Ethical Hacking & Cyber Security – Professional

Training Highlights:

- Total: 24 Hours of Live Training
- Supplementary Recorded Videos
- Live Q&A Sessions
- Highly Interactive
- Mapped content with the current job market

Once you register Yourself:

- You will receive an welcome email and document
- Our team will contact you and add you in a WhatsApp group prior to training

For and questions contact us : Email: support@cybrot.com
WhatsApp/Call : +91-7987638795

Training Syllabus

Introduction to Ethical Hacking

Module 1: Foundations of Information Security

- **Overview of Information Security**
  Understanding the essential principles of protecting digital information.
- **Core Components of Information Security**
  Exploring key elements: confidentiality, integrity, and availability.
- **Types of Information Security Threats**
  Identifying various attacks and their implications.
- **Motivations Behind Cyber Attacks**
  Analyzing the reasons individuals or groups engage in hacking.
- **Tactics, Techniques, and Procedures (TTPs)**
  Insight into common methods employed by attackers.

- **Understanding Vulnerabilities**
  Examining weaknesses in systems that can be exploited.
- **Classifying Cyber Attacks**
  Differentiating between various forms of attacks based on characteristics.
- **Information Warfare**
  Discussing the strategic use of information technology in conflict.

Module 2: Hacking Fundamentals

- **Defining Hacking**
  What it means to hack in today's digital landscape.
- **The Hacker Profile**
  Who are hackers? Understanding their motivations and ethics.
- **Introduction to Ethical Hacking**
  The principles and importance of hacking for defensive purposes.
- **The Necessity of Ethical Hacking**
  Why organizations must adopt ethical hacking practices.
- **Boundaries of Ethical Hacking**
  Understanding the scope and limitations of ethical hacking efforts.
- **Essential Skills for Ethical Hackers**
  Key competencies needed for success in ethical hacking roles.

Module 3: AI in Ethical Hacking

- **AI-Driven Ethical Hacking**
  Exploring how artificial intelligence enhances the capabilities of ethical hackers.
- **Myth Busting: AI vs. Ethical Hackers**
  Debunking the misconception that AI will replace human ethical hackers.
- **ChatGPT-Powered AI Tools**
  Utilizing advanced AI tools to support ethical hacking practices.

Module 4: Security Controls and Management

- **Understanding Information Security Controls**
  Strategies to protect sensitive information.
- **Information Assurance**
  Principles of maintaining the integrity and availability of information.
- **Adaptive Security Strategies**
  Developing a dynamic approach to evolving security threats.
- **Defense-in-Depth Strategies**
  Implementing layered security measures for robust protection.

Module 5: Risk Management in Cybersecurity

- **Defining Risk in Cybersecurity**
  Understanding risk and its significance in information security.
- **Fundamentals of Risk Management**
  Approaches to identifying and mitigating risks.
- **Cyber Threat Intelligence**
  Gathering and analyzing data to anticipate threats.
- **The Threat Intelligence Lifecycle**
  Stages involved in transforming threat data into actionable intelligence.
- **Threat Modeling Techniques**
  Identifying and evaluating potential threats to systems.

Module 6: Incident Management

- **Incident Management Framework**
  Overview of processes for managing security incidents.
- **Incident Handling and Response**
  Effective strategies for responding to security breaches.

Module 7: The Role of AI and ML in Cybersecurity

- **Integrating AI and Machine Learning**
  How AI and ML contribute to advanced security measures.

Module 8: Regulatory Compliance and Standards

- **Information Security Regulations**
  Overview of key laws and standards affecting cybersecurity:
- **PCI DSS**
- **ISO/IEC Standards**
- **HIPAA**
- **GDPR**
- **Data Protection Act 2018 and IT Act 2000**

Setting up Lab Environment

Module 9: Introduction to Linux and Its Role in Ethical Hacking

- Exploring the significance of Linux in the ethical hacking landscape.
- Overview of Linux distributions commonly used in penetration testing.

Module 10: Setting Up Your Virtual Hacking Lab

- **System Requirements**
  Hardware and software prerequisites for an effective virtual hacking environment.

