SPYRIOT SECURITY CYBER HUB

CERTIFIED ETHICAL HACKER (CEH V13) TRAINING PROGRAM

Course Overview

The Certified Ethical Hacker (CEH v13) program provides in-depth knowledge and practical skills required to identify vulnerabilities, secure systems, and perform ethical hacking using real-world tools and techniques

Course Modules

- Introduction to Ethical Hacking
- Footprinting and Reconnaissance
- Scanning Networks
- Enumeration
- Vulnerability Analysis
- System Hacking
- Malware Threats
- Sniffing
- Social Engineering
- Denial-of-Service
- Session Hijacking
- Evading IDS, Firewalls, Honeypots
- Hacking Web Servers
- Hacking Web Applications
- SQL Injection
- Hacking Wireless Networks
- Hacking Mobile Platforms
- IoT and OT Hacking
- Cloud Computing Security
- Cryptography

20 comprehensive modules covering all EC-Council CEH V13 exam domains with hands-on lab exercises

PHASE 01 — Foundation & Reconnaissance

Module 01 – 04

MODULE 01 — Introduction to Ethical Hacking

Fundamentals of Cybersecurity & Ethical Hacking Concepts

- Elements of Information Security: CIA Triad — Confidentiality, Integrity, and Availability
- Cyber Kill Chain methodology and hacking phases (Reconnaissance → Exploitation → Post-Exploitation)
- Types of hackers: White Hat, Black Hat, Grey Hat, Script Kiddies, Nation-State Actors
- Legal framework: Cyber Laws, Responsible Disclosure, Rules of Engagement for pen testers
- Information Security Controls: Policies, Procedures, Guidelines, Standards
- Threat Intelligence and Threat Modeling concepts (MITRE ATT&CK Framework)
- Overview of penetration testing methodologies: PTES, OWASP, NIST

MODULE 02 — Footprinting and Reconnaissance

OSINT, Passive & Active Intelligence Gathering

- Footprinting concepts and objectives — gathering target info without detection
- OSINT (Open Source Intelligence) techniques: Google Dorking, Shodan, Maltego, theHarvester
- Whois lookups, DNS enumeration, and IP geolocation techniques
- Website footprinting using Netcraft, Archive.org, and metadata extraction
- Social media OSINT: LinkedIn, Facebook, Twitter/X reconnaissance for target profiling
- Email footprinting: tracing email headers, detecting open relays
- Competitive intelligence gathering and VPN/Proxy detection techniques
- Footprinting countermeasures and detection evasion strategies

MODULE 03 — Scanning Networks

Port Scanning, Host Discovery & Network Mapping

- TCP/IP communication fundamentals: 3-way handshake, TCP flags, ICMP, UDP protocols
- Network scanning techniques: TCP Connect, SYN Stealth, FIN, XMAS, NULL, ACK scans
- Nmap — comprehensive usage: host discovery, port scanning, service versioning (-sV), OS detection (-O)
- Nmap Scripting Engine (NSE) for vulnerability detection and automation
- Banner grabbing techniques using Telnet, Netcat, Nmap
- OS fingerprinting — active vs passive techniques using p0f, Ettercap
- Vulnerability scanning using Nessus, OpenVAS, and Qualys
- IDS/Firewall evasion during scanning: fragmentation, decoys, spoofing source IPs
-

MODULE 04 — Enumeration

Service Enumeration, User Harvesting & Network Resource Discovery

- NetBIOS Enumeration: nbtstat, SuperScan, NetBIOS Enumerator tools
- SNMP Enumeration: community strings, MIB tree walking with SNMPwalk, SolarWinds
- LDAP Enumeration: extracting AD users, groups, and policies
- NTP Enumeration: ntptrace, ntpdc, ntpq for network topology discovery
- SMTP Enumeration: VRFY, EXPN, RCPT TO techniques for email user harvesting
- DNS Zone Transfer attacks and DNS cache poisoning fundamentals
- SMB Enumeration using Enum4Linux, CrackMapExec, and Metasploit modules
- FTP, SSH, Telnet enumeration and countermeasures

