PROFESSIONAL CYBERSECURITY CERTIFICATION OUTLINE

Penetration Testing Certification

Advanced Offensive Security & Practical Adversary Simulation • Modern Penetration Testing

The ultimate hands-on modern penetration testing curriculum engineered for enterprise security assessments, adversary simulations, network pivoting, manual and automated exploitation, server-side flaws, Web LLM vulnerabilities, and Active Directory attack paths.

WHY ALL SAFE • Industry Achievements & Institutional Credibility

VERIFIED TRACK RECORD

PILLAR 01 • MARKET LEADERSHIP

1. Pakistan's Leading Cyber Security Platform

Pioneering offensive and defensive cybersecurity training, trusted by leading universities, corporate enterprises, and defense professionals nationwide for elite technical capacity building.

PILLAR 02 • GLOBAL IMPACT

2. Trained 2,000+ Students Internationally

Empowered a diverse global alumni network spanning 15+ countries, equipping learners with practical command-line muscle memory, live cyber range experience, and enterprise deployment skills.

PILLAR 03 • CAREER OUTCOMES

3. Global Success Stories

Alumni actively employed across multinational technology firms, telecom providers, Fortune 500 infrastructure teams, and Security Operations Centers (SOC) across the globe.

PILLAR 04 • NEXT-GEN INNOVATION

4. Partner of First Security AI Platform

Official partner integrating **Securiti AI Pro**—the pioneering AI-powered platform for automated threat intelligence, vulnerability correlation, and AI-driven cyber defense simulation.

16	100%	24/7	FREE
MODERN BLUEPRINT MODULES	LIVE HANDS-ON LAB RANGES	RED TEAM MENTORSHIP	SECURITI AI PRO™ ACCESS

Enrollment: +92 321 2077222 • allsafeus@gmail.com
www.allsafeinnovate.com

MODERN OFFENSIVE SECURITY ENGINEERING

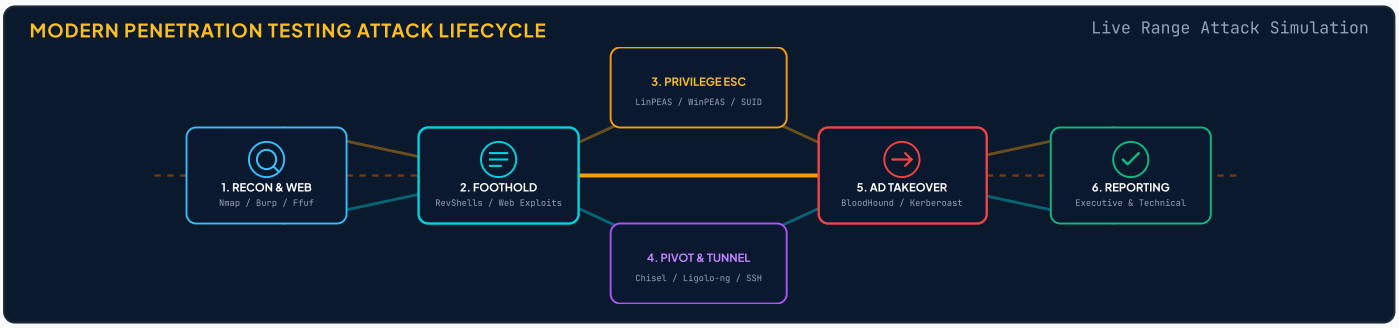
Modern Penetration Testing Methodology & The ALL SAFE Advantage

Mastering the world's most rigorous practical penetration testing standards through real-world target exploitation, network pivoting, and Active Directory compromise.

Modern Practical Penetration Testing Benchmark

Elite Practical Standard

Unlike multiple-choice theoretical tests, **Modern Penetration Testing** demands 100% hands-on practical execution and deep adversary simulation skills. Candidates are dropped into live, fully-defended multi-tier enterprise networks and must enumerate services, exploit web applications, execute manual and automated exploitation, pivot across segmented subnets, and compromise Active Directory enterprise environments. ALL SAFE equips you with the exact technical tradecraft, persistence, and muscle memory demanded in modern industry assessments.



The 6 ALL SAFE Institutional Advantages

WHY CHOOSE ALL SAFE?

1. Live Practical Sessions

Hands-on offensive labs mimicking modern corporate networks. Master real exploitation, double pivots, and Active Directory privilege escalation.

2. 24/7 Mentorship Support

Around-the-clock technical mentorship from experienced penetration testers to troubleshoot exploits, overcome rabbit holes, and accelerate learning.

3. Free International Certs

Free international certification opportunities through eligible ALL SAFE programs. **Eligibility and applicable program criteria must be confirmed.*

4. International Experts Community

Connect with a global community of penetration testers, red team operators, and security researchers for technical collaboration and career advancement.

5. Securiti AI Pro — Free

Complimentary access to Securiti AI Pro, ALL SAFE's proprietary AI-assisted security platform. Accelerate attack analysis and vulnerability assessment.

6. Career-Oriented Learning

Build career-ready skills for high-paying roles: Penetration Tester, Vulnerability Assessor, Red Team Operator, and Application Security Engineer.

MODERN PENETRATION TESTING BLUEPRINT

Modern Penetration Testing Modules

Modern enterprise-aligned curriculum mastering practical exploitation, server-side flaws, privilege escalation, Web LLM vulnerabilities, and Active Directory.

01. Pentest Methodologies & Tools
Foundation

Kali Linux CLI mastery, Bash & Python 3 scripting for pentesters, Netcat, Socat, Wireshark, Tmux, and essential terminal utilities.

02. Information Gathering & Recon
OSINT Recon

Passive & active OSINT, DNS zone transfers, port scanning mechanics (TCP SYN/Connect/UDP), Nmap NSE scripting, and service fingerprinting.

