Syllabus

Network Security

CYBERIUM ARENA
-SIMULATOR-

Description

Network security is a broad term that covers multiple technologies, devices, and processes. Nowadays, every organization, regardless of size, industry, or infrastructure, requires a network security expert in place to protect it from the ever-growing landscape of cyber threats today. After this course, you will discover security vulnerabilities across the entire network using network hacking techniques and vulnerability scanning. You will understand the various types of firewalls available and master both Windows and Linux servers' hardening.

The course helps prepare for the certification exams CySA+ (CompTIA), Security+ (CompTIA), GISP (SANS), and GISF (SANS).

Target Audience

The course targets IT or networking knowledge participants who wish to understand corporate cybersecurity and cyber defense from a technical perspective.

Pre-requisites

Linux

SOC or Penetration-Testing

Objectives

- Learning the cyber threat landscape that modern organizations face
- Acquiring the necessary knowledge and tools to defend the corporate network
- Identifying when attacks are happening on the network
- Becoming familiar with available tools for performing security-related tasks

Module 1: Cyber Security in Networks

In this module, students will dive deeper into the world of cybersecurity, the primary goal being to teach participants to embrace the attacker state-of-mind to recognize the necessary defense mechanisms.

Network Security Fundamentals

- Principles of Network Security
- Security Components
- Security Policies
- Physical Security
- Securing Devices

Network Attacks

- Lab Setup: Creating your Organization Domain
- Identifying Application Attacks
- Analyzing C&C Communications
- Reversing Malware Network Behaviour

Module 2: Advanced Network Awareness

Organizations these days suffer greatly from network attacks and malicious intrusions. Those who manage the organization's network have an immense impact on ensuring its safety. This module will teach the student to embrace the role of the network security administrator. Students will learn to inspect the network and find targets and possible security issues before the attackers can use them.

Analyzing the Network

- Automations Using NMAP
- Detecting Service Changes Using Shodan CLI
- Launching NSE to Detect Possible Vulnerabilities
- Capturing Fake MAC and IP Addresses
- Spying on the Local Network
- Hunting for Rootkits with Windbg
- Using Sysinternals Suite to Identify Unusual Ports

Module 3: Cryptography in Theory

In this module, students will discuss cryptography, in theory, and understand different types of algorithms.

Introduction to Cryptography

- Ciphers in General
- Encodings

Usage of Cryptography in the Cyber World

- The Theory of Cryptography in Cyber-Security
- Hash-Based Password Verification
- VPNs and SSL Based VPNs
- IPsec and Tunnelling
- Poor Cryptography Threats
- Algorithm Problems
- Collision Attacks
- Random Number Generation
- Key Management Problems

Module 4: Practical Cryptography

In this module, students will learn how to implement famous techniques practically. Students will cover private keys cryptosystems such as Caesar cipher, Vigenere cipher, Data Encryption Standard (DES), and Advanced Encryption Standard (AES).

Key Based Encryptions

- Ciphers in General
- Symmetric-Key
- Asymmetric-Key
- Block Ciphers
- Attacks on Block Ciphers

Practical Ciphering

- Classical Encryption Types
- Mechanical - Enigma and Lorenz
- Encryption in Application

Module 5: Hardening the Network

In this module, students will learn a wide variety of IT security concepts and tools. The students will learn the step-by-step hardening measures. Explore some security weaknesses of the Linux operating system, and learn to protect against those weaknesses. Learn how to secure the various account types on a Linux system, enforce strong passwords, configure the firewall, and more.

Routing and Network Components Hardening
- Iptables vs. UFW
- Monitoring the FW using Tshark
- Mitigating DoS Techniques
- Static ARP and DHCP Entry to Prevent Poisoning

IPv6 Security
- IPv6 Protocols
- Protecting Against Rogue DHCPv6 Servers
- Mitigate IPv6 Attacks
- DDoS in IPv6

Counter-Measuring Attacks
- Host vs. Network-Based IDS
- Snort as IDS and IPS
- Constructing Honeypots
- Identifying Log Tampering