Ethical Hacking

Duration: (60 hours)

Venue: Computer Engineering Department,

Fr. Conceicao Rodrigues college of Engineering, Bandstand, Bandra (W)

Prerequisite: Basics of Computer Networks.

Course Index

1. Introduction to Ethical Hacking (safeguarding systems and networks) (week 1)

- Information security overview
- Information security threats and attack vectors
- Hacking concepts
- Hacking phases
- Types of attacks
- Information security controls

2. Foot printing and Reconnaissance (week 1)

This section will teach you to collect information about the target system.

- Footprinting concepts
- Footprinting tools
- Footprinting countermeasures

3. Enumeration & Scanning Networks (week 1)

From this section, you will learn how to gather more technical insights of the target system such as user names, machine names, network resources and services.

- Overview of network scanning
- Scanning techniques
- Vulnerability scanning
- Anonymizers
- Scanning countermeasures
- What is Enumeration?
- Techniques for Enumeration
- Services and ports to enumerate
- Enumeration countermeasures

4. System Hacking (Linux and Windows platform) (week 1)

You will be able to hack into others machine like Linux and windows OS, after this section.

- System hacking Goals
- Hacking Methodology
- Password cracking
- Privilege escalation
- Stealing passwords using key loggers
- Anti key loggers and Anti-spywares
- Steganography
- Covering tracks

5. Malicious Codes (week 2)

Learn to create and deploy malicious code over the network.

- What is a Trojan
- Indication of Trojan attacks
- How to deploy a Trojan
- Trojan countermeasures
- Introduction to viruses
- Virus maker
- Worm maker
- Viruses and worms countermeasures

6. Sniffers (week 2)

You will be able to capture and read data transmitting over wired and wireless channels after this section.

- Packet Sniffing
- Sniffing threats
- Mac flooding
- Rogue DHCP server attack
- ARP spoofing techniques
- ARP poisoning tools
- Defense against ARP spoofing
- Sniffing tools
- DNS spoofing and defense

7. Social Engineering (week 2)

Learn modern day techniques used to trap potential victims.

- What is social engineering?
- Factors that make companies vulnerable to attacks
- Phases in social engineering attacks
- Human based social engineering
- Computer based social engineering
- Identity theft
- Phishing and Pharming attacks
- Social engineering countermeasures

8. Denial of Service (week 2)

You will learn how to disrupt the availability of services over the network.

- What is denial of service attack?
- What are distributed denial of service attacks
- Botnet
- DoS/DDoS attack tools
- DoS/DDoS countermeasures

9. Session Hijacking (week 2)

Impersonating the target and taking control of his dialogue will be dealt with in this section.

- What is session hijacking?
- Key session hijacking techniques
- Man-in-the-Middle Attack
- Cross-site Script Attacks
- Protecting against session hijacking

10. SQL Injection (week 3)

Exploiting the flaws in database systems will be taught in this section.

- SQL Injection attacks
- Types of SQL injection
- Bypass website logins using sql injection
- Password grabbing
- SQL injection tools
- How to defend against SQL injection

11. Hacking Wireless Networks (week 3)

Exploiting the flaws in wireless networks will be covered in this section.

- Types of wireless networks
- Wireless terminologies
- How to break WEP encryption
- Footprint wireless networks
- How to defend against wireless attacks

12. Hacking Mobile Platforms (week 3)

You will learn the hacking and taking control of android devices.

- Mobile attack vectors
- Mobile platform vulnerabilities and risk
- Android vulnerabilities
- Hacking android phones
- Mobile device protection tools

13. Evading IDS, Firewalls and Honeypot (week 3)

This section will teach implementing security solutions to help overcome the vulnerabilities in a system.

- Types of intrusion detection system
- Firewall architecture
- Linux IP tables

- How to setup a honeypot
- How snort works
- Evading IDS/FIREWALLS
- Countermeasures

14. Digital Forensic (week 3)

Learn how to collect evidences from the post attack scenarios.

- Disk imaging
- Disk forensic
- Ram forensic
- Network forensic