03. Vulnerability Assessment
Scanning

Vulnerability scanning with Nikto, Nessus, and OpenVAS; banner grabbing, manual flaw identification, and finding default credentials.

04. Web App Attacks (OWASP Top 10)
Web Exploits

SQLi (Union, Blind, Time), XSS, Command Injection, Directory Traversal, LFI/RFI with log poisoning, File Upload bypasses, SSRF, IDOR, Burp Pro.

05. Modifying Public Exploits
Exploit Custom

Searchsploit, Exploit-DB, GitHub POC repositories; compiling C/C++ exploits for Linux/Windows; modifying offsets, shellcode, and IP sockets.

06. Buffer Overflows (x86/x64)
Binary Exploitation

Memory architecture, CPU registers (EIP/ESP/EBP), stack framing, controlling execution flow, finding bad characters, and shellcode synthesis.

07. Client-Side Attacks & Phishing
Client Exploits

Weaponizing Office documents, malicious VBA macros, HTML smuggling, client-side payload staging, and payload execution bypasses.

08. Server-Side Vulnerabilities
Server Exploits

Server-Side Request Forgery (SSRF), Server-Side Template Injection (SSTI), XML External Entity (XXE), OS command injection, and insecure deserialization.

09. Password Attacks & Cracking
Hash Cracking

Wordlist generation (CeWL, Crunch), online brute-force (Hydra), offline hash cracking with Hashcat & John, Pass-the-Hash (PtH), and NTLM.

10. Pivoting, Tunneling & Proxies
Network Pivoting

SSH local/remote port forwarding, dynamic SOCKS (Proxychains), Chisel, Ligolo-ng, Plink, double pivoting across multi-subnet networks.

11. Linux Privilege Escalation
Linux Root

SUID/SGID abuse, misconfigured SUDO rights, cron job hijacking, Linux capabilities, writable /etc/passwd, shared object injection, PwnKit.

12. Manual & Automated Exploitation
Exploit Execution

Manual proof-of-concept verification, custom Python exploit weaponization, automated vulnerability scanning integration, payload staging, and execution.

13. Web LLM Vulnerabilities
AI Security

OWASP Top 10 for LLMs, prompt injection, indirect prompt injection, sensitive data leakage, training data poisoning, and AI application attack vectors.

14. Active Directory Exploitation
AD Attacks

AS-REP Roasting, Kerberoasting, LLMNR/NBT-NS poisoning with Responder, Pass-the-Ticket, Golden/Silver tickets, and DCSync domain dump.

15. Payload Creation & Research
Payload Research

Msfvenom shellcode synthesis, payload encoding, dynamic payload research, multi/handler listeners, Meterpreter post-modules, and pivoting.

16. Professional Pentest Reporting
Documentation

Executive summary drafting, CVSSv3 risk ratings, detailed proof-of-concept steps, reproducible vulnerability walkthroughs, and remediation.

CAREER TRANSFORMATION

Penetration Testing Career Scope, Roadmap & Admissions

How modern penetration testing capabilities accelerate high-paying offensive security careers, cohort details, and enrollment.

Penetration Testing Career Scope & Target Enterprise Roles — Offensive Security Matrix

ENTERPRISE ROLE	CORE OPERATIONAL RESPONSIBILITIES	CAREER TRAJECTORY
Penetration Tester	Conduct authorized penetration tests on enterprise networks and web applications, document attack paths, and verify remediations.	Senior Pentester / Lead
Red Team Operator	Execute advanced adversary simulations against corporate infrastructure, test defensive controls, bypass EDR systems, and train blue teams.	Red Team Lead / Director
Security Consultant	Deliver client assessments, define testing scopes and rules of engagement, perform compliance security audits, and advise CISOs.	Principal Consultant
Vulnerability Analyst	Run continuous vulnerability scanning operations, triage CVSS severity ratings, coordinate with sysadmins, and audit patch rollouts.	SecOps / Vuln Manager
AppSec Engineer	Perform deep web application, API, and mobile source code reviews, identify logic flaws, and secure CI/CD software pipelines.	Lead AppSec Engineer
SOC Escalation Analyst	Leverage offensive hacker tradecraft knowledge to dissect active intrusions, investigate advanced malware, and conduct threat hunting.	Incident Response Lead

The 7-Step Student Penetration Testing Journey

1. **Enrollment** — Lab Onboarding
2. **Linux & Scripting** — Kali & Python
3. **Recon & Web** — Burp & Nmap
4. **Privilege Esc** — Linux & Windows
5. **Active Directory** — Pivots & Kerberos
6. **Reporting** — Commercial Reports
7. **Cert Readiness** — OSCP & CPTS Ready

Course Duration:	6 Months (Comprehensive Range Practice)	**Training Mode:**	Live Interactive Online + 24/7 Lab Access
Class Schedule:	Weekend & Weekday Evening Batches	**Trainer Credentials:**	Senior Penetration Testers & Elite Red Team Leads
Starting Date:	Upcoming Cohort (Contact Admissions)	**Course Fee:**	Inquire for Cohort Packages & Discounts

CERTIFICATION PREP **Includes Comprehensive CPTS & OSCP Preparations:** Hands-on training, methodology drills, and cyber range simulations specifically prepare candidates for official OSCP and CPTS examinations.

START BUILDING YOUR OFFENSIVE SECURITY CAREER WITH ALL SAFE

Take the next step toward developing professional penetration testing and adversary simulation skills through practical training, expert mentorship, and a supportive technical learning community.

DIRECT EMAIL
allsafeus@gmail.com

ENROLLMENT CONTACT
+92 321 2077222

OFFICIAL WEBSITE
www.allsafeinnovate.com

Contact ALL SAFE Today to Enroll in the Penetration Testing Program.