PHASE 02 — Vulnerability Analysis & System Hacking

Module 05 – 07

MODULE 05 — Vulnerability Analysis

CVE, CVSS, Vulnerability Classification & Assessment Tools

- Vulnerability assessment concepts: CVE, CWE, CVSS scoring system (Base, Temporal, Environmental)
- Types of vulnerabilities: Zero-day, Misconfiguration, Known CVEs, Logic flaws
- Automated vulnerability scanners: Nessus, OpenVAS, Nexpose, Qualys Guard
- Manual vulnerability discovery using exploit-db.com, vulhub, NVD database
- Risk scoring and vulnerability prioritization using CVSS 3.1
- Patch management and vulnerability lifecycle management
- Vulnerability assessment report writing for clients and management

MODULE 06 — System Hacking

Password Attacks, Privilege Escalation, Persistence & Covering Tracks

- Password cracking techniques: Dictionary, Brute-Force, Rainbow Tables, Pass-the-Hash
- Tools: John the Ripper, Hashcat, Hydra, Medusa for password attacks
- Privilege escalation on Windows: UAC bypass, token impersonation, kernel exploits
- Privilege escalation on Linux: SUID/SGID, cron jobs, PATH injection, sudo misconfig
- Maintaining access: Rootkits, Backdoors, Netcat listeners, Scheduled tasks
- Steganography: Hiding data in images, audio, and files using OpenStego, SteghideGUI
- Covering tracks: Clearing event logs, modifying timestamps, NTFS alternate data streams
- Windows Registry manipulation for persistence and stealth

MODULE 07 — Malware Threats

Trojans, Ransomware, Viruses, Worms & Malware Analysis

- Types of malware: Virus, Worm, Trojan, Ransomware, Spyware, Adware, Rootkit, Botnet
- Creating and deploying RATs (Remote Access Trojans) for ethical lab testing
- APT (Advanced Persistent Threat) attack lifecycle and TTP analysis
- Static Malware Analysis: PE header analysis, strings extraction, YARA rules
- Dynamic Malware Analysis: Behavioral analysis in sandboxes (Cuckoo, AnyRun, VirusTotal)
- Anti-malware evasion: Polymorphic code, packing, obfuscation techniques
- Malware reverse engineering basics using IDA Free, Ghidra, x64dbg
- Malware countermeasures: EDR tools, application whitelisting, behavior monitoring

PHASE 03 — Network & Application Attacks

Module 08 – 12

MODULE 08 — Sniffing

Packet Capture, MITM Attacks & Network Traffic Analysis

- Network sniffing concepts: passive vs active sniffing, promiscuous mode
- MAC Flooding attacks: disrupting switch CAM tables using macof, Yersinia
- ARP Poisoning / ARP Spoofing for Man-in-the-Middle (MITM) attacks using Arpspoof, Ettercap
- DNS Poisoning: Redirecting traffic using fake DNS responses
- SSL Stripping attacks: downgrading HTTPS to HTTP using SSLstrip, Bettercap
- Wireshark: Deep packet analysis, filtering, and credential extraction
- Sniffing countermeasures: Dynamic ARP Inspection, DHCP Snooping, port security

MODULE 09 — Social Engineering

Human Hacking, Phishing, Vishing & Manipulation Techniques

- Social engineering attack types: Phishing, Spear Phishing, Whaling, Smishing, Vishing
- Pretexting, Baiting, Quid Pro Quo, Tailgating/Piggybacking attacks
- Building phishing campaigns using Gophish and Social Engineering Toolkit (SET)
- Creating convincing credential harvesting pages and fake login portals
- Insider threat identification and behavioral analysis
- Security awareness training design to defend against social engineering
- AI-powered social engineering: Deepfake voice/video attacks (CEH V13 new topic)

MODULE 10 — Denial-of-Service (DoS/DDoS)

Volumetric Attacks, Amplification, Botnets & Mitigation

- DoS vs DDoS attack concepts: volumetric, protocol, and application layer attacks
- SYN Flood, UDP Flood, ICMP Flood, Smurf, Fraggle attacks explained
- Amplification attacks: DNS amplification, NTP amplification, SSDP reflection
- Botnet architecture: C&C servers, bot herders, zombie networks (Mirai, Zeus)
- Application-layer DDoS: HTTP Flood, Slowloris, RUDY, XML bomb attacks
- DoS attack tools: LOIC, HOIC, Metasploit DoS modules (lab environment only)
- DDoS mitigation: CDN scrubbing, rate limiting, Anycast diffusion, BCP38

