SUPPORT ME
— BY THE DEVELOPERS' GROUP

Where trainees meet real Support

Cyber Security

Learn Offensive & Defensive Security • Hands-On Labs • Industry Readiness

8 Weeks Duration • 40 Total Lectures (5 Lectures/Week) • Beginner to Advanced

About the Course

- **Structured Learning Journey:** Core security fundamentals to offensive & defensive operations
- **Career-Oriented:** Designed for beginners & IT professionals seeking industry-ready security skills
- **Comprehensive Scope:** Covers Linux, Networking, Vulnerability Assessment, Web Pentesting (OWASP), and SOC
- **Hands-On Methodology:** Develop skills through guided lab practice, virtualized war rooms & real tools
- **Portfolio Capstone:** Complete a guided enterprise penetration testing capstone project

Who Can Attend?

- Students and recent graduates seeking to enter the cybersecurity industry
- Software and IT professionals wanting to specialize in security engineering
- Developers, testers, analysts, and support professionals looking to upskill
- Professionals planning to transition towards offensive pentesting or SOC roles

**No previous cybersecurity experience required. Starting points are tailored to learner background.*

Learning Themes

1. Foundations of Cyber Security, Linux & Networking (Lectures 01 – 05)

- Cyber security landscape, threat vectors, CIA triad, security policies & ethical boundaries
- Building an isolated pentesting lab: VirtualBox/VMware setup, Kali Linux installation & configuration
- Linux command line mastery: file hierarchy, user permissions (chmod, chown), processes & Bash scripting
- TCP/IP networking deep dive: OSI 7-layer model, 3-way handshake, DNS, DHCP & CIDR subnetting
- Network traffic sniffing & packet inspection using Wireshark: protocol filters & stream analysis

2. Reconnaissance, OSINT & Attack Surface Discovery (Lectures 06 – 10)

- Passive reconnaissance & Open Source Intelligence (OSINT): Whois lookups, DNS recon & Shodan queries
- Advanced Google Dorking operators, email harvesting with theHarvester & metadata extraction via ExifTool
- Active port scanning mechanics: Nmap scan types (TCP Connect, SYN stealth, UDP) & timing flags (-T0 to -T5)
- Nmap Scripting Engine (NSE): vulnerability scripts, service fingerprinting & OS detection
- Target surface enumeration using Netcat, Masscan & DNS zone transfer exploitation

3. Vulnerability Assessment & Exploitation Fundamentals (Lectures 11 – 15)

- Vulnerability assessment methodologies: CVE database, NVD analysis & CVSS v3.1 scoring
- Automated vulnerability scanning with Nessus Essentials: credentialed scans & report interpretation
- Metasploit Framework architecture: modules, exploits, staged vs. unstaged payloads & multi-handlers
- Network service exploitation: SMB (EternalBlue MS17-010), RDP BlueKeep, anonymous FTP & Telnet
- Payload generation with MSFVenom: encoding, evasion techniques, multi-handlers & persistence

Learning Themes (Continued)

4. Web Application Penetration Testing: Injection Attacks (Lectures 16 – 20)

- Web architecture & HTTP/S deep dive: status codes, cookies, session headers, JWT tokens & CORS policies
- Burp Suite Professional hands-on: Intercept Proxy, Repeater manual testing, Intruder & Scope configuration
- SQL Injection (SQLi) foundations: UNION-based, Error-based exploitation & database extraction
- Advanced SQLi & automated database exploitation using SQLMap: dumping tables & shell access
- Cross-Site Scripting (XSS): Stored, Reflected, DOM-based attacks & session cookie hijacking

5. Advanced Web Vulnerabilities & API Security (Lectures 21 – 25)

- Broken Access Control & Insecure Direct Object References (IDOR): vertical & horizontal privilege escalation
- Cross-Site Request Forgery (CSRF) & Server-Side Request Forgery (SSRF) into cloud metadata endpoints
- Local & Remote File Inclusion (LFI/RFI), unrestricted file uploads & Remote Code Execution (RCE)
- Broken authentication, brute-force mitigation bypasses & JWT signature stripping attacks
- REST & GraphQL API security testing with Postman, Nikto & automated OWASP ZAP scanning

6. Applied Cryptography, Password Attacks & Privilege Escalation (Lectures 26 – 30)

- Applied cryptography: Symmetric (AES) vs. Asymmetric (RSA), hash functions (MD5, SHA256, Bcrypt) & salts
- Password cracking mechanics with John the Ripper: dictionary, brute-force & hybrid rules
- High-speed GPU hash cracking with Hashcat: NTLM/Kerberos hashes, custom wordlists via CeWL
- Linux privilege escalation: LinPEAS enumeration, SUID abuse, sudo misconfigurations & kernel exploits
- Windows privilege escalation: WinPEAS analysis, unquoted service paths, token impersonation & UAC bypass

7. Defensive Operations: SOC, SIEM & Incident Response (Lectures 31 – 35)

- Security Operations Center (SOC) architecture: Tier 1-3 analyst workflows & MITRE ATT&CK framework
- Security telemetry & event logging: Windows Event IDs (4624, 4625, 4688), Sysmon & Linux auth.log
- SIEM log analysis using Splunk: writing search queries (SPL), building alert dashboards & anomaly detection
- Incident response lifecycle (NIST SP 800-61): triage, containment protocols, eradication & lessons learned
- Malware triage & network forensics: Any.run dynamic sandboxing, extracting network IOCs & YARA rules

8. Capstone Pentest Project, CTF & Career Acceleration (Lectures 36 – 40)

- Full-scope enterprise network penetration testing lab: simulated DMZ, database & internal targets
- Capture The Flag (CTF) tournament: multi-flag offensive challenge testing web, crypto & privilege escalation
- Professional penetration test report authoring: executive risk summaries, technical remediation & CVSS scoring
- Cybersecurity certification strategy: CompTIA Security+, CEH v12, eJPT & Blue Team Level 1 (BTL1)
- Technical interview coaching: mock war-room scenarios, portfolio defense, resume optimization & career launch

Certification Alignment & Target Roles

- **Industry Certifications Aligned:** CompTIA Security+ (SY0-701), Certified Ethical Hacker (CEH v12), eJPT, Blue Team Level 1
- **Target Roles:** Junior Penetration Tester, SOC Analyst (Tier 1 & 2), Cybersecurity Associate, Vulnerability Analyst
- **Training Support:** Live Interactive Sessions, 1-on-1 Mentorship, Recorded Video Access & Job Support