Network Research

Index: **NS106**

Duration: **40 hours – 5 Days**

Description

Companies large and small 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 penetrating testing.

Target Audience

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

- IT security personnel
- Incident responders
- Security analysts

Pre-requisites

- None

Objectives

- Becoming familiar with the cyber threat landscapes that modern organizations face.
- Acquiring the knowledge and tools to recognize threats in the network.
- Testing networks and network-based-systems for vulnerabilities.
- Understanding cyber-attacks.
- Becoming familiar with a variety of available tools for performing security-related tasks.

Day 1

Module 1: Introduction to Linux

During this module, students will study the fundamentals of the Linux OS - 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
    - Packages Commands
    - Updating
    - Installing and Managing
  - File Manipulation Commands
  - Variables
    - Internal
    - External
    - Terminal
  - Text and File Manipulation Technics
  - Writing Linux Scripts
    - Permissions
    - Conditions
    - Loops
    - Automation
  - Services
    - FTP
    - SSH
    - SimpleHTTPServer
    - Apache
  - Making Linux executables

Day 2

Module 2: Networking

During this module, participants will study the basics of network infrastructures, common network types, network Layers, and communications between protocols, communication between network devices from different Layers, and network anonymity methods.

- **Protocols and Services**
  - TCP/IP and OSI Model
    - Network Routing Basics
  - DNS
  - DHCP
  - ARP
  - Intro to Subnetting
  - Worldwide 1Pv4
  - Remote Connection Protocols
  - Important Protocols
- **Nmap**
  - Introduction to Scanning
  - Etherape and Wireshark
  - Scanning Methods in Nmap
  - Nmap vs faster tools
  - Scanning with Shodan
- **Anonymous**
  - Proxy
  - VPN
  - Tor
- **Wireshark - Diving into Packets**
  - Non-Secure and Secure Packets
  - Filtering and Parsing
  - Extracting Objects and Files from PCAP Files
  - Windows Built-In Tools

Day 3

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 will learn the ability to locate and better understand various attacks.

- **MiTM**
  - Intro to MiTM
  - About the ARP protocol
  - ARP poisoning
- **Scapy**
  - Basic commands
  - Crafting your packets

- **Windows Tools**
  - Advanced Wireshark
    - OS-Fingerprinting
    - Detecting Suspicious Traffic
    - GeoIP Mapping
  - NetworkMiner
  - Sysinternals

- **Linux Tools**
  - TShark - Network Analyzing Automation
    - Capture Packet Data from Live Network
    - Filter Packets from Live Network
    - Filter Packet from PCAP File
    - Traffic Statistics
    - Automating Network Capture and Filtering
    - File-Carving
  - Zeek Tools: Bro and Bro-Cut
    - Extracting Information
    - Parsing Traffic Logs
  - CAPInfo

Days 4-5

Module 4: Cyber Security

The primary goal of this module is teaching 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 the organization as vulnerable to those attacks. Social engineering and honeypot techniques will also be demonstrated.

- **Cyber Security Vectors**
  - Anti-Viruses
  - Firewalls and FWNG
  - DoS and DDoS
  - CNC Servers and Botnets
  - Wireless Attack Concepts:
    - Handshake Based Authorization
    - Deauthentication Attacks MiTM
    - Evil-Twin
  - Steganography
- **Network Attacks**
  - Introduction to Scanning
  - Scanning Methods in Nmap
  - Scanning with Shodan
  - MiTM
    - ARP poisoning
    - DNS Spoofing
  - DHCP Starvation
  - LLMNR Attacks
    - Offline Password Brute-Force
    - Working with Responder
- **Cyber Attack Practice**
  - Backdooring
    - Payloads: Reverse vs. Bind
    - Multi-Handler
  - Privilege Escalation
- **Introduction to vulnerabilities**
  - Metasploit
  - Basic exploit use
  - Penetration basics
  - Remote and local exploits
  - DNS Spoofing
  - DHCP Starvation