MODULE 11 — Session Hijacking
Cookie Theft, Token Interception & Account Takeover

- Session hijacking fundamentals: session tokens, cookies, and authentication flows
- Application-level hijacking: XSS-based cookie theft, CSRF attacks
- Network-level hijacking: TCP sequence prediction, RST injection
- Session fixation and session prediction attacks
- Man-in-the-Browser (MitB) attacks using browser extensions and trojans
- JWT token attacks: algorithm confusion, none-algorithm bypass, weak secrets
- Countermeasures: Secure/HttpOnly cookie flags, SameSite attribute, re-authentication
-

MODULE 12 — Evading IDS, Firewalls & Honeypots
Detection Evasion, Obfuscation & Anti-Forensics

- IDS (Intrusion Detection System) types: NIDS, HIDS, Signature-based vs Anomaly-based
- IDS evasion: Packet fragmentation, TTL manipulation, Unicode encoding, obfuscated shellcode
- Firewall types: Packet filtering, Stateful inspection, Next-Gen Firewalls (NGFW)
- Firewall evasion: HTTP tunneling, ICMP tunneling, DNS over HTTPS (DoH), SSH port forwarding
- Honeypot detection techniques: latency analysis, error fingerprinting, limited interaction responses
- WAF (Web Application Firewall) bypass techniques for web pen testing
- Proxy chains, Tor network usage, and traffic obfuscation with Obfs4

PHASE 04 — Web & Application Security
Module 13 – 15
MODULE 13 — Hacking Web Servers
Apache, IIS, Nginx Exploitation & Server Hardening

- Web server architecture: Apache, IIS, Nginx — configuration, modules, default files
- Web server attack methodology: information gathering → vulnerability mapping → exploitation
- Directory traversal and path traversal attacks to access server files
- HTTP Response Splitting, Cache Poisoning, and HTTP Request Smuggling
- Web cache deception attacks and server-side request forgery (SSRF)
- Default credentials exploitation, misconfigured admin panels discovery
- Web server hardening: disabling directory listing, security headers (HSTS, CSP, X-Frame)
- Patch management, SSL/TLS configuration best practices (TLS 1.3, HPKP)

MODULE 14 — Hacking Web Applications
OWASP Top 10, BurpSuite, XSS, IDOR & Web Exploitation

- OWASP Top 10 (2021): Broken Access Control, Cryptographic Failures, Injection, etc.
- Burp Suite Pro: Intercepting proxy, Scanner, Intruder, Repeater, Decoder usage
- Cross-Site Scripting (XSS): Reflected, Stored, DOM-based — exploitation & impact
- Cross-Site Request Forgery (CSRF) exploitation and token bypass techniques
- Insecure Direct Object Reference (IDOR) and Broken Access Control exploitation
- File upload vulnerabilities: bypassing extension filters, uploading web shells
- XML External Entity (XXE) injection and Server-Side Template Injection (SSTI)

- Authentication bypass: Password reset flaws, 2FA bypass, OAuth misconfigurations
-

MODULE 15 — SQL Injection

SQLi Attack Types, Exploitation, Automation & WAF Bypass

- SQL Injection concepts: In-band (UNION, Error-based), Inferential (Boolean, Time-based Blind), Out-of-band
- Manual SQLi exploitation: identifying injection points, extracting database names, tables, and data
- UNION-based SQLi: column count detection, data extraction across multiple columns
- Blind Boolean SQLi: True/False condition-based data extraction (manual & automated)
- Time-based Blind SQLi using SLEEP(), WAITFOR DELAY — slow data extraction
- SQLMap: Automated injection, database dumping, OS-shell access, file read/write
- Second-order SQLi and Stored Procedure exploitation
- Countermeasures: Parameterized queries, stored procedures, input validation, WAF rules

