilled professionals. This Vulnerability & Assessment Management lab bundle, which includes 19 distinct, hands-on labs, will prepare you with the tools and techniques to detect and exploit security vulnerabilities in web-based applications, networks, and computer systems that use the Windows and Linux OS, as well as recommend mitigation countermeasures.

What you'll learn

- Apply the objectives outlined in the National Cybersecurity Workforce Framework's professional role for the Vulnerability Assessment Analyst per NIST SP-800-181
- Detect and exploit security vulnerabilities in web applications, networks, and computer systems that use Windows and Linux operating systems, and recommend mitigating countermeasures
- Perform the steps required to configure a firewall from the basic command line interface

Pre-requisites

- None

Curriculum

Module 1: 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).

Module 2: 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.

Module 3: 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.

Module 4: Analyze Various Data Sources to Confirm Suspected Infection

-

Module 5: Students will review network traffic to confirm the presence of malicious activity using various tools including Wireshark and VirusTotal.com.

-

Module 6: 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 the "Practitioner" level.

Module 7: Core Impact Web Application Penetration Testing

-

Module 8: Data Backup and Recovery

- In this lab we will simulate the recovery phase where we must perform a backup in a server environment.

Module 9: Gap Analysis of Firewall Rules

- Students will log into an organization's firewall, document existing firewall rules, analyze these rules and making recommendations based on this analysis. Students will then make make the necessary changes.

Module 10: 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.

Module 11: Microsoft Baseline Security Analyzer

-

Module 12: Monitoring Network Traffic

- In this lab we will replicate potentially malicious scans from the Internet against a corporate asset. Scans from the Internet are very common.

Module 13: Network Discovery

- The Network Discovery lab is designed to help students facilitate open source collection by teaching them how to use more intimate network discovery techniques.

Module 14: 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.

Module 15: Using Snort and Wireshark to Analyze Traffic

- In this lab we will replicate the need for Analysts to be able to analyze network traffic and detect suspicious activity. Tools like Wireshark and Snort can be utilized to read,

capture, and analyze traffic.

Module 16: 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.

Module 17: Whitelisting & Suspicious File Verification

- Students will become familiar with procedures used in the validation of suspicious files.

Module 18: Firewall 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 machine