## Outline



**Cyber Infrastructure Attacks**

4.5 Days

In this course, you will take your first steps in Cyber Security!

The lessons will guide you through the initial stage of an attack, in which information is gathered, and then you will learn how to make your way into the organization. You will be introduced to network data analysis, and how to make sure you are not discovered when involved in offensive cyber activity.

## Target Audience

* Students who want to learn about the information gathering process.
* Students who aspire to be ethical hackers.
* Students who want to understand basic methods of hacking into a network.

## Prerequisites

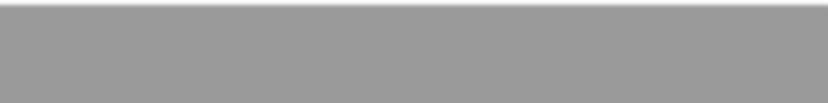
Before attending this course, students must have the following technical knowledge:

* Basic knowledge of the Linux OS.
* Basic knowledge of the Windows OS.
* Basic knowledge of networking.
* Basic knowledge of Python programming.

## Objectives

Upon completing this course, graduates will be able to:

* Analyze network traffic.
* Gather information about targeted victims.



* Scan networks and find possible ways to breach them.
* Perform online and offline brute-force attacks against targets without leaving any footprints.

**Contents**

# Day 1:

Module 1: Introduction to Information Security

* Cybersecurity Terminology
* Attack Types & Surfaces
* Cyber Security Attacks
* The anatomy of a cyber-attack cycle in practice

Module 2: Web anonymity & Dark Web

* Terminology
* Search Engines
* Automated Framework
* Creating malicious files

# Day2:

Module 3: Network Scanning & Footprinting & Reconnaissance methodology

* Hping3
* Nmap Basics

# Day 3:

* Advanced Nmap Features
* IDLE Scan
* Masscan
* ~~Banner Grabbing~~

Module 4: Enumeration

* Windows Domain Environment
* Domain Enumeration Techniques
* Manual Enumeration
* Automatic Enumeration

Module 5: Brute-force & Password Cracking

* Passwords and Hashes
* Attack Vectors
* Dictionary Attack
* ~~Brute-Force Tools~~
* ~~Automation Tools~~

# Day 4:

Module 6: Hacking Frameworks &Automation using Metasploit

* Basic Hacking Terminology
* Vulnerabilities Search-Engines
* Metasploit Framework
* Hacking Frameworks - Pros & Cons
* Means of Protection

Module 7: Men In The Middle

* MITM Technique
* ARP Protocol
* MITM Automated Frameworks
* Arp spoof
* MITM Automated Frameworks
* DNS spoof

# Day 5:

Module 8: Python Programming for Security

* Socket Fundamentals (Client & Server)
* Data Exchange
* Echo Communication
* Reverse Shell
* Banner Grabbing
* Breaking Down a Protocol
* FTP Communication using Python
* SSH Communication
* Scapy Introduction
* Scapy Programming as Offensive tool