Eduva Tech

# CEH V11 ETHICAL HACKING

## SYLLABUS

**Prepared For :**
Eduva Tech

**Contact Us:**

info@eduvatech.com
Call/Whatsapp: +91 9315519124

Eduva Tech

C|EH

Certified | Ethical Hacker

# Course Outline

## INTRODUCTION TO ETHICAL HACKING

- INFORMATION SECURITY OVERVIEW
- CYBER KILL CHAIN CONCEPTS
- HACKING CONCEPTS
- ETHICAL HACKING CONCEPTS
- INFORMATION SECURITY CONTROLS
- INFORMATION SECURITY LAWS AND STANDARDS

## FOOTPRINTING AND RECONNAISSANCE

- FOOTPRINTING CONCEPTS
- FOOTPRINTING METHODOLOGY
- FOOTPRINTING THROUGH SEARCH ENGINES
- FOOTPRINTING THROUGH WEB SERVICES
- FOOTPRINTING THROUGH SOCIAL NETWORKING SITES
- WEBSITE FOOTPRINTING
- EMAIL FOOTPRINTING
- WHOIS FOOTPRINTING
- DNS FOOTPRINTING
- NETWORK FOOTPRINTING
- FOOTPRINTING THROUGH SOCIAL ENGINEERING
- FOOTPRINTING TOOLS
- FOOTPRINTING COUNTERMEASURES

## SCANNING NETWORKS

- NETWORK SCANNING CONCEPTS
- SCANNING TOOLS
- HOST DISCOVERY
- PORT AND SERVICE DISCOVERY
- OS DISCOVERY (BANNER GRABBING/OS FINGERPRINTING)
- SCANNING BEYOND IDS AND FIREWALL
- DRAW NETWORK DIAGRAMS

## ENUMERATION

- ENUMERATION CONCEPTS
- NETBIOS ENUMERATION
- SNMP ENUMERATION
- LDAP ENUMERATION
- NTP AND NFS ENUMERATION
- SMTP AND DNS ENUMERATION
- OTHER ENUMERATION TECHNIQUES (IPSEC, VOIP, RPC, UNIX/LINUX, TELNET, FTP, TFTP, SMB, IPV6, AND BGP ENUMERATION)
- ENUMERATION COUNTERMEASURES

## VULNERABILITY ANALYSIS

- VULNERABILITY ASSESSMENT CONCEPTS
- VULNERABILITY CLASSIFICATION AND ASSESSMENT TYPES
- VULNERABILITY ASSESSMENT SOLUTIONS AND TOOLS
- VULNERABILITY ASSESSMENT REPORTS

## SYSTEM HACKING

- SYSTEM HACKING CONCEPTS
- GAINING ACCESS
- CRACKING PASSWORDS
- VULNERABILITY EXPLOITATION
- ESCALATING PRIVILEGES
- MAINTAINING ACCESS
- EXECUTING APPLICATIONS
- HIDING FILES
- CLEARING LOGS

## MALWARE THREATS

- MALWARE CONCEPTS
- APT CONCEPTS
- TROJAN CONCEPTS
- VIRUS AND WORM CONCEPTS
- FILE-LESS MALWARE CONCEPTS
- MALWARE ANALYSIS
- MALWARE COUNTERMEASURES
- ANTI-MALWARE SOFTWARE

## SNIFFING

- SNIFFING
- SNIFFING TECHNIQUE: MAC ATTACKS
- SNIFFING TECHNIQUE: DHCP ATTACKS
- SNIFFING TECHNIQUE: ARP POISONING
- SNIFFING TECHNIQUE: SPOOFING ATTACKS
- SNIFFING TECHNIQUE: DNS POISONING
- SNIFFING TOOLS
- SNIFFING COUNTERMEASURES
- SNIFFING DETECTION TECHNIQUES

## SOCIAL ENGINEERING

- SOCIAL ENGINEERING CONCEPTS
- SOCIAL ENGINEERING TECHNIQUES
- INSIDER THREATS
- IMPERSONATION ON SOCIAL
- NETWORKING SITES
- IDENTITY THEFT
- SOCIAL ENGINEERING COUNTERMEASURES

