

Cybersecurity and Ethical Hacking Foundations

Authorised testing, evidence analysis and defensive controls

FA-0723 · 3 days

Cybersecurity

Introduction

Explore how common network and application weaknesses are identified, demonstrated and mitigated in an authorised training lab. Learn foundational terminology, selected Kali Linux tools and evidence-oriented analysis, then relate observations to practical defensive controls.

This three-day introduction uses selected guided exercises and prepared captures. It does not guarantee intermediate expertise, access to arbitrary devices, password recovery or universal bypass of encryption and modern wireless protections.

Learning outcomes

- Define an authorised test scope and document observations, limitations and remediation.
- Use basic Kali/Linux commands, lab networking and selected discovery tools.
- Inspect traffic captures and explain what encryption prevents an observer from reading.
- Recognise ARP/DNS manipulation, insecure wireless configurations and social-engineering risks.
- Investigate selected SQL injection, XSS, upload and command-execution weaknesses in intentionally vulnerable applications.
- Compare observed risks with network, endpoint, application and wireless hardening measures.

Prerequisites

- Basic operating-system, browser and file-management knowledge; no previous penetration-testing experience required.

- A compatible computer or supplied remote environment capable of running the isolated training VMs, with approved installation privileges only where needed.
- Reliable internet for remote delivery; a supported adapter and isolated wireless test equipment are needed only for an optional authorised radio demonstration.
- Exercises are limited to provided applications, captures and explicitly authorised lab targets.

Training outline

1. Day 1 — Scope, networking and the testing lab

- Security roles, attack categories and the relationship between a finding, impact and remediation.
- IP addressing, subnets, NAT, