Ethical Hacking

Certification Training

Table of Contents

About the Program

This Certified Ethical Hacking course will help you clear the EC Council's CEH v11 certification. It has carefully been designed with help of top Ethical hacker from various major organizations. This CEH certification course will help you master skils sets like system penetration testing, building firewalls, network security and more to become certified Ethical hacker. This Ethical hacking training will help you master methodologies used by the hackers to help you prevent and block security attacks at your organization.

About Intellipaat

Intellipaat is one of the leading online e-learning training providers with more than 600,000 learners across 55+ countries. We are on a mission to democratize education as we believe that everyone has the right to quality education.

Our courses are delivered by subject matter experts from top MNCs, and our world-class pedagogy enables to quickly learn difficult topics in no time. Our 24/7 technical support and career services will help learners jump-start their careers in their dream companies.

Key Features

40 HRS INSTRUCTOR-LED TRAINING

8 HRS SELF-PACED TRAINING

6 Months Access to Cloud Lab

LIFETIME ACCESS

24/7 TECHNICAL SUPPORT

INDUSTRY-RECOGNIZED CERTIFICATION

JOB ASSISTANCE THROUGH 80+ CORPORATE TIE-UPS

FLEXIBLE SCHEDULING

Career Support

SESSIONS WITH INDUSTRY MENTORS

Attend sessions from top industry experts and get guidance on how to boost your career growth

MOCK INTERVIEWS

Mock interviews to make you prepare for cracking interviews by top employers

GUARANTEED INTERVIEWS & JOB SUPPORT

Get interviewed by our 400+ hiring partners

RESUME PREPARATION

Get assistance in creating a world-class resume from our career services team

Why take up this course?

- The United States offers 4,000+ CEH jobs for certified professionals – LinkedIn
- Major companies, like Citibank, Deloitte, Accenture, IBM, Oracle, etc., are mass hiring professionals in Ethical Hacking – Indeed
- The average salary of Ethical Hackers in India is about ₹655k per annum – Glassdoor

.

Who should take up this course?

- Network Security Officers
- Site Administrators
- IT/IS Auditors
- IT Security Officers
- Technical Support Engineers
- IT/IS Analysts and Specialists
- System Analysts
- Network Specialists
- IT Operations Managers
- Senior System Engineers

Program Curriculum

Ethical Hacking Training Course Content

1. Introduction to Ethical Hacking

- Information Security Overview

1.1 Internet is Integral Part of Business and Personal Life – What Happens Online in 60 Seconds

1.2 Essential Terminology

1.3 Elements of Information Security

1.4 The Security, Functionality, and Usability Triangle

- Information Security Threats and Attack Vectors

1.5 Motives, Goals, and Objectives of Information Security Attacks

1.6 Top Information Security Attack Vectors

1.7 Information Security Threat Categories

1.8 Types of Attacks on a System

1.9 Information Warfare

- Hacking Concepts

1.10 What is Hacking?

1.11Who is a Hacker?

1.12 Hacker Classes

1.13 Hacking Phases

  - Reconnaissance
  - Scanning
  - Gaining Access
  - Maintaining Access
  - Clearing Tracks

- Ethical Hacking Concepts

1.14 What is Ethical Hacking?

1.15 Why Ethical Hacking is Necessary

1.16 Scope and Limitations of Ethical Hacking

1.17 Skills of an Ethical Hacker

- Information Security Controls

1.18 Information Assurance (IA)

1.19 Information Security Management Program

1.20 Enterprise Information Security Architecture (EISA)

1.21 Network Security Zoning

1.22 Defense-in-Depth

1.23 Information Security Policies

  - Types of Security Policies
  - Examples of Security Policies
  - Privacy Policies at Workplace
  - Steps to Create and Implement Security Policies
  - HR/Legal Implications of Security Policy Enforcement

1.24 Physical Security

  - Types of Physical Security Control
  - Physical Security Controls

1.25 What is Risk?

  - Risk Management
  - Key Roles and Responsibilities in Risk Management

1.26 Threat Modeling

1.27 Incident Management

  - Incident Management Process
  - Responsibilities of an Incident Response Team

1.28 Security Incident and Event Management (SIEM)

  - SIEM Architecture

1.29 User Behavior Analytics (UBA)

1.30 Network Security Controls

- Access Control
- Types of Access Control
- User Identification, Authentication, Authorization and Accounting

1.31 Identity and Access Management (IAM)

1.32 Data Leakage

- Data Leakage Threats
- What is Data Loss Prevention (DLP)?

1.33 Data Backup

1.34 Data Recovery

1.35 Role of AI/ML in Cyber Security

- Penetration Testing Concepts

1.36 Penetration Testing

1.37 Why Penetration Testing

1.38 Comparing Security Audit, Vulnerability Assessment, and Penetration Testing

1.39 Blue Teaming/Red Teaming

1.40 Types of Penetration Testing

1.41 Phases of Penetration Testing

1.42 Security Testing Methodology

- Information Security Laws and Standards

1.43 Payment Card Industry Data Security Standard (PCI-DSS)

1.44 ISO/IEC 27001:2013

1.45 Health Insurance Portability and Accountability Act (HIPAA)

1.46 Sarbanes Oxley Act (SOX)

1.47 The Digital Millennium Copyright Act (DMCA)

1.48 Federal Information Security Management Act (FISMA)

1.49 Cyber Law in Different Countries

2. Footprinting and Reconnaissance

- Footprinting Concepts

2.1 What is Footprinting?

2.2 Objectives of Footprinting

- Footprinting through Search Engines

2.3 Footprinting through Search Engines

2.4 Footprint Using Advanced Google Hacking Techniques

2.5 Information Gathering Using Google Advanced Search and Image Search

2.6 Google Hacking Database

2.7 VoIP and VPN Footprinting through Google Hacking Database

- Footprinting through Web Services

2.8 Finding Company’s Top-level Domains (TLDs) and Sub-domains

2.9 Finding the Geographical Location of the Target

2.10 People Search on Social Networking Sites and People Search Services

2.11 Gathering Information from LinkedIn

2.12 Gather Information from Financial Services

2.13 Footprinting through Job Sites

2.14 Monitoring Target Using Alerts

2.15 Information Gathering Using Groups, Forums, and Blogs

2.16 Determining the Operating System

2.17 VoIP and VPN Footprinting through SHODAN

- Footprinting through Social Networking Sites

2.18 Collecting Information through Social Engineering on Social Networking Sites

- Website Footprinting

2.19 Website Footprinting

2.20 Website Footprinting using Web Spiders

2.21 Mirroring Entire Website

2.22 Extracting Website Information from https://archive.org

2.23 Extracting Metadata of Public Documents

2.24 Monitoring Web Pages for Updates and Changes

- Email Footprinting

2.25 Tracking Email Communications

2.26 Collecting Information from Email Header

2.27 Email Tracking Tools

- Competitive Intelligence

2.28 Competitive Intelligence Gathering

2.29 Competitive Intelligence – When Did this Company Begin? How Did it Develop?

2.30 Competitive Intelligence – What Are the Company's Plans?

2.31 Competitive Intelligence – What Expert Opinions Say About the Company

2.32 Monitoring Website Traffic of Target Company

2.33 Tracking Online Reputation of the Target

- Whois Footprinting

2.34 Whois Lookup

2.35 Whois Lookup Result Analysis

2.36 Whois Lookup Tools

2.37 Finding IP Geolocation Information

- DNS Footprinting

2.38 Extracting DNS Information

2.39 DNS Interrogation Tools

- Network Footprinting

2.40 Locate the Network Range

2.41 Traceroute

2.42 Traceroute Analysis

2.43 Traceroute Tools

- Footprinting through Social Engineering

2.44 Footprinting through Social Engineering

2.45 Collect Information Using Eavesdropping, Shoulder Surfing, and Dumpster Diving

- Footprinting Tools

2.46 Maltego

2.47 Recon-ng

2.48 FOCA

2.49 Recon-Dog

2.50 OSRFramework

2.51 Additional Footprinting Tools

- Countermeasures

2.52 Footprinting Countermeasures

- Footprinting Pen Testing

2.53 Footprinting Pen Testing

2.54 Footprinting Pen Testing Report Templates

3. Scanning Networks

- Network Scanning Concepts

3.1 Overview of Network Scanning

3.2 TCP Communication Flags

3.3 TCP/IP Communication

3.4 Creating Custom Packet Using TCP Flags

3.5 Scanning in IPv6 Networks

- Scanning Tools

3.6 Nmap

3.7 Hping2 / Hping3

  - Hping Commands

3.8 Scanning Tools

3.9 Scanning Tools for Mobile

- Scanning Techniques

3.10 Scanning Techniques

  - ICMP Scanning – Checking for Live Systems
  - Ping Sweep – Checking for Live Systems
    - Ping Sweep Tools

    - ICMP Echo Scanning
    - TCP Connect / Full Open Scan
    - Stealth Scan (Half-open Scan)
    - Inverse TCP Flag Scanning
    - Xmas Scan
    - ACK Flag Probe Scanning
    - IDLE/IPID Header Scan
    - UDP Scanning
    - SSDP and List Scanning
    - Port Scanning Countermeasures
- Scanning Beyond IDS and Firewall

3.11 IDS/Firewall Evasion Techniques

- Packet Fragmentation
- Source Routing
- IP Address Decoy
- IP Address Spoofing
    - IP Spoofing Detection Techniques: Direct TTL Probes
    - IP Spoofing Detection Techniques: IP Identification Number
    - IP Spoofing Detection Techniques: TCP Flow Control Method
    - IP Spoofing Countermeasures
- Proxy Servers
    - Proxy Chaining
    - Proxy Tools
    - Proxy Tools for Mobile
- Anonymizers

    - Censorship Circumvention Tools: Alkasir and Tails
    - Anonymizers
    - Anonymizers for Mobile

- Banner Grabbing

  3.12 Banner Grabbing
  3.13 How to Identify Target System OS
  3.14 Banner Grabbing Countermeasures

- Draw Network Diagrams

  3.15 Drawing Network Diagrams
  3.16 Network Discovery and Mapping Tools
  3.17 Network Discovery Tools for Mobile

- Scanning Pen Testing

  3.18 Scanning Pen Testing

4. Enumeration

- Enumeration Concepts

  4.1 What is Enumeration?
  4.2 Techniques for Enumeration
  4.3 Services and Ports to Enumerate

- NetBIOS Enumeration

  4.4 NetBIOS Enumeration
  4.5 NetBIOS Enumeration Tools
  4.6 Enumerating User Accounts
  4.7 Enumerating Shared Resources Using Net View

- SNMP Enumeration

  4.8 SNMP (Simple Network Management Protocol) Enumeration
  4.9 Working of SNMP
  4.10 Management Information Base (MIB)
  4.11 SNMP Enumeration Tools

- LDAP Enumeration

  4.12 LDAP Enumeration
  4.13 LDAP Enumeration Tools

- NTP Enumeration

  4.14 NTP Enumeration
  4.15 NTP Enumeration Commands
  4.16 NTP Enumeration Tools

- SMTP and DNS Enumeration

  4.17 SMTP Enumeration
  4.18 SMTP Enumeration Tools
  4.19 DNS Enumeration Using Zone Transfer

- Other Enumeration Techniques

  4.20 IPsec Enumeration
  4.21 VoIP Enumeration
  4.22 RPC Enumeration
  4.23 Unix/Linux User Enumeration

- Enumeration Countermeasures

  4.24 Enumeration Countermeasures

- Enumeration Pen Testing

  4.25 Enumeration Pen Testing

5. Vulnerability Analysis

- Vulnerability Assessment Concepts

  5.1 Vulnerability Research
  5.2 Vulnerability Classification
  5.3 What is Vulnerability Assessment?
  5.4 Types of Vulnerability Assessment
  5.5 Vulnerability-Management Life Cycle

- Pre-Assessment Phase: Creating a Baseline
- Vulnerability Assessment Phase
- Post Assessment Phase

- Vulnerability Assessment Solutions

5.6 Comparing Approaches to Vulnerability Assessment
5.7 Working of Vulnerability Scanning Solutions
5.8 Types of Vulnerability Assessment Tools
5.9 Characteristics of a Good Vulnerability Assessment Solution
5.10 Choosing a Vulnerability Assessment Tool
5.11 Criteria for Choosing a Vulnerability Assessment Tool
5.12 Best Practices for Selecting Vulnerability Assessment Tools

- Vulnerability Scoring Systems

5.13 Common Vulnerability Scoring System (CVSS)
5.14 Common Vulnerabilities and Exposures (CVE)
5.15 National Vulnerability Database (NVD)
5.16 Resources for Vulnerability Research

- Vulnerability Assessment Tools

5.17 Vulnerability Assessment Tools

- Qualys Vulnerability Management
- Nessus Professional
- GFI LanGuard
- Qualys FreeScan
- Nikto
- OpenVAS
- Retina CS
- SAINT
- Microsoft Baseline Security Analyzer (MBSA)
- AVDS – Automated Vulnerability Detection System

    - Vulnerability Assessment Tools

  5.18 Vulnerability Assessment Tools for Mobile

- Vulnerability Assessment Reports

  5.19 Vulnerability Assessment Reports
  5.20 Analyzing Vulnerability Scanning Report

6. System Hacking

- System Hacking Concepts

  6.1 CEH Hacking Methodology (CHM)
  6.2 System Hacking Goals

- Cracking Passwords

  6.3 Password Cracking
  6.4 Types of Password Attacks

    - Non-Electronic Attacks
    - Active Online Attack
        - Dictionary, Brute Forcing and Rule-based Attack
        - Password Guessing
        - Default Passwords
        - Trojan/Spyware/Keylogger
        - Example of Active Online Attack Using USB Drive
        - Hash Injection Attack
        - LLMNR/NBT-NS Poisoning
    - Passive Online Attack
        - Wire Sniffing
        - Man-in-the-Middle and Replay Attack
    - Offline Attack
        - Rainbow Table Attack

        - Tools to Create Rainbow Tables: rtgen and Winrtgen
        - Distributed Network Attack

6.5 Password Recovery Tools

6.6 Microsoft Authentication

6.7 How Hash Passwords Are Stored in Windows SAM?

6.8 NTLM Authentication Process

6.9 Kerberos Authentication

6.10 Password Salting

6.11 Tools to Extract the Password Hashes

6.12 Password Cracking Tools

6.13 How to Defend against Password Cracking

6.14 How to Defend against LLMNR/NBT-NS Poisoning

- Escalating Privileges

6.15 Privilege Escalation

6.16 Privilege Escalation Using DLL Hijacking

6.17 Privilege Escalation by Exploiting Vulnerabilities

6.18 Privilege Escalation Using Dylib Hijacking

6.19 Privilege Escalation using Spectre and Meltdown Vulnerabilities

6.20 Other Privilege Escalation Techniques

6.21 How to Defend Against Privilege Escalation

- Executing Applications

6.22 Executing Applications

    - Tools for Executing Applications

6.23 Keylogger

    - Types of Keystroke Loggers
    - Hardware Keyloggers
    - Keyloggers for Windows
    - Keyloggers for Mac