PHASE 05 — Wireless, Mobile & IoT Hacking

Module 16 – 18

- MODULE 16 — Hacking Wireless Networks
- WEP/WPA/WPA2/WPA3 Cracking, Rogue APs & Evil Twin
- Wireless standards: IEEE 802.11 a/b/g/n/ac/ax (Wi-Fi 6) and security protocols (WEP/WPA/WPA3)
- WEP cracking: IV attack using Aircrack-ng suite (airmon-ng, airodump-ng, aircrack-ng)
- WPA/WPA2 cracking: 4-way handshake capture and dictionary attack with Hashcat/Aircrack
- WPA3 SAE (Dragonblood) vulnerabilities and downgrade attacks
- Rogue Access Point attacks and Evil Twin Wi-Fi honeypot setup
- PMKID Attack: Offline WPA2 cracking without deauth using Hcxtools
- Bluetooth hacking: BlueSmack, BlueSnarfing, BlueJacking, and Blueborne vulnerabilities
- Wireless IDS and enterprise Wi-Fi security with WPA2-Enterprise (RADIUS/802.1X)

MODULE 17 — Hacking Mobile Platforms
Android & iOS Security, OWASP Mobile Top 10 & App Analysis

- Mobile attack surface: Device, Network, Application, Cloud, and Data Storage
- Android security model: Permissions, APK structure, ADB, Activity Manager exploitation
- Android app analysis: APKTool, JADX, MobSF for static & dynamic analysis
- iOS security architecture: Secure Enclave, App Sandbox, JailBreak detection bypass
- OWASP Mobile Top 10: Improper Platform Usage, Insecure Data Storage, Insecure Communication
- Mobile Malware: Spyware, Stalkerware, Banking Trojans on Android (TrickMo, Cerberus)
- SMS phishing (Smishing), SIM swapping attacks and OTP interception techniques
- Mobile Device Management (MDM) security and BYOD policy enforcement

- MODULE 18 — IoT and OT Hacking
- Smart Devices, SCADA/ICS Vulnerabilities & Industrial Security
- IoT architecture layers: Perception, Network, Middleware, Application, and Business
- IoT attack surface: Firmware extraction, UART/JTAG interfaces, default credentials, cloud APIs
- Shodan & Censys for IoT device discovery and vulnerability assessment
- Firmware analysis: Binwalk, Firmwalker for extracting and analyzing IoT firmware
- OT (Operational Technology) security: SCADA, ICS, PLC, and DCS attack concepts
- Modbus, DNP3, BACnet protocol vulnerabilities and industrial exploitation techniques
- Real-world ICS attack case studies: Stuxnet, Ukraine Power Grid, Colonial Pipeline
- IoT security frameworks: OWASP IoT Top 10, IEC 62443 standards
- PHASE 06 — Cloud, Cryptography & AI (CEH V13 New)
- Module 19 – 20
- MODULE 19 — Cloud Computing Security
- AWS/Azure/GCP Attack Surfaces, Container Security & Cloud Pentesting
- Cloud service models: IaaS, PaaS, SaaS — shared responsibility model and security implications
- AWS attack techniques: S3 bucket misconfiguration, IAM privilege escalation, EC2 metadata attacks
- Azure Active Directory attacks: Password spray, Token theft, Conditional Access bypass
- Google Cloud Platform (GCP) security misconfigurations and exploitation
- Container security: Docker escape, Kubernetes RBAC misconfig, etcd access exploitation

- Serverless security: Lambda function injection, function privilege escalation, event data poisoning
- Cloud security tools: Pacu (AWS), ROADtools (Azure), Checkov, ScoutSuite, CloudSploit
- Cloud security best practices: CIS Benchmarks, CSA Cloud Controls Matrix, Zero Trust
- MODULE 20 — Cryptography
- Encryption, PKI, Hashing, Cryptanalysis & AI-Powered Attacks
- Cryptography fundamentals: Symmetric (AES, DES, 3DES) vs Asymmetric (RSA, ECC, Diffie-Hellman)
- Hashing algorithms: MD5, SHA-1, SHA-256, SHA-3 and their collision vulnerabilities
- PKI (Public Key Infrastructure): Digital Certificates, CA, CRL, OCSP, TLS handshake
- Cryptanalysis attacks: Brute force, Birthday attack, Man-in-the-Middle, Meet-in-the-Middle
- Disk encryption tools: BitLocker, VeraCrypt, LUKS — forensic acquisition challenges
- Ransomware encryption analysis: understanding key generation and encrypted file structures
- Post-Quantum Cryptography: NIST PQC standards (Kyber, Dilithium) and quantum threats
- AI-powered cryptanalysis: using ML models for hash cracking and cipher pattern recognition