Module 11: Virtualization Fundamentals

- **Introduction to Virtual Machines**
  Understanding virtualization with platforms like VMware and VirtualBox.
- **Comparing Live Operating Systems and Virtual Machines**
  Distinguishing between using a Live OS and deploying a VM for testing.

Module 12: Getting Started with Kali Linux

- **Overview of Kali Linux**
  Introduction to this powerful penetration testing distribution.
- **Configuring VMware for Kali Linux**
  Steps to optimize your VMware setup for running Kali Linux smoothly.

Module 13: Installing Kali Linux

- **Installation Methods**
  Guidance on installing Kali Linux in VMware using both Typical and Custom setups.

Module 14: Networking in Virtual Environments

- **Understanding Network Adapter Types**
  A comprehensive look at NAT, Bridge, Host-Only, and Internal network adapters and their use cases in a virtual lab.

Module 15: Setting Up Metasploitable

- **Installation of Metasploitable in VMware**
  Step-by-step process for setting up Metasploitable, a target for penetration testing exercises.

Footprinting and Reconnaissance

Module 16: Introduction to Footprinting and Reconnaissance

- Understanding the fundamentals of footprinting
- Importance of reconnaissance in ethical hacking

Module 17: Footprinting Fundamentals

- Key concepts and definitions
- Goals and objectives of footprinting
- Identifying potential threats through footprinting

Module 18: Types of Reconnaissance Techniques

- Differentiating between passive and active reconnaissance
- Methods used for effective information gathering

Module 19: Information Gathering Objectives

- What information can be obtained through footprinting
- Assessing the value of gathered data

Module 20: Footprinting Methodologies

- Systematic approaches to effective footprinting
- Tools and techniques for conducting thorough reconnaissance

Module 21: Utilizing Search Engines for Footprinting

- Techniques for extracting information from search engines
- Advanced search strategies and Google Dorks

Module 22: Google Hacking Techniques

- Exploring the capabilities of Google for security research
- Practical examples of advanced Google hacking techniques
- Understanding the Google Hacking Database (GHDB)

Module 23: Exploring SHODAN for Footprinting

- Overview of the SHODAN search engine
- Techniques for finding exposed devices and services

Module 24: Comprehensive Internet Footprinting

- Techniques for discovering a company’s domains and subdomains
- Using the Wayback Machine for historical data extraction
- People search methods and job site research

Module 25: Competitive Intelligence Gathering

- Researching company history and development
- Analyzing future plans and expert opinions

Module 26: Social Media Footprinting

- Information gathering through social networking platforms
- Leveraging LinkedIn for professional insights

Module 27: Whois and DNS Footprinting

- Understanding Whois lookup processes
- Extracting DNS information: techniques and tools
- Reverse DNS lookup methods

Module 28: Network and Email Reconnaissance

- Techniques for locating network ranges
- Using traceroute for path analysis
- Analyzing email headers for information extraction

Scanning

Module 29: Introduction to Scanning Techniques

- Understanding the role of scanning in ethical hacking
- Overview of different scanning methodologies

Module 30: Scanning Tools and Approaches

- Essential tools for network scanning
- Effective methodologies for comprehensive scanning

Module 31: Exploring Network Ports

- Introduction to network ports and their functions
- Differentiating between port states: open, closed, and filtered

Module 32: Port Categories

- Understanding well-known, registered, and dynamic ports

- Identifying common services associated with different ports

Module 33: Utilizing Ping for Network Discovery

- Basics of using ping for host discovery
- Interpreting ping results for network analysis

Module 34: IP Scanning with Angry IP Scanner

- Setting up and using Angry IP Scanner
- Analyzing scan results for network assessment

Module 35: Techniques for Banner Grabbing

- What is banner grabbing and its significance
- Tools and methods for effective banner grabbing

Module 36: Exploring WAF Detection with Wafw00f

- Introduction to Web Application Firewalls (WAF)
- Using Wafw00f to identify WAFs in use