6.24 Spyware

- Spyware
- USB Spyware
- Audio Spyware
- Video Spyware
- Telephone/Cellphone Spyware
- GPS Spyware

6.25 How to Defend Against Keyloggers

- Anti-Keylogger

6.26 How to Defend Against Spyware

- Anti-Spyware

- Hiding Files

6.27 Rootkits

- Types of Rootkits
- How Rootkit Works
- Rootkits
  - Horse Pill
  - GrayFish
  - Sirefef
  - Necurs
- Detecting Rootkits
- Steps for Detecting Rootkits
- How to Defend against Rootkits
- Anti-Rootkits

6.28 NTFS Data Stream

- How to Create NTFS Streams
- NTFS Stream Manipulation
- How to Defend against NTFS Streams
- NTFS Stream Detectors

6.29 What is Steganography?

- Classification of Steganography
- Types of Steganography based on Cover Medium
    - Whitespace Steganography
    - Image Steganography
        - Image Steganography Tools
    - Document Steganography
    - Video Steganography
    - Audio Steganography
    - Folder Steganography
    - Spam/Email Steganography
- Steganography Tools for Mobile Phones
- Steganalysis
- Steganalysis Methods/Attacks on Steganography
- Detecting Steganography (Text, Image, Audio, and Video Files)
- Steganography Detection Tools
- Covering Tracks

6.31 Disabling Auditing: Auditpol
6.32 Clearing Logs
6.33 Manually Clearing Event Logs
6.34 Ways to Clear Online Tracks
6.35 Covering BASH Shell Tracks

6.36 Covering Tracks on Network

6.37 Covering Tracks on OS

6.38 Covering Tracks Tools

- Penetration Testing

6.39 Password Cracking

6.40 Privilege Escalation

6.41 Executing Applications

6.42 Hiding Files

6.43 Covering Tracks

7. **Malware Threats**

- Malware Concepts

7.1 Introduction to Malware

7.2 Different Ways a Malware can Get into a System

7.3 Common Techniques Attackers Use to Distribute Malware on the Web

7.4 Components of Malware

- Trojan Concepts

7.5 What is a Trojan?

7.6 How Hackers Use Trojans

7.7 Common Ports used by Trojans

7.8 How to Infect Systems Using a Trojan

7.9 Trojan Horse Construction Kit

7.10 Wrappers

7.11 Crypters

7.12 How Attackers Deploy a Trojan

7.13 Exploit Kits

7.14 Evading Anti-Virus Techniques

7.15 Types of Trojans

  - Remote Access Trojans
  - Backdoor Trojans
  - Botnet Trojans

        - Rootkit Trojans
        - E-banking Trojans
            - Working of E-banking Trojans
            - E-banking Trojan: ZeuS
        - Proxy Server Trojans
        - Covert Channel Trojans
        - Defacement Trojans
        - Service Protocol Trojans
        - Mobile Trojans
        - IoT Trojans
        - Other Trojans

- Virus and Worm Concepts

7.16 Introduction to Viruses
7.17 Stages of Virus Life
7.18 Working of Viruses
7.19 Indications of Virus Attack
7.20 How does a Computer Get Infected by Viruses
7.21 Virus Hoaxes
7.22 Fake Antiviruses
7.23 Ransomware
7.24 Types of Viruses

    - System and File Viruses
    - Multipartite and Macro Viruses
    - Cluster and Stealth Viruses
    - Encryption and Sparse Infector Viruses
    - Polymorphic Viruses

- Metamorphic Viruses
- Overwriting File or Cavity Viruses
- Companion/Camouflage and Shell Viruses
- File Extension Viruses
- FAT and Logic Bomb Viruses
- Web Scripting and E-mail Viruses
- Other Viruses

7.25 Creating Virus
7.26 Computer Worms
7.27 Worm Makers

1. Malware Analysis

7.28 What is Sheep Dip Computer?
7.29 Anti-Virus Sensor Systems
7.30 Introduction to Malware Analysis
7.31 Malware Analysis Procedure: Preparing Testbed
7.32 Static Malware Analysis

1.18.1 File Fingerprinting

1.18.2 Local and Online Malware Scanning

1.18.3 Performing Strings Search

1.18.4 Identifying Packing/ Obfuscation Methods

1.18.5 Finding the Portable Executables (PE) Information

1.18.6 Identifying File Dependencies

1.18.7 Malware Disassembly

7.33 Dynamic Malware Analysis

1.18.8 Port Monitoring

1.18.9 Process Monitoring

1.18.10 Registry Monitoring

1.18.11 Windows Services Monitoring

1.18.12 Startup Programs Monitoring

1.18.13 Event Logs Monitoring/Analysis

1.18.14 Installation Monitoring

1.18.15 Files and Folder Monitoring

1.18.16 Device Drivers Monitoring

1.18.17 Network Traffic Monitoring/Analysis

1.18.18 DNS Monitoring/ Resolution

1.18.19 API Calls Monitoring

7.34 Virus Detection Methods
7.35 Trojan Analysis: ZeuS/Zbot
7.36 Virus Analysis: WannaCry

2. Countermeasures

7.37 Trojan Countermeasures
7.38 Backdoor Countermeasures
7.39 Virus and Worms Countermeasures

3. Anti-Malware Software

7.40 Anti-Trojan Software
7.41 Antivirus Software

4. Malware Penetration Testing

7.42 Malware Penetration Testing

8. **Sniffing**

Sniffing Concepts

8.1 Network Sniffing
8.2 Types of Sniffing
8.3 How an Attacker Hacks the Network Using Sniffers

8.4 Protocols Vulnerable to Sniffing

8.5 Sniffing in the Data Link Layer of the OSI Model

8.6 Hardware Protocol Analyzers

8.7 SPAN Port

8.8 Wiretapping

8.9 Lawful Interception

Sniffing Technique: MAC Attacks

8.10 MAC Address/CAM Table

8.11 How CAM Works

8.12 What Happens When CAM Table Is Full?

8.13 MAC Flooding

8.14 Switch Port Stealing

8.15 How to Defend against MAC Attacks

Sniffing Technique: DHCP Attacks

8.16 How DHCP Works

8.17 DHCP Request/Reply Messages

8.18 DHCP Starvation Attack

8.19 Rogue DHCP Server Attack

8.20 How to Defend Against DHCP Starvation and Rogue Server Attack

Sniffing Technique: ARP Poisoning

8.21 What Is Address Resolution Protocol (ARP)?

8.22 ARP Spoofing Attack

8.23 Threats of ARP Poisoning

8.24 ARP Poisoning Tools

8.25 How to Defend Against ARP Poisoning

8.26 Configuring DHCP Snooping and Dynamic ARP Inspection on Cisco Switches

8.27 ARP Spoofing Detection Tools

Sniffing Technique: Spoofing Attacks

8.28 MAC Spoofing/Duplicating

8.29 MAC Spoofing Technique: Windows

8.30 MAC Spoofing Tools

8.31 IRDP Spoofing

8.32 How to Defend Against MAC Spoofing

Sniffing Technique: DNS Poisoning

8.33 DNS Poisoning Techniques

- Intranet DNS Spoofing
- Internet DNS Spoofing
- Proxy Server DNS Poisoning
- DNS Cache Poisoning