## DENIAL-OF-SERVICE

- DOS/DDOS CONCEPTS
- DOS/DDOS ATTACK TECHNIQUES
- BOTNETS
- DDOS
- CASE STUDY
- DOS/DDOS ATTACK TOOLS
- DOS/DDOS COUNTERMEASURES
- DOS/DDOS PROTECTION TOOLS

## SESSION HIJACKING

- SESSION HIJACKING CONCEPTS
- APPLICATION LEVEL SESSION HIJACKING
- NETWORK LEVEL SESSION HIJACKING
- SESSION HIJACKING TOOLS
- SESSION HIJACKING COUNTERMEASURES

## EVADING IDS, FIREWALLS, AND HONEYPOTS

- IDS, IPS, FIREWALL, AND HONEYPOT CONCEPTS
- IDS, IPS, FIREWALL, AND HONEYPOT SOLUTIONS
- EVADING IDS
- EVADING FIREWALLS
- IDS/FIREWALL EVADING TOOLS
- DETECTING HONEYPOTS
- IDS/FIREWALL EVASION COUNTERMEASURES

Eduva Tech

## HACKING WEB SERVERS

- WEB SERVER CONCEPTS
- WEB SERVER ATTACKS
- WEB SERVER ATTACK METHODOLOGY
- WEB SERVER ATTACK TOOLS
- WEB SERVER COUNTERMEASURES
- PATCH MANAGEMENT
- WEB SERVER SECURITY TOOLS

## HACKING WEB APPLICATIONS

- WEB APP CONCEPTS
- WEB APP THREATS
- WEB APP HACKING METHODOLOGY
- FOOTPRINT WEB INFRASTRUCTURE
- ANALYZE WEB APPLICATIONS
- BYPASS CLIENT-SIDE CONTROLS
- ATTACK AUTHENTICATION MECHANISM
- ATTACK AUTHORIZATION SCHEMES
- ATTACK ACCESS CONTROLS
- ATTACK SESSION MANAGEMENT MECHANISM
- PERFORM INJECTION ATTACKS
- ATTACK APPLICATION LOGIC FLAWS
- ATTACK SHARED ENVIRONMENTS
- ATTACK DATABASE CONNECTIVITY
- ATTACK WEB APP CLIENT
- ATTACK WEB SERVICES
- WEB API, WEBHOOKS, AND WEB SHELL
- WEB APP SECURITY

## SQL INJECTION

- SQL INJECTION CONCEPTS
- TYPES OF SQL INJECTION
- SQL INJECTION METHODOLOGY
- SQL INJECTION TOOLS
- EVASION TECHNIQUES- SQL INJECTION COUNTERMEASURES

## HACKING WIRELESS NETWORKS

- WIRELESS CONCEPTS
- WIRELESS ENCRYPTION
- WIRELESS THREATS
- WIRELESS HACKING METHODOLOGY
- WIRELESS HACKING TOOLS
- BLUETOOTH HACKING
- WIRELESS COUNTERMEASURES
- WIRELESS SECURITY TOOLS

## HACKING MOBILE PLATFORMS

- MOBILE PLATFORM ATTACK VECTORS
- HACKING ANDROID OS
- HACKING IOS
- MOBILE DEVICE MANAGEMENT
- MOBILE SECURITY GUIDELINES AND TOOLS

Eduva Tech

## IOT AND OT HACKING

- IOT CONCEPTS
- IOT ATTACKS
- IOT HACKING METHODOLOGY
- IOT HACKING TOOLS
- IOT COUNTERMEASURES
- OT CONCEPTS
- OT ATTACKS
- OT HACKING METHODOLOGY
- OT HACKING TOOLS
- OT COUNTERMEASURES

## CLOUD COMPUTING

- CLOUD COMPUTING CONCEPTS
- CONTAINER TECHNOLOGY
- SERVERLESS COMPUTING
- CLOUD COMPUTING THREATS
- CLOUD HACKING
- CLOUD SECURITY

## CRYPTOGRAPHY

- CRYPTOGRAPHY CONCEPTS
- ENCRYPTION ALGORITHMS
- CRYPTOGRAPHY TOOLS
- PUBLIC KEY INFRASTRUCTURE (PKI)
- EMAIL ENCRYPTION
- DISK ENCRYPTION
- CRYPTANALYSIS
- COUNTERMEASURES