Network Cyber-Research

Course 71576 – 40 Hours

Overview

Large and small companies face a critical stage; cyber-attacks have transformed dramatically over the past few years. Unfortunately, organizations are still being breached too often and are under more pressure than ever to secure their systems. The Network Security course aims to address cyber challenges experienced on the network level. The course covers various attack techniques and how to defend against them.

By the end of the course, participants will have the ability to build and maintain a secure network, protect data, manage vulnerabilities, implement active access control measures, and regularly monitor the network for inconsistencies.

The course sets the groundwork for later specialization in cyber forensics, advanced cyber defense, and penetration testing.

The course helps prepare for the certification exams Linux+ (CompTIA) and LPIC-2 (LPI).

On completion, Delegates will be able to

- Become familiar with the cyber threat landscapes
- Acquire the knowledge and tools to recognize threats in the network
- Test networks and network-based-systems for vulnerabilities
- Understand cyber-attacks
- Become familiar with a variety of available tools for performing security-related tasks

Who should attend

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

- IT security personnel
- Incident responders
- Security analysts

Course Contents:

Module Title	Description
Module 1: Introduction to Linux Students will study the Linux OS fundamentals during this module – How to use basic commands, manipulation of text and command outputs, understanding the Terminal-Emulator, permissions, and other security concepts.	▪ **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 ○ Writing Linux Scripts
Module 2: Networking During this module, participants will study network infrastructures, common network types, network Layers, communication between protocols, communication between network devices from different Layers, and network anonymity methods.	▪ **Protocols and Services** ○ TCP/IP and OSI Model ○ DNS ○ DHCP ○ ARP ○ Remote Connection Protocols ○ Important Protocols ▪ **Wireshark – Diving into Packets** ○ Non-Secure and Secure Packets ○ Filtering and Parsing ○ Extracting Objects and Files from PCAP Files
Module 3: Introduction to Network Forensics Large 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 introduce participants to Network Forensics and learn how to locate and better understand various attacks.	▪ **Windows Tools** ○ Advanced Wireshark ○ NetworkMiner ○ Sysinternals ▪ **Linux Tools** ○ TShark - Network Analyzing Automation ○ Zeek Tools: Bro and Bro-Cut
Module 4: Cyber Security This module's primary goal is to teach participants to embrace the attacker state-of-mind to recognize the necessary defense mechanisms. Participants will deal with several types of attacks. Students will learn about hash functions; furthermore, they will learn how wireless networks are attacked and how they are vulnerable to those attacks. Social engineering	▪ **Cyber Security Vectors** ○ Anti-Viruses ○ Firewalls and FWNG ○ DoS and DDoS ○ CNC Servers and Botnets ○ Wireless Attack Concepts ○ Steganography ▪ **Network Attacks**

and honeypot techniques will also be demonstrated.	○ Introduction to Scanning ○ Scanning Methods in Nmap ○ Scanning with Shodan ○ MiTM ○ ARP Poisoning ○ DHCP Starvation ○ LLMNR Attacks ▪ **Cyber Attack Practice** ○ Backdooring ○ Privilege Escalation