8.34 How to Defend Against DNS Spoofing

Sniffing Tools

8.35 Sniffing Tool: Wireshark

- Follow TCP Stream in Wireshark

8.36 Display Filters in Wireshark

8.37 Additional Wireshark Filters

8.38 Sniffing Tools

8.39 Packet Sniffing Tools for Mobile

Countermeasures

8.40 How to Defend Against Sniffing

Sniffing Detection Techniques

8.41 How to Detect Sniffing

8.42 Sniffer Detection Techniques

- Ping Method
- DNS Method
- ARP Method

8.43 Promiscuous Detection Tools

- Sniffing Pen Testing

8.44 Sniffing Penetration Testing

9. **Social Engineering**

Social Engineering Concepts

9.1 What is Social Engineering?

9.2 Phases of a Social Engineering Attack

Social Engineering Techniques

9.3 Types of Social Engineering

9.4 Human-based Social Engineering

- Impersonation
- Impersonation (Vishing)
- Eavesdropping
- Shoulder Surfing
- Dumpster Diving
- Reverse Social Engineering
- Piggybacking
- Tailgating

9.5 Computer-based Social Engineering

- Phishing

9.6 Mobile-based Social Engineering

- Publishing Malicious Apps
- Repackaging Legitimate Apps
- Fake Security Applications
- SMiShing (SMS Phishing)

Insider Threats

9.7 Insider Threat / Insider Attack

9.8 Type of Insider Threats

Impersonation on Social Networking Sites

9.9 Social Engineering Through Impersonation on Social Networking Sites

9.10 Impersonation on Facebook

9.11 Social Networking Threats to Corporate Networks

Identity Theft

9.12 Identity Theft

Countermeasures

9.13 Social Engineering Countermeasures

9.14 Insider Threats Countermeasures

9.15 Identity Theft Countermeasures

9.16 How to Detect Phishing Emails?

9.17 Anti-Phishing Toolbar

9.18 Common Social Engineering Targets and Defense Strategies

Social Engineering Pen Testing

9.19 Social Engineering Pen Testing

- Using Emails
- Using Phone
- In Person

9.20 Social Engineering Pen Testing Tools

10. **Denial-of-Service**

DoS/DDoS Concepts

10.1 What is a Denial-of-Service Attack?

10.2 What is Distributed Denial-of-Service Attack?

DoS/DDoS Attack Techniques

10.3 Basic Categories of DoS/DDoS Attack Vectors

10.4 UDP Flood Attack

10.5 ICMP Flood Attack

10.6 Ping of Death and Smurf Attack

10.7 SYN Flood Attack

10.8 Fragmentation Attack

10.9 HTTP GET/POST and Slowloris Attacks

10.10 Multi-Vector Attack

10.11 Peer-to-Peer Attacks

10.12 Permanent Denial-of-Service Attack

10.13 Distributed Reflection Denial-of-Service (DRDoS)

Botnets

10.14 Organized Cyber Crime: Organizational Chart

10.15 Botnet

10.16 A Typical Botnet Setup

10.17 Botnet Ecosystem

10.18 Scanning Methods for Finding Vulnerable Machines

10.19 How Malicious Code Propagates?

10.20 Botnet Trojans

DDoS Case Study

10.21 DDoS Attack

10.22 Hackers Advertise Links to Download Botnet

10.23 Use of Mobile Devices as Botnets for Launching DDoS Attacks

10.24 DDoS Case Study: Dyn DDoS Attack

DoS/DDoS Attack Tools

10.25 DoS/DDoS Attack Tools

10.26 DoS and DDoS Attack Tool for Mobile

Countermeasures

10.27 Detection Techniques

10.28 DoS/DDoS Countermeasure Strategies

10.29 DDoS Attack Countermeasures

- Protect Secondary Victims
- Detect and Neutralize Handlers
- Prevent Potential Attacks

- Deflect Attacks
- Mitigate Attacks
- Post-Attack Forensics

10.30 Techniques to Defend against Botnets

10.31 DoS/DDoS Countermeasures

10.32 DoS/DDoS Protection at ISP Level

10.33 Enabling TCP Intercept on Cisco IOS Software

DoS/DDoS Protection Tools

10.34 Advanced DDoS Protection Appliances

10.35 DoS/DDoS Protection Tools

DoS/DDoS Penetration Testing

10.36 Denial-of-Service (DoS) Attack Pen Testing

11. Session Hijacking

Session Hijacking Concepts

11.1 What is Session Hijacking?

11.2 Why Session Hijacking is Successful?

11.3 Session Hijacking Process

11.4 Packet Analysis of a Local Session Hijack

11.5 Types of Session Hijacking

11.6 Session Hijacking in OSI Model

11.7 Spoofing vs. Hijacking

Application Level Session Hijacking

11.8 Application Level Session Hijacking

11.9 Compromising Session IDs using Sniffing and by Predicting Session Token

How to Predict a Session Token

11.10 Compromising Session IDs Using Man-in-the-Middle Attack

11.11 Compromising Session IDs Using Man-in-the-Browser Attack

- Steps to Perform Man-in-the-Browser Attack

11.12 Compromising Session IDs Using Client-side Attacks

11.13 Compromising Session IDs Using Client-side Attacks: Cross-site Script Attack

11.14 Compromising Session IDs Using Client-side Attacks: Cross-site Request Forgery Attack

11.15 Compromising Session IDs Using Session Replay Attack

11.16 Compromising Session IDs Using Session Fixation

11.17 Session Hijacking Using Proxy Servers

11.18 Session Hijacking Using CRIME Attack

11.19 Session Hijacking Using Forbidden Attack

Network Level Session Hijacking

11.20 TCP/IP Hijacking

11.21 IP Spoofing: Source Routed Packets

11.22 RST Hijacking

11.23 Blind Hijacking

11.24 UDP Hijacking

11.25 MiTM Attack Using Forged ICMP and ARP Spoofing

Session Hijacking Tools

11.26 Session Hijacking Tools

11.27 Session Hijacking Tools for Mobile

Countermeasures

11.28 Session Hijacking Detection Methods

11.29 Protecting against Session Hijacking

11.30 Methods to Prevent Session Hijacking: To be Followed by Web Developers

11.31 Methods to Prevent Session Hijacking: To be Followed by Web Users

11.32 Session Hijacking Detection Tools

11.33 Approaches Vulnerable to Session Hijacking and their Preventative Solutions

11.34 Approaches to Prevent Session Hijacking

11.35 IPSec

- Components of IPsec

- Benefits of IPsec

- Modes of IPsec
- IPsec Architecture
- IPsec Authentication and Confidentiality

11.36 Session Hijacking Prevention Tools

Penetration Testing

11.37 Session Hijacking Pen Testing

12. Evading IDS, Firewalls, and Honeypots

IDS, Firewall and Honeypot Concepts

12.1 Intrusion Detection System (IDS)

- How IDS Detects an Intrusion
- General Indications of Intrusions
- Types of Intrusion Detection Systems
- Types of IDS Alerts

12.2 Firewall

- Firewall Architecture
- DeMilitarized Zone (DMZ)
- Types of Firewalls
- Firewall Technologies
- Packet Filtering Firewall
- Circuit-Level Gateway Firewall
- Application-Level Firewall
- Stateful Multilayer Inspection Firewall
- Application Proxy
- Network Address Translation (NAT)
- Virtual Private Network

