Ethical Hacking and Countermeasures Expert

www.us-council.com

Introduction to Ethical Hacking

- What is Hacking
- Who is a Hacker
- Skills of a Hacker
- Types of Hackers
- Reasons for Hacking
- Who are at the risk of Hacking attacks
- Effects of Computer Hacking on an organization
- Network Security Challenges
- Elements of Information Security
- The Security, Functionality & Usability Triangle
- What is Ethical Hacking
- Why Ethical Hacking is Necessary
- Scope & Limitations of Ethical Hacking
- What is Penetration Testing
- What is Vulnerability Auditing

FootPrinting

- What is FootPrinting
- Objectives of FootPrinting
- Finding a company's details
- Finding a company's domain name
- Finding a company's Internal URLs
- Finding a company's Public and Restricted URLs

- Finding a company's Server details
- Finding the details of domain registration
- Finding the range of IP Address
- Finding the DNS information
- Finding the services running on the server
- Finding the location of servers
- Traceroute analysis
- Tracking e-mail communications

Scanning

- What is network scanning
- Objectives of network scanning
- Finding the live hosts in a network
- SNMP Enumeration
- SMTP Enumeration
- DNS Enumeration
- Finding open ports on a server
- Finding the services on a server
- OS fingerprinting
- Server Banner grabbing tools
- What is a Vulnerability Scanning
- Vulnerability Scanner tools
- Finding more details about a vulnerability
- What is a proxy server
- How does proxy server work
- Types of proxy servers
- How to find proxy servers
- Why do hackers use proxy servers
- What is a TOR network
- Why hackers prefer to use TOR networks

Hacking Web Servers & Web Applications

- What is a web server
- Different webserver applications in use
- Why are webservers hacked & its consequences
- Directory traversal attacks
- Website defacement
- Website password brute forcing
- How to defend against web server hacking

Session Hijacking

- What is session hijacking
- Dangers of session hijacking attacks
- Session hijacking techniques
- Cross-Site scripting attack
- Session hijacking tools
- How to defend against session hijacking

SQL Injection

- What is SQL Injection
- Effects of SQL Injection attacks
- Types of SQL Injection attacks
- SQL Injection detection tools

Evading Firewalls, IDS & Honeypots

- What is a Firewall
- What are the functions of a Firewall
- What is an IDS
- How does an IDS work
- SPAN
- IDS tools
- What is a honeypot

- Types of honeypots
- Honeypot tools
- Honeypot detection tools

Buffer Overflow

- What is a buffer
- Understanding usage of buffers in applications
- What is buffer overflow
- Simple buffer overflow in C programming
- How to detect a buffer overflow
- How to defend against buffer overflow attacks

Denial of Service

- What is a DoS attack
- What is a DDoS attack
- Symptoms of a Dos attack
- DoS attack techniques
- What is a Botnet
- Defending DoS attacks

Cryptography

- What is Cryptography
- Types of cryptography
- Cipher algorithms
- Public key infrastructure
- What is a Hash
- Cryptography attacks

System Hacking

- What is system Hacking
- Goals of System Hacking
- Password Cracking

- Password complexity
- Finding the default passwords of network devices and software's
- Password cracking methods
    - Online password cracking
        - Man-in-the-middle attack
        - Password guessing
    - Offline password cracking
        - Brute force cracking
        - Dictionary based cracking
        - Hybrid attack
- USB password stealers
- Elcomsoft Distributed password recovery tools
- Active password changer
- What is a keylogger
- How to deploy a keylogger to a remote pc
- How to defend against a keylogger

Sniffers

- What is a sniffer
- How sniffer works
- Types of sniffing
    - Active sniffing
    - Passive Sniffing
- What is promiscuous mode
- How to put a PC into promiscuous mode
- What is ARP
- ARP poison attack
- Threats of ARP poison attack
- How MAC spoofing works
- MAC Flooding
- What is a CAM Table

- How to defend against MAC Spoofing attacks
- How to defend against Sniffers in network

Phishing

- What is Phishing
- How Phishing website is hosted
- How victims are tricked to access Phishing websites
- How to differentiate a Phishing webpage from the original webpage
- How to defend against Phishing attacks

Malware

- What is malware
- Types of malware
    - Virus
        - What is a virus program
        - What are the properties of a virus program
        - How does a computer get infected by virus
        - Types of virus
        - Virus making tools
        - How to defend against virus attacks
    - Worm
        - What is a worm program
        - How worms are different from virus
    - Trojan
        - What is a Trojan horse
        - How does a Trojan operate
        - Types of Trojans
        - Identifying Trojan infections
        - How to defend against Trojans
    - Spyware
        - What is a spyware

        - Types of spywares
        - How to defend against spyware
    - Rootkits
        - What is a Rootkit
        - Types of Rootkits
        - How does Rootkit operate
        - How to defend against Rootkits

Wireless Hacking

- Types of wireless networks
- Wi-Fi usage statistics
- Finding a Wi-Fi network
- Types of Wi-Fi authentications
    - Using a centralized authentication server
    - Using local authentication
- Types of Wi-Fi encryption methods
    - WEP
    - WPA
    - WPA2
- How does WEP work
- Weakness of WEP encryption
- How does WPA work
- How does WPA2 work
- Hardware and software required to crack Wi-Fi networks
- How to crack WEP encryption
- How to crack WPA encryption
- How to crack WPA2 encryption
- How to defend against Wi-Fi cracking attacks

Kali Linux

- What is Kali Linux

- How Kali Linux is different from other Linux distributions
- What are the uses of Kali Linux
- Tools for Footprinting, Scanning & Sniffing
- What is Metasploit framework
- Using Metasploit framework to attack Windows machines
- Using Metasploit framework to attack Android devices

Penetration Testing

- What is Penetration Testing
- Types of Penetration Testing
- What is to be tested
  - Testing the network devices for mis-configuration
  - Testing the servers and hosting applications for mis-configuration
  - Testing the servers and hosting applications for vulnerabilities
  - Testing wireless networks
  - Testing for Denial of Service attacks

Counter Measure Techniques for Network level attacks

- Types of Firewall
  - Packet Filtering Firewall
  - Circuit-Level Gateway Firewall
  - Application-Level Firewall
  - Stateful Multilayer Inspection Firewall
  - Limitations of a Firewall
- IDS / IPS
  - What is an IDS
  - What is a IPS
  - Difference between IDS & IPS
  - Placement of IDS in the Network
  - Configuring an IDS in the Network
  - Placement of IPS in the Network

    - Configuring an IPS in the Network
- UTM / Next-Generation Firewall
    - What is a UTM
    - Features of UTM
    - Difference between a Firewall & a UTM
    - Placement of UTM in the Network
    - Configuring a UTM in the Network
    - Monitoring attacks using UTM
    - Configuring IPS module in UTM to detect and stop attacks

Counter Measure Techniques for Local Systems

- Identifying the Vulnerabilities of a system
- Understanding the Vulnerabilities of a system
    - CVE ID
    - Bugtraq ID
    -
- Patch Management
    - Identifying the patch for a Vulnerability
    - Downloading the Patch
    - Testing the patch for stability in test environment
    - Deploying the patch to Live Network
- Finding the missing updates in an Operating System
    - Microsoft Baseline Security Analyzer
    - Belarc Advisor

Counter Measure Techniques for Malware Attacks

- Scanning systems for Malware infections
- Types of anti-malwares
    - Anti-Virus
    - Anti-Worm

    - Anti-Trojan
    - Anti-Rootkit
    - Internet Security Suites
- HIDS
- HIPS