CYBERIUM ARENA

Description

The Network Research program is designed to introduce learners to the fundamental aspects of information security, employing Linux as a primary tool and providing exposure to various security threats.

NETWORK RESEARCH

Module 1: Intro to Linux

This module provides an in-depth look into virtualization, focusing on Linux. It begins with an overview of virtualization and Linux distros, guides on Linux installation, and using VMWare. It addresses network configurations, Linux administration topics like directory structures, user management, packages, file manipulation commands, and concludes with scripting and automation in Linux.

Virtualization
Introduction to Virtualization
About Linux Distro
Installing Linux
Working with VMWare
Bridged vs. NAT
Working with Linux
Linux Directories
Linux Users
Packages
File Manipulation Commands
Text and File Manipulation Technics
Linux Scripts and Automation

Module 2: Networking

This module offers a deep dive into key networking protocols and services. It starts by exploring the TCP/IP model, followed by detailed examinations of DNS, DHCP, and ARP protocols, then transitions into network services, providing insights into the workings of SSH, FTP, and the Apache web server. This comprehensive study of networking equips learners with crucial knowledge for managing and securing digital networks.

Protocols
TCP/IP Model
DNS
DHCP
ARP
Network Services
SSH
FTP
Apache

Module 3: Network Security

This module dives into network scanning and attack techniques. It starts with Nmap and Masscan, powerful tools for network scanning, then covers brute force and offline attack strategies. This course offers invaluable skills for network security testing.

Scanning
Nmap
Masscan
Brute Force
Offline Attacks
Creating Wordlists
Wireshark
Filtering and Parsing
Extracting Objects

Module 4: Cyber Security

This module delves into various network attacks and defense techniques. It covers Man-in-the-Middle (MiTM) and ARP Poisoning strategies, service brute-forcing, and analysis of cyberattacks. Learners are introduced to reverse and bind payloads, and hands-on training with Msfvenom and Msfconsole. Finally, it explores firewall operation, including port blocking and device monitoring, imparting critical skills for network security.

Network Attacks
MiTM
ARP Poisoning
Service Brute-Force
Analyzing Attacks
Cyber Attack
Reverse and Bind Payloads
Working with Msfvenom
Working with Msfconsole
Firewall
About Firewall Operation
Blocking Ports
Monitoring Devices

NX Defense | LEVEL: 2 | DURATION: 40h