- Firewall Limitations

12.3 Honeypot

- Types of Honeypots
- IDS, Firewall and Honeypot Solutions

12.4 Intrusion Detection Tool

- Snort
- Snort Rules
- Snort Rules: Rule Actions and IP Protocols
- Snort Rules: The Direction Operator and IP Addresses
- Snort Rules: Port Numbers
- Intrusion Detection Tools: TippingPoint and AlienVault® OSSIM™
- Intrusion Detection Tools
- Intrusion Detection Tools for Mobile

12.5 Firewalls

- ZoneAlarm Free Firewall 2018 and Firewall Analyzer
- Firewalls
- Firewalls for Mobile

12.6 Honeypot Tools

- KFSensor and SPECTER
- Honeypot Tools
- Honeypot Tools for Mobile
- Evading IDS

12.7 IDS Evasion Techniques

- Insertion Attack
- Evasion

- Denial-of-Service Attack (DoS)
- Obfuscating
- False Positive Generation
- Session Splicing
- Unicode Evasion
- Fragmentation Attack
- Overlapping Fragments
- Time-To-Live Attacks
- Invalid RST Packets
- Urgency Flag
- Polymorphic Shellcode
- ASCII Shellcode
- Application-Layer Attacks
- Desynchronization
- Other Types of Evasion
- Evading Firewalls

12.8 Firewall Evasion Techniques

- Firewall Identification
- IP Address Spoofing
- Source Routing
- Tiny Fragments
- Bypass Blocked Sites Using IP Address in Place of URL
- Bypass Blocked Sites Using Anonymous Website Surfing Sites
- Bypass a Firewall Using Proxy Server
- Bypassing Firewall through ICMP Tunneling Method

- Bypassing Firewall through ACK Tunneling Method
- Bypassing Firewall through HTTP Tunneling Method
- Why do I Need HTTP Tunneling
- HTTP Tunneling Tools
- Bypassing Firewall through SSH Tunneling Method
- SSH Tunneling Tool: Bitvise and Secure Pipes
- Bypassing Firewall through External Systems
- Bypassing Firewall through MITM Attack
- Bypassing Firewall through Content
- Bypassing WAF using XSS Attack
- IDS/Firewall Evading Tools

12.9 IDS/Firewall Evasion Tools
12.10 Packet Fragment Generator Tools

- Detecting Honeypots

12.11 Detecting Honeypots
12.12 Detecting and Defeating Honeypots
12.13 Honeypot Detection Tool: Send-Safe Honeypot Hunter

- IDS/Firewall Evasion Countermeasures

12.14 How to Defend Against IDS Evasion
12.15 How to Defend Against Firewall Evasion

- Penetration Testing

12.16 Firewall/IDS Penetration Testing

- Firewall Penetration Testing
- IDS Penetration Testing

13. Hacking Web Servers

Web Server Concepts

13.1 Web Server Operations

13.2 Open Source Web Server Architecture

13.3 IIS Web Server Architecture

13.4 Web Server Security Issue

13.5 Why Web Servers Are Compromised?

13.6 Impact of Web Server Attacks

Web Server Attacks

13.7 DoS/DDoS Attacks

13.8 DNS Server Hijacking

13.9 DNS Amplification Attack

13.10 Directory Traversal Attacks

13.11 Man-in-the-Middle/Sniffing Attack

13.12 Phishing Attacks

13.13 Website Defacement

13.14 Web Server Misconfiguration

13.15 HTTP Response Splitting Attack

13.16 Web Cache Poisoning Attack

13.17 SSH Brute Force Attack

13.18 Web Server Password Cracking

13.19 Web Application Attacks

Web Server Attack Methodology

13.20 Information Gathering

- Information Gathering from Robots.txt File

13.21 Web Server Footprinting/Banner Grabbing

- Web Server Footprinting Tools
- Enumerating Web Server Information Using Nmap

13.22 Website Mirroring

- Finding Default Credentials of Web Server
- Finding Default Content of Web Server
- Finding Directory Listings of Web Server

13.23 Vulnerability Scanning

- Finding Exploitable Vulnerabilities

13.24 Session Hijacking

13.25 Web Server Passwords Hacking

13.26 Using Application Server as a Proxy

Web Server Attack Tools

13.27 Metasploit

- Metasploit Exploit Module
- Metasploit Payload and Auxiliary Module
- Metasploit NOPS Module
- 13.28 Web Server Attack Tools
- Countermeasures

13.29 Place Web Servers in Separate Secure Server Security Segment on Network

13.30 Countermeasures

- Patches and Updates
- Protocols
- Accounts
- Files and Directories

13.31 Detecting Web Server Hacking Attempts

13.32 How to Defend Against Web Server Attacks

13.33 How to Defend against HTTP Response Splitting and Web Cache Poisoning

13.34 How to Defend against DNS Hijacking

- Patch Management

13.35 Patches and Hotfixes

13.36 What is Patch Management

13.37 Installation of a Patch

13.38 Patch Management Tools

- Web Server Security Tools

13.39 Web Application Security Scanners

13.40 Web Server Security Scanners

13.41 Web Server Security Tools

- Web Server Pen Testing

13.42 Web Server Penetration Testing

13.43 Web Server Pen Testing Tools

14. Hacking Web Applications

Web App Concepts

14.1 Introduction to Web Applications

14.2 Web Application Architecture

14.3 Web 2.0 Applications

14.4 Vulnerability Stack

Web App Threats

14.5 OWASP Top 10 Application Security Risks – 2017

A1 – Injection Flaws

- SQL Injection Attacks
- Command Injection Attacks
- Command Injection Example
- File Injection Attack
- LDAP Injection Attacks

A2 – Broken Authentication

A3 – Sensitive Data Exposure

A4 – XML External Entity (XXE)

A5 – Broken Access Control

A6 – Security Misconfiguration

A7 – Cross-Site Scripting (XSS) Attacks

- Cross-Site Scripting Attack Scenario: Attack via Email
- XSS Attack in Blog Posting
- XSS Attack in Comment Field
- Websites Vulnerable to XSS Attack

A8 – Insecure Deserialization

A9 – Using Components with Known Vulnerabilities

A10 – Insufficient Logging and Monitoring

14.6 Other Web Application Threats

- Directory Traversal
- Unvalidated Redirects and Forwards
- Watering Hole Attack
- Cross-Site Request Forgery (CSRF) Attack
- Cookie/Session Poisoning
- Web Services Architecture
- Web Services Attack
- Web Services Footprinting Attack
- Web Services XML Poisoning
- Hidden Field Manipulation Attack
- Hacking Methodology

14.7 Web App Hacking Methodology

14.8 Footprint Web Infrastructure

- Server Discovery

- Service Discovery
- Server Identification/Banner Grabbing
- Detecting Web App Firewalls and Proxies on Target Site
- Hidden Content Discovery
- Web Spidering Using Burp Suite
- Web Crawling Using Mozenda Web Agent Builder

14.9 Attack Web Servers

14.10 Analyze Web Applications

- Identify Entry Points for User Input
- Identify Server- Side Technologies
- Identify Server- Side Functionality
- Map the Attack Surface

14.11 Bypass Client-Side Controls

- Attack Hidden Form Fields
- Attack Browser Extensions
- Perform Source Code Review

