About the Course

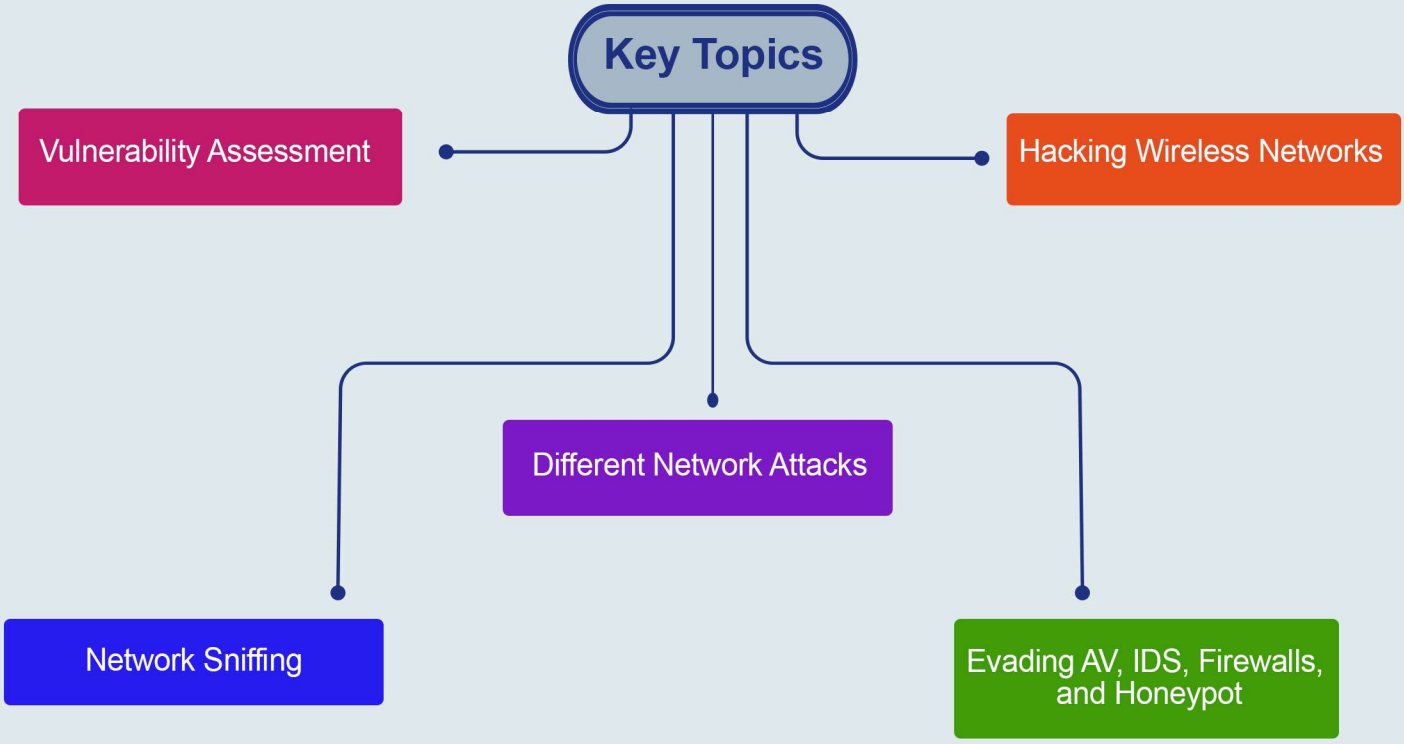
In this course you will learn the latest hacking methodologies and use of different attack methods on the Networks. Coupled with customize scenario set in real-world security lab environment, you are able to expect the attacks you are most likely to face in your work and how to apply the best practices to secure the interconnected network within your organization.
The course provides you with not only the attack techniques, but also countermeasure methodologies to protect the Network and IT infrastructure to mitigate risks.

Learning Objectives

1. Discover vulnerabilities in Network Infrastructure
2. Able to create exploits and take advantage of Network vulnerabilities
3. Explore various Network attacks
4. Use different tools to secure the environment of Network
5. Learn how to harden Network
6. Understanding the commonly used server roles and explore how to secure it

Terminus System

Key Topics



Pre Requisites

It is necessary to take the following course:

- Ethical Hacking & Penetration Testing Concepts
- Ethical Hacking & Penetration Testing Tools

Terminus System

What You Will Receive

- Course Presentation File
- Complementary Files
- Network Ethical Hacking & Penetration Testing eBook

Who Should Attend

Anybody who is in charge of security assessment and penetration testing and also:

- CISOs
- Network PenTesters
- Threat & Vulnerability Analysts

Syllabus

Vulnerability Assessment

- Technology Brief
- Vulnerability Assessment Concept:
- Vulnerability Assessment
- Vulnerability Assessment Life-Cycle
- Vulnerability Assessment Solutions
- Vulnerability Scoring Systems
- Vulnerability Scanning

Network Sniffing

- Sniffing Concepts
- MAC Attacks
- DHCP Attacks
- ARP Poisoning
- Spoofing Attacks
- DNS Poisoning
- Sniffing Tools
- Sniffing Detection Techniques
- Countermeasures

Denial-of-Service

- DoS/DDoS Concepts
- DoS/DDoS Attack Techniques
- DoS/DDoS Attack Tools
- DoS/DDoS Protection Tools
- Countermeasures

Syllabus

Session Hijacking

- Session Hijacking Concepts
- Application-Level Session Hijacking
- Network-Level Session Hijacking
- Session Hijacking Tools
- Countermeasures

Evading AV, IDS, Firewalls, and Honeypot

- IDS, Firewall and Honeypot Concepts
- Evading IDS
- Foiling IDS at the Network Level
- Foiling IDS at the Application Level
- Web Attack IDS Evasion Tactics
- Bypassing IDS/IPS with TCP Obfuscation Techniques
- Evading Firewalls
- IDS, Firewalls Evading Tools
- IDS, Firewalls Evasion Countermeasures
- Detecting Honeypots
- AV Evading Overview
- Countermeasures

System Hacking

- System Hacking Concepts
- System Hacking Methodology
- Password Cracking

Syllabus

Hacking Wireless Networks

- Sniffing WiFi
- Monitoring network probing activity
- Wireless anonymity attacks
- Sniffing, modifying, and dropping packets as MitM
- Exploiting WiFi Hotspots
- WiFi Client Attacks
- WiFi Fuzzing for Bug Discovery
- Attacking WPA2 Pre-Shared Key Networks
- Wireless Hacking Tools
- Countermeasures

Windows Hacking

- Domain Reconnaissance
- User Enumeration
- Active Directory
- Windows Patch Management Strategies
- Desktop Lockdown & Exchange Server
- Overview DEP, ASLR and CFG
- Fuzzing
- Crash Replication
- Controlling EIP
- Locating space for our Shellcode
- Bad Characters
- Redirecting Execution
- Introducing Mona
- Shellcode Payload
- Windows Privilege Escalation

Syllabus

Linux Hacking

- o Overview DEP, ASLR and Canaries
- o Controlling EIP
- o Locating Space
- o First Stage Shellcode
- o Locating RET
- o Generating Shellcode
- o Linux Privilege Escalation

Hands-on Training

- Lab 1 – Sniffing
- Lab 2 – DoS and DDoS Attacks
- Lab 3 – Session Hijacking
- Lab 4 – Intrusion Detection
- Lab 5 – Evade Firewalls
- Lab 6 – Footprint a Wireless Network
- Lab 7 – Wireless Traffic Analysis
- Lab 8 – Wireless Attacks