Module 37: Nmap Fundamentals

- Introduction to Nmap and its capabilities
- Installing Nmap on Windows and Kali Linux

Module 38: Nmap Scanning Techniques

- Understanding various scan types and their uses
- Best practices for effective Nmap scanning

Module 39: Advanced Nmap Features

- Techniques for advanced port scanning with Nmap
- Strategies for bypassing firewalls using Nmap

Module 40: Nmap Scripting Engine (NSE)

- Introduction to NSE and its functionalities
- Using scripts to automate scanning tasks

Module 41: Identifying Open Ports and Services

- Techniques for discovering open ports and service versions
- Using Nmap to gather detailed service information

Module 42: Vulnerabilities, Exploits, and Payloads

- Understanding key concepts: vulnerabilities, exploits, and payloads
- How to identify exploitable services using searchsploit and Metasploit

Module 43: Introduction to Zenmap

- Utilizing Zenmap as a graphical front-end for Nmap
- Practical exercises using Zenmap on Windows

Module 44: Fundamentals of Enumeration

- Introduction to enumeration and its importance
- Overview of enumeration techniques

Module 45: NetBIOS Enumeration Techniques

- Techniques for enumerating NetBIOS information
- Tools: Using nbtstat and NetBIOS Enumerator on Windows

Module 46: NetBIOS Scanning in Kali Linux

- Practical exercises using nbtscan for NetBIOS enumeration
- Analyzing results for network insights

System Hacking

Module 47: Overview of System Hacking

- Understanding the fundamentals of system hacking
- Key concepts and techniques used in system compromises

Module 48: Introduction to Password Cracking Techniques

- Overview of password cracking and its importance
- Methods and strategies for cracking passwords

Module 49: Password Guessing and Complexity Requirements

- Exploring password guessing techniques
- Importance of password complexity and best practices

Module 50: Understanding Hashing Mechanisms

- Overview of hashing and its applications in security
- Comparison of common hashing algorithms

Module 51: Dictionary Attacks Explained

- Techniques for performing dictionary attacks
- Creating effective dictionaries for cracking

Module 52: Brute Force Attack Techniques

- Understanding brute force attacks and their effectiveness
- Tools and methods for executing brute force attacks

Module 53: Hybrid Attack Strategies

- Combining techniques for more effective password cracking
- Overview of hybrid attack methodologies

Module 54: Rainbow Table Attacks

- Introduction to rainbow tables and their use in cracking
- Techniques for utilizing rainbow tables effectively

Module 55: Extracting SAM Database Information

- Methods for accessing and extracting the SAM database
- Understanding the significance of the SAM database in security

Module 56: Generating Custom Password Lists with Crunch

- Using Crunch in Kali Linux to create tailored password lists
- Practical exercises on generating effective password lists

Module 57: Cracking Passwords for ZIP Files

- Techniques for cracking ZIP file passwords with John the Ripper
- Hands-on practice with file encryption

Module 58: Utilizing Hashcat for Password Cracking

- Introduction to Hashcat and its capabilities
- Practical examples of using Hashcat effectively

Module 59: Windows Password Cracking with L0phtcrack

- Overview of L0phtcrack and its functionalities
- Techniques for cracking Windows passwords

Module 60: Bypassing Windows Passwords with KonBoot

- Using KonBoot for password bypassing
- Practical demonstrations and techniques

Module 61: Understanding Keyloggers

- Overview of keyloggers and their functionalities
- Ethical considerations and legal implications of using keyloggers

Module 62: Types of Keyloggers

- Distinguishing between software and hardware keyloggers
- How each type is used in system hacking

Module 63: Capturing Passwords with Keyloggers

- Techniques for using keyloggers to capture credentials
- Real-world applications and ethical concerns

Module 64: Using Pwdump for Password Hash Extraction

- Techniques for utilizing pwdump effectively
- Practical examples of extracting password hashes

Social Engineering

Module 65: Understanding Social Engineering

- Overview of social engineering and its significance in cybersecurity
- The psychology behind human hacking