14.12 Attack Authentication Mechanism

User Name Enumeration

- Password Attacks: Password Functionality Exploits
- Password Attacks: Password Guessing and Brute-forcing
- Session Attacks: Session ID Prediction/Brute-forcing
- Cookie Exploitation: Cookie Poisoning

14.13 Attack Authorization Schemes

- HTTP Request Tampering
- Cookie Parameter Tampering

14.14 Attack Access Controls

14.15 Attack Session Management Mechanism

- Attacking Session Token Generation Mechanism
- Attacking Session Tokens Handling Mechanism: Session Token Sniffing

14.16 Perform Injection/Input Validation Attacks

14.17 Attack Application Logic Flaws

14.18 Attack Database Connectivity

- Connection String Injection
- Connection String Parameter Pollution (CSPP) Attacks
- Connection Pool DoS

14.19 Attack Web App Client

14.20 Attack Web Services

- Web Services Probing Attacks
- Web Service Attacks: SOAP Injection
- Web Service Attacks: XML Injection
- Web Services Parsing Attacks
- Web Service Attack Tools
- Web App Hacking Tools

14.21 Web Application Hacking Tools

Countermeasures

14.22 Web Application Fuzz Testing

14.23 Source Code Review

14.24 Encoding Schemes

14.25 How to Defend Against Injection Attacks

14.26 Web Application Attack Countermeasures

14.27 How to Defend Against Web Application Attacks

Web App Security Testing Tools

14.28 Web Application Security Testing Tools

14.29 Web Application Firewall

Web App Pen Testing

14.30 Web Application Pen Testing

- Information Gathering
- Configuration Management Testing
- Authentication Testing
- Session Management Testing
- Authorization Testing
- Data Validation Testing
- Denial-of-Service Testing
- Web Services Testing
- AJAX Testing

14.31 Web Application Pen Testing Framework

15. SQL Injection

SQL Injection Concepts

15.1 What is SQL Injection?

15.2 SQL Injection and Server-side Technologies

15.3 Understanding HTTP POST Request

15.4 Understanding Normal SQL Query

15.5 Understanding an SQL Injection Query

15.6 Understanding an SQL Injection Query – Code Analysis

15.7 Example of a Web Application Vulnerable to SQL Injection: aspx

15.8 Example of a Web Application Vulnerable to SQL Injection: Attack Analysis

15.9 Examples of SQL Injection

Types of SQL Injection

15.10 Types of SQL injection

- In-Band SQL Injection
- Error Based SQL Injection
- Union SQL Injection
- Blind/Inferential SQL Injection
- No Error Messages Returned
- Blind SQL Injection: WAITFOR DELAY (YES or NO Response)
- Blind SQL Injection: Boolean Exploitation and Heavy Query
- Out-of-Band SQL injection
- SQL Injection Methodology

15.11 SQL Injection Methodology

- Information Gathering and SQL Injection Vulnerability Detection
- Information Gathering
- Identifying Data Entry Paths
- Extracting Information through Error Messages
- Testing for SQL Injection
- Additional Methods to Detect SQL Injection
- SQL Injection Black Box Pen Testing
- Source Code Review to Detect SQL Injection Vulnerabilities
- Testing for Blind SQL Injection Vulnerability in MySQL and MSSQL
- Launch SQL Injection Attacks
- Perform Union SQL Injection
- Perform Error Based SQL Injection
- Perform Error Based SQL Injection using Stored Procedure Injection
- Bypass Website Logins Using SQL Injection

- Perform Blind SQL Injection – Exploitation (MySQL)
- Blind SQL Injection – Extract Database User
- Blind SQL Injection – Extract Database Name
- Blind SQL Injection – Extract Column Name
- Blind SQL Injection – Extract Data from ROWS
- Perform Double Blind SQL Injection – Classical Exploitation (MySQL)
- Perform Blind SQL Injection Using Out of Band Exploitation Technique
- Exploiting Second-Order SQL Injection
- Bypass Firewall using SQL Injection
- Perform SQL Injection to Insert a New User and Update Password
- Exporting a Value with Regular Expression Attack
- Advanced SQL Injection
- Database, Table, and Column Enumeration
- Advanced Enumeration
- Features of Different DBMSs
- Creating Database Accounts
- Password Grabbing
- Grabbing SQL Server Hashes
- Extracting SQL Hashes (In a Single Statement
- Transfer Database to Attacker's Machine
- Interacting with the Operating System
- Interacting with the File System
- Network Reconnaissance Using SQL Injection
- Finding and Bypassing Admin Panel of a Website
- PL/SQL Exploitation

- Creating Server Backdoors using SQL Injection
- SQL Injection Tools

15.12 SQL Injection Tools

- SQL Power Injector and sqlmap
- The Mole and jSQL Injection

15.13 SQL Injection Tools

15.14 SQL Injection Tools for Mobile

- Evasion Techniques

15.15 Evading IDS

15.16 Types of Signature Evasion Techniques

- In-line Comment
- Char Encoding
- String Concatenation
- Obfuscated Codes
- Manipulating White Spaces
- Hex Encoding
- Sophisticated Matches
- URL Encoding
- Null Byte
- Case Variation
- Declare Variable
- IP Fragmentation
- Countermeasures

15.17 How to Defend Against SQL Injection Attacks

- Use Type-Safe SQL Parameters

15.18 SQL Injection Detection Tools

- IBM Security AppScan and Acunetix Web Vulnerability Scanner
- Snort Rule to Detect SQL Injection Attacks

15.19 SQL Injection Detection Tools

16. Hacking Wireless Networks

Wireless Concepts

16.1 Wireless Terminologies
16.2 Wireless Networks
16.3 Wireless Standards
16.4 Service Set Identifier (SSID)
16.5 Wi-Fi Authentication Modes
16.6 Wi-Fi Authentication Process Using a Centralized Authentication Server
16.7 Types of Wireless Antennas

Wireless Encryption

16.8 Types of Wireless Encryption

- WEP (Wired Equivalent Privacy) Encryption
- WPA (Wi-Fi Protected Access) Encryption
- WPA2 (Wi-Fi Protected Access 2) Encryption

16.9 WEP vs. WPA vs. WPA2
16.10 WEP Issues
16.11 Weak Initialization Vectors (IV)

Wireless Threats

16.12 Wireless Threats

- Rogue Access Point Attack
- Client Mis-association
- Misconfigured Access Point Attack
- Unauthorized Association

- Ad Hoc Connection Attack
- Honeypot Access Point Attack
- AP MAC Spoofing
- Denial-of-Service Attack
- Key Reinstallation Attack (KRACK)
- Jamming Signal Attack
- Wi-Fi Jamming Devices
- Wireless Hacking Methodology

16.13 Wireless Hacking Methodology

- Wi-Fi Discovery
- Footprint the Wireless Network
- Find Wi-Fi Networks in Range to Attack
- Wi-Fi Discovery Tools
- Mobile-based Wi-Fi Discovery Tools
- GPS Mapping
- GPS Mapping Tools
- Wi-Fi Hotspot Finder Tools
- How to Discover Wi-Fi Network Using Wardriving
- Wireless Traffic Analysis
- Choosing the Right Wi-Fi Card
- Wi-Fi USB Dongle: AirPcap
- Wi-Fi Packet Sniffer
- Perform Spectrum Analysis
- Launch Wireless Attacks
- Aircrack-ng Suite

