SDA-ACADEMY
Cybersecurity training

THINKCYBER

NX-201

Syllabus

Network Research

CYBERIUM **ARENA**

- SIMULATOR -

Description

The Network Research program is aimed at the basic worlds of information security with the help of Linux and familiarity with various attacks in the worlds of security. The course sets the groundwork for later specialization in cyber forensics, advanced cyber defense, and penetration testing. 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).

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

Objectives

- Becoming familiar with the cyber threat landscapes
- Acquiring the knowledge and tools to recognize threats in the network
- Understanding cyber-attacks
- Becoming familiar with a variety of available tools for performing security-related tasks

Module 1: Introduction to Linux

Students will study the Linux OS fundamentals. This module uses Linux commands, manipulating text and command outputs, understanding terminal-emulators, permissions, and other security concepts.

Virtualization
Introduction to Virtualization
About Linux Distro
Installing Linux
Working with VMWare
Bridged vs. NAT

Working with Linux
Linux Users' Packages
File Manipulation Commands
Text and File Manipulation Techniques
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
Network Routing Basics
DNS
DHCP
ARP
Remote Connection Protocols

Wireshark
Diving into packets
Non-Secure and Secure Packets
Filtering and Parsing
Extracting Objects

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
Network Miner
Advanced Wireshark
OS-Fingerprinting
Detecting Suspicious Traffic
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
File-Carving Parsing
Traffic Logs
CAPInfo

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 and honeypot techniques will also be demonstrated.

Cyber Security Vectors
Anti-Viruses
DoS and DDoS
CNC Servers and Botnets
Steganography

Network Attacks
Scanning Methods
MiTM
ARP Poisoning
DHCP Starvation
LLMNR Attacks
Offline Password Brute-Force
Working with Responder

Cyber Attack Practice
Payloads: Reverse vs. Bind