Module 66: The Dominance of Social Engineering Attacks

- Why social engineering is often more effective than technical attacks
- Case studies demonstrating its impact

Module 67: Categories of Social Engineering Attacks

- Exploring different types of social engineering attacks
- Recognizing the methods used by attackers

Module 68: Distinguishing Human and Technical Attacks

- Comparing human-based versus computer-based social engineering tactics
- Examples of each type and their effectiveness

Module 69: Exploring Identity Theft

- Understanding the process of identity theft
- Techniques used by cybercriminals to steal identities

Module 70: Email Spoofing and Fake Communications

- Techniques for creating spoofed emails
- Understanding the risks of fake communications

Module 71: Concealing Malicious Links in Emails

- Strategies for hiding harmful links within email content
- Identifying and mitigating risks associated with malicious links

Module 72: Introduction to Phishing Attacks

- What phishing is and how it operates
- The various forms of phishing attacks

Module 73: Common Phishing Techniques

- Analyzing popular phishing strategies used by attackers
- Practical examples of successful phishing campaigns

Network Sniffing Techniques

Module 74: Overview of Network Sniffing

- Understanding the fundamentals of network sniffing
- The role of sniffing in network security assessments

Module 75: Sniffing Tools in Kali Linux

- Introduction to various sniffing tools available in Kali Linux
- Setting up a sniffing environment for practical exercises

Module 76: Using dsniff for Network Analysis

- Overview of dsniff and its functionalities
- Practical applications for password and data sniffing

Module 77: Capturing Passwords in Network Traffic

- Techniques for sniffing passwords transmitted over networks
- Identifying vulnerable protocols for password capture

Module 78: Password Sniffing with Ettercap

- Using Ettercap to intercept and analyze HTTP traffic
- Practical exercises on capturing user credentials

Module 79: Sniffing HTTPS Traffic with Bettercap

- Understanding challenges of sniffing HTTPS
- Configuring Bettercap for effective password interception

Module 80: Exploiting ARP Spoofing

- Techniques for ARP spoofing to intercept network traffic
- Hands-on exercises demonstrating ARP attacks

Module 81: Implementing DNS Spoofing

- Overview of DNS spoofing and its implications
- Practical exercises for executing DNS spoofing attacks

Module 82: Analyzing Traffic with Wireshark

- Introduction to Wireshark for packet analysis
- Techniques for capturing and interpreting network traffic

Denial of Service (DoS) Attacks

Module 83: Introduction to DoS and DDoS Attacks

- Understanding Denial of Service (DoS) and Distributed Denial of Service (DDoS)
- The impact and implications of these attacks on organizations

Module 84: Types of Denial of Service Attacks

- Overview of various types of DoS attacks
- Identifying attack vectors and their characteristics

Module 85: Smurf and Fraggle Attacks

- Exploring the mechanics of Smurf and Fraggle attacks
- Techniques for launching and mitigating these attacks

Module 86: SYN Flood and Ping of Death Attacks

- Understanding SYN flood attacks and their execution
- Overview of the Ping of Death attack and its effects

Module 87: DDoS Attacks Utilizing Zombie PCs

- The concept of zombie PCs in DdoS attacks
- Techniques for controlling and using zombie networks

Module 88: Introduction to Botnets

- Understanding botnets and their role in DDoS attacks
- Strategies for detecting and mitigating botnet threats

Module 89: Conducting DoS Attacks on Live Systems

- Practical demonstration of DoS attacks on live websites
- Ethical considerations and legal implications

Module 90: Using GoldenEye for DoS Attacks

- Overview of the GoldenEye tool for executing DoS attacks
- Practical exercises with GoldenEye

Module 91: Slowloris Attack Techniques

- Understanding the Slowloris attack and its methodology
- Implementing Slowloris in a controlled environment

Module 92: Defending Against DoS and DDoS Attacks

- Countermeasures for mitigating DoS and DDoS attacks
- Developing a comprehensive defense strategy
-

Wireless Hacking Techniques

Module 93: Introduction to Wireless Hacking

- Overview of ethical hacking principles in the context of wireless security.

Module 94: Fundamentals of Wireless Networking

- Understanding the architecture and components that comprise wireless networks.

Module 95: Vulnerabilities of WEP (Wired Equivalent Privacy)

- In-depth exploration of WEP's mechanisms and associated security flaws.

Module 96: Advancements in WPA and WPA2 Protocols

- Analyzing the enhancements in wireless security offered by WPA and WPA2.

Module 97: Comparative Study of Wireless Security Protocols

- Examining the strengths and weaknesses of WEP, WPA, and WPA2.

Module 98: Wi-Fi Protected Setup (WPS) and Its Risks

- Understanding WPS and its implications for wireless security vulnerabilities.

Module 99: Wi-Fi Encryption Methods and Their Weaknesses

- Investigating various encryption techniques and their vulnerabilities.

Module 100: Choosing the Right External Wireless Adapter

- Criteria and considerations for selecting effective wireless adapters for testing.

Module 101: Monitor Mode and Packet Injection Techniques

- Techniques for capturing and manipulating wireless traffic effectively.

Module 102: Discovering Wireless Networks

- Methods for scanning and identifying nearby wireless networks.

Module 103: Exploiting WEP Encryption Vulnerabilities

- Step-by-step instructions for executing attacks on WEP-encrypted networks.

Module 104: Leveraging Aircrack and Airmon for Analysis

- Hands-on practices using Aircrack and Airmon to analyze wireless networks.

Module 105: Cracking WPA/WPA2 Security

- Techniques for manual and automated cracking of WPA/WPA2 protections.

Module 106: Wi-Fi Phishing Tactics

- Exploring social engineering methods applicable in wireless contexts.

Module 107: Advanced Topics in Wireless Security and Practical Exercises

- Further exploration of wireless security challenges and hands-on applications.

Network Security Devices

Module 108: Importance of Network Security Devices

- Exploring the critical role of security devices in network protection.

Module 109: Understanding Firewall Mechanisms

- Differentiating between hardware and software firewalls and best configuration practices.

Module 110: Intrusion Detection vs. Intrusion Prevention Systems

- Understanding the functionalities of IDS and IPS and effective deployment strategies.

Module 111: Virtual Private Networks (VPNs) Essentials

- Overview of VPN technologies, including IPSec and SSL, and guidelines for secure implementation.

Module 112: Unified Threat Management (UTM) Solutions

- Key features and benefits of UTM devices in integrated security frameworks.

Module 113: Security Information and Event Management (SIEM) Systems

- The significance of SIEM in security operations and incident analysis.

Module 114: Network Access Control (NAC) Strategies

- Principles of NAC and approaches for ensuring network compliance and security.

Module 115: Endpoint Security Approaches

- Insights into endpoint protection strategies and effective threat mitigation.

Module 116: Next-Generation Firewalls (NGFW) Overview

- Understanding the characteristics and deployment of NGFWs for enhanced security.

Module 118: Best Practices for Device Management and Security

- Emphasizing the importance of regular updates, configuration hardening, and incident response planning.

Cryptography in Ethical Hacking

Module 119: Fundamentals of Cryptography

- Definition and historical evolution of cryptography
- The significance of cryptography in enhancing network security
- Key principles and terminology associated with cryptographic practices

Module 120: Symmetric Key Cryptography

- Exploration of symmetric key algorithms and their functionalities
- Overview of prevalent symmetric encryption methods (e.g., AES, DES, RC4)
- Challenges related to key management and distribution

Module 121: Asymmetric Key Cryptography

- Introduction to Public Key Infrastructure (PKI)
- Core concepts of asymmetric algorithms (e.g., RSA, ECC)
- Applications of asymmetric cryptography, including encryption and digital signatures

Module 122: Understanding Cryptographic Hash Functions

- Definition and characteristics of hashing functions
- Commonly used hash algorithms (e.g., SHA-256, MD5, SHA-1)
- The role of hashing in ensuring data integrity and password security

Module 123: Digital Signatures and Certificates Explained

- Mechanisms behind digital signatures and their significance
- The function of digital certificates and the role of Certificate Authorities (CAs)
- Implementation of digital signatures for secure communications

Module 124: Cryptographic Protocols Overview

- Examination of widely-used cryptographic protocols (e.g., SSL/TLS, IPsec)
- Mechanisms of how these protocols secure data during transmission
- Analyzing vulnerabilities and potential attacks on cryptographic protocols

Module 125: Practical Applications of Cryptography in Ethical Hacking

- Utilizing cryptographic tools within penetration testing environments
- Hands-on exercises for encrypting and decrypting various types of data

Module WAPT or Bug Hunting

Module 126: Introduction to Bug Hunting

- Understanding the Bug Hunting Landscape
- The Importance of Bug Hunting in Cybersecurity
- Profiles of Successful Bug Hunters

Module 127: OAuth Vulnerabilities

- Exploring Common Misconfigurations in OAuth
- Case Studies on OAuth Exploits

Module 128: Issues with Cache Control

- Identifying and Exploiting Cache Misconfigurations
- Practical Demonstrations of Cache Vulnerabilities

Module 129: Cryptographic Weaknesses

- Analyzing Cryptographic Flaws in Applications
- Live Exploit Scenarios for Cryptographic Vulnerabilities

Module 130: Challenges with Password Confirmation

- Understanding the Risks of Missing Password Confirmation
- Hands-on Exploits Demonstrating This Vulnerability

Module 131: Getting Started with Burp Suite

- Overview of Burp Suite Features and Configuration
- Practical Exercises with Burp Suite Tools

Module 132: Rate Limiting Issues

- Understanding Rate Limiting and Its Vulnerabilities
- Real-world Exploits Demonstrating Rate Limit Bypasses

Module 135: Flaws in Session Management

- Analyzing Session Handling and Invalidation Issues
- Live Exploits on Session Management Flaws

Module 136: Misconfigurations in Mail Servers

- Key Concepts: DMARC, SPF, and DKIM
- Exploiting Mail Server Misconfigurations for Attack Vectors

Module 137: Cross-Site Scripting (XSS) Attacks

- Fundamentals of XSS and Its Variants
- Case Studies and Exploits Related to XSS

Module 138: URL Redirection Vulnerabilities

- Understanding URL Redirection Flaws
- Hands-on Exercises for Identifying Redirection Issues

Module 139: Website Defacement Attacks

- Techniques and Prevention for Website Defacement
- Real-World Examples of Defacement and Response Strategies

Module 140: Bug Hunter Methodology

- Effective Techniques for Target Identification
- Best Practices for Reporting Vulnerabilities
- Platforms for Bug Hunting: An Overview of Bugcrowd, HackerOne, and Dorks

Bonus : Cloud Security and Fundamentals

Module 141: Introduction to Cloud Security

- Definition and Importance of Cloud Security
- Overview of Cloud Computing Models (IaaS, PaaS, SaaS)
- Understanding the Shared Responsibility Model

Module 142: Cloud Security Risks

- Common Threats and Vulnerabilities in Cloud Environments
  - Data Breaches
  - Account Hijacking
  - Insecure APIs
- Case Studies of Cloud Security Incidents

Module 143: Security Principles in Cloud Computing

- Key Security Principles
  - Data Encryption (at rest and in transit)
  - Identity and Access Management (IAM)
  - Security Monitoring and Logging

Module 144: Best Practices for Cloud Security

- Implementing Strong Authentication (e.g., MFA)

- Regular Updates and Patch Management
- Conducting Security Audits and Assessments
- Data Loss Prevention (DLP) Strategies

Module 145: Compliance and Regulatory Frameworks

- Understanding Compliance Standards (GDPR, HIPAA, PCI-DSS)
- Strategies for Meeting Regulatory Requirements
- The Role of Audits in Compliance

Module 146: Emerging Trends in Cloud Security

- Threat Intelligence and Machine Learning in Cloud Security
- Future Challenges and Opportunities
- The Impact of Zero Trust Security Models

Module 147: Future Roadmap

- Roadmap and Guidance