- How to Reveal Hidden SSIDs
- Fragmentation Attack
- How to Launch MAC Spoofing Attack
- Denial-of-Service: Disassociation and Deauthentication Attacks
- Man-in-the-Middle Attack
- MITM Attack Using Aircrack-ng
- Wireless ARP Poisoning Attack
- Rogue Access Points
- Evil Twin
- How to Set Up a Fake Hotspot (Evil Twin)
- Crack Wi-Fi Encryption
- How to Break WEP Encryption
- How to Crack WEP Using Aircrack-ng
- How to Break WPA/WPA2 Encryption
- How to Crack WPA-PSK Using Aircrack-ng
- WEP Cracking and WPA Brute Forcing Using Cain & Abel

Wireless Hacking Tools

16.14 WEP/WPA Cracking Tools
16.15 WEP/WPA Cracking Tool for Mobile
16.16 Wi-Fi Sniffer
16.17 Wi-Fi Traffic Analyzer Tools
16.18 Other Wireless Hacking Tools

Bluetooth Hacking

16.19 Bluetooth Stack
16.20 Bluetooth Hacking
16.21 Bluetooth Threats

16.22 How to BlueJack a Victim

16.23 Bluetooth Hacking Tools

Countermeasures

16.24 Wireless Security Layers

16.25 How to Defend Against WPA/WPA2 Cracking

16.26 How to Defend Against KRACK Attacks

16.27 How to Detect and Block Rogue AP

16.28 How to Defend Against Wireless Attacks

16.29 How to Defend Against Bluetooth Hacking

Wireless Security Tools

16.30 Wireless Intrusion Prevention Systems

16.31 Wireless IPS Deployment

16.32 Wi-Fi Security Auditing Tools

16.33 Wi-Fi Intrusion Prevention System

16.34 Wi-Fi Predictive Planning Tools

16.35 Wi-Fi Vulnerability Scanning Tools

16.36 Bluetooth Security Tools

16.37 Wi-Fi Security Tools for Mobile

Wireless Pen Testing

16.38 Wireless Penetration Testing

16.39 Wireless Penetration Testing Framework

- Pen Testing for General Wi-Fi Network Attack
- Pen Testing WEP Encrypted WLAN
- Pen Testing WPA/WPA2 Encrypted WLAN
- Pen Testing LEAP Encrypted WLAN
- Pen Testing Unencrypted WLAN

17. **Hacking Mobile Platforms**

Mobile Platform Attack Vectors

17.1 Vulnerable Areas in Mobile Business Environment

17.2 OWASP Top 10 Mobile Risks – 2016

17.3 Anatomy of a Mobile Attack

17.4 How a Hacker can Profit from Mobile when Successfully Compromised

17.5 Mobile Attack Vectors and Mobile Platform Vulnerabilities

17.6 Security Issues Arising from App Stores

17.7 App Sandboxing Issues

17.8 Mobile Spam

17.9 SMS Phishing Attack (SMiShing) (Targeted Attack Scan)

SMS Phishing Attack Examples

17.10 Pairing Mobile Devices on Open Bluetooth and Wi-Fi Connections

Hacking Android OS

17.11 Android OS

Android Device Administration API

17.12 Android Rooting

- Rooting Android Using KingoRoot
- Android Rooting Tools

17.13 Blocking Wi-Fi Access using NetCut

17.14 Hacking with zANTI

17.15 Hacking Networks Using Network Spoofer

17.16 Launching DoS Attack using Low Orbit Ion Cannon (LOIC)

17.17 Performing Session Hijacking Using DroidSheep

17.18 Hacking with Orbot Proxy

17.19 Android-based Sniffers

17.20 Android Trojans

17.21 Securing Android Devices

17.22 Android Security Tool: Find My Device

17.23 Android Security Tools

17.24 Android Vulnerability Scanner

17.25 Android Device Tracking Tools

Hacking iOS

17.26 Apple iOS

17.27 Jailbreaking iOS

- Jailbreaking Techniques
- Jailbreaking of iOS 11.2.1 Using Cydia
- Jailbreaking of iOS 11.2.1 Using Pangu Anzhuang
- Jailbreaking Tools

17.28 iOS Trojans

17.29 Guidelines for Securing iOS Devices

17.30 iOS Device Tracking Tools

17.31 iOS Device Security Tools

Mobile Spyware

17.32 Mobile Spyware

17.33 Mobile Spyware: mSpy

17.34 Mobile Spywares

Mobile Device Management

17.35 Mobile Device Management (MDM)

17.36 Mobile Device Management Solutions

17.37 Bring Your Own Device (BYOD)

- BYOD Risks
- BYOD Policy Implementation
- BYOD Security Guidelines

Mobile Security Guidelines and Tools

17.38 General Guidelines for Mobile Platform Security

17.39 Mobile Device Security Guidelines for Administrator

17.40 SMS Phishing Countermeasures

17.41 Mobile Protection Tools

17.42 Mobile Anti-Spyware

Mobile Pen Testing

17.43 Android Phone Pen Testing

17.44 iPhone Pen Testing

17.45 Mobile Pen Testing Toolkit: Hackode

18. IoT Hacking

IoT Concepts

18.1 What is IoT

18.2 How IoT Works

18.3 IoT Architecture

18.4 IoT Application Areas and Devices

18.5 IoT Technologies and Protocols

18.6 IoT Communication Models

18.7 Challenges of IoT

18.8 Threat vs Opportunity

IoT Attacks

18.9 IoT Security Problems

18.10 OWASP Top 10 IoT Vulnerabilities and Obstacles

18.11 IoT Attack Surface Areas

18.12 IoT Threats

18.13 Hacking IoT Devices: General Scenario

18.14 IoT Attacks

- DDoS Attack
- Exploit HVAC
- Rolling Code Attack
- BlueBorne Attack
- Jamming Attack
- Hacking Smart Grid / Industrial Devices: Remote Access using Backdoor
- Other IoT Attacks

18.15 IoT Attacks in Different Sectors

18.16 Case Study: Dyn Attack

IoT Hacking Methodology

- 18.17 What is IoT Device Hacking?
  18.18 IoT Hacking Methodology
- Information Gathering Using Shodan
- Information Gathering using MultiPing
- Vulnerability Scanning using Nmap
- Vulnerability Scanning using RIoT Vulnerability Scanner
- Sniffing using Foren6
- Rolling code Attack using RFCrack
- Hacking Zigbee Devices with Attify Zigbee Framework
- BlueBorne Attack Using HackRF One
- Gaining Remote Access using Telnet
- Maintain Access by Exploiting Firmware
- IoT Hacking Tools

18.19 Information Gathering Tools
18.20 Sniffing Tools
18.21 Vulnerability Scanning Tools
18.22 IoT Hacking Tools

Countermeasures

18.23 How to Defend Against IoT Hacking
18.24 General Guidelines for IoT Device Manufacturing Companies
18.25 OWASP Top 10 IoT Vulnerabilities Solutions
18.26 IoT Framework Security Considerations
18.27 IoT Security Tools

IoT Pen Testing

18.28 IoT Pen Testing

19. Cloud Computing

Cloud Computing Concepts

19.1 Introduction to Cloud Computing

19.2 Separation of Responsibilities in Cloud

19.3 Cloud Deployment Models

19.4 NIST Cloud Deployment Reference Architecture

19.5 Cloud Computing Benefits

19.6 Understanding Virtualization

Cloud Computing Threats

19.7 Cloud Computing Threats

Cloud Computing Attacks

19.8 Service Hijacking using Social Engineering Attacks

19.9 Service Hijacking using Network Sniffing

19.10 Session Hijacking using XSS Attack

19.11 Session Hijacking using Session Riding

19.12 Domain Name System (DNS) Attacks

19.13 Side Channel Attacks or Cross-guest VM Breaches

19.14 SQL Injection Attacks

19.15 Cryptanalysis Attacks

19.16 Wrapping Attack

19.17 Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks

19.18 Man-in-the-Cloud Attack

Cloud Security

19.19 Cloud Security Control Layers

19.20 Cloud Security is the Responsibility of both Cloud Provider and Consumer

19.21 Cloud Computing Security Considerations

19.22 Placement of Security Controls in the Cloud

19.23 Best Practices for Securing Cloud

19.24 NIST Recommendations for Cloud Security

19.25 Organization/Provider Cloud Security Compliance Checklist

Cloud Security Tools

19.26 Cloud Security Tools

Cloud Penetration Testing

19.27 What is Cloud Pen Testing?

19.28 Key Considerations for Pen Testing in the Cloud

19.29 Cloud Penetration Testing

19.30 Recommendations for Cloud Testing

20. Cryptography

Cryptography Concepts

20.1 Cryptography

Types of Cryptography

20.2 Government Access to Keys (GAK)

Encryption Algorithms

20.3 Ciphers

20.4 Data Encryption Standard (DES)

20.5 Advanced Encryption Standard (AES)

20.6 RC4, RC5, and RC6 Algorithms

20.7 Twofish

20.8 The DSA and Related Signature Schemes

20.9 Rivest Shamir Adleman (RSA)

20.10 Diffie-Hellman

20.11 Message Digest (One-Way Hash) Functions

- Message Digest Function: MD5
- Secure Hashing Algorithm (SHA)
- RIPEMD – 160
- HMAC
- Cryptography Tools

20.12 MD5 Hash Calculators

20.13 Hash Calculators for Mobile

20.14 Cryptography Tools

- Advanced Encryption Package 2017
- BCTextEncoder
- Cryptography Tools

20.15 Cryptography Tools for Mobile

Public Key Infrastructure (PKI)

20.16 Public Key Infrastructure (PKI)

- Certification Authorities
- Signed Certificate (CA) Vs. Self Signed Certificate
- Email Encryption

20.17 Digital Signature

20.18 Secure Sockets Layer (SSL)

20.19 Transport Layer Security (TLS)

20.20 Cryptography Toolkit

- OpenSSL
- Keyczar

20.21 Pretty Good Privacy (PGP)

Disk Encryption

20.22 Disk Encryption

20.23 Disk Encryption Tools

- VeraCrypt
- Symantec Drive Encryption
- Disk Encryption Tools
- Cryptanalysis

20.24 Cryptanalysis Methods

- Linear Cryptanalysis
- Differential Cryptanalysis

- Integral Cryptanalysis

20.25 Code Breaking Methodologies
20.26 Cryptography Attacks

- Brute-Force Attack
- Birthday Attack
- Birthday Paradox: Probability
- Meet-in-the-Middle Attack on Digital Signature Schemes
- Side Channel Attack
- Hash Collision Attack
- DUHK Attack
- Rainbow Table Attack

20.27 Cryptanalysis Tools
20.28 Online MD5 Decryption Tools

- Countermeasures

20.29 How to Defend Against Cryptographic Attacks

Project Work

Ethical Hacker Projects Covered

Threat Detection

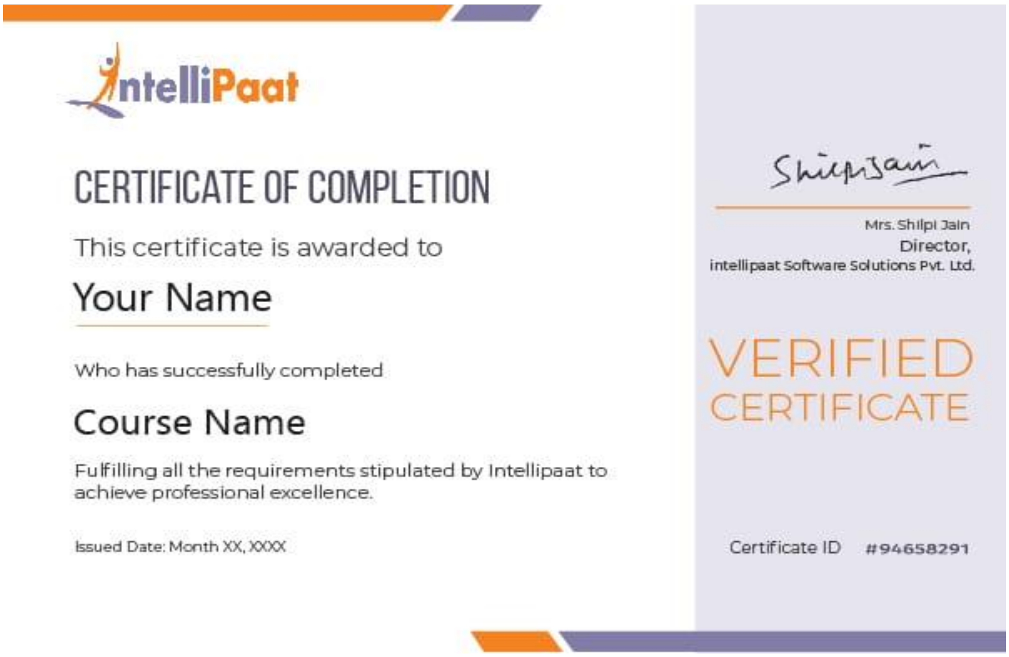
Being a part of your organization's Ethical Hacking team, you need to detect threats and data breaches through in-depth strategies to predict and protect your company from cybercrimes.

Cracking Wifi

You have to use various tools, technologies, and techniques to crack WPA/WPA2 wifi routers.

Certification

After the completion of the course, you will get a certificate from Intellipaat.



IntelliPaat

CERTIFICATE OF COMPLETION

This certificate is awarded to

Your Name

Who has successfully completed

Course Name

Fulfilling all the requirements stipulated by Intellipaat to achieve professional excellence.

Issued Date: Month XX, XXXX

ShilpiJain

Mrs. Shilpi Jain
Director,
intellipaat Software Solutions Pvt. Ltd.

VERIFIED CERTIFICATE

Certificate ID #94658291

Intellipaat Success Stories

Tushar Patil

Excellent course The manner in which Intellipaat conducted the course was really good. The trainer was extremely knowledgable. The biggest plus point of this course was the support. I was able to ask my concern and they were readily available for assistance. I highly recommend Intellipaat if you are planning to learn any trending technology.

Vishal Pentakota

The best part of this course is the series of hands-on demonstrations that the trainer performed. Not only did he explain each concept theoretically, but also implemented all those concepts practically. Great job. Must go for beginners.

Rinki Dutta

The Cyber Security online training course I completed with Intellipaat was great. The trainer was really helpful in explaining all topics in depth. I was able to understand the topics clearly. The trainer also used real-life examples in order to explain complicated modules and topics. The online sessions were also extremely helpful.

CONTACT US

INTELLIPAAT SOFTWARE SOLUTIONS PVT. LTD.

Bangalore

AMR Tech Park 3, Ground Floor, Tower B,
Hongasandra Village, Bommanahalli,
Hosur Road, Bangalore – 560068

USA

1219 E. Hillsdale Blvd. Suite 205,
Foster City, CA 94404

If you have any further queries or just want to have a conversation with us, then do call us.

IND: +91-7022374614 | US: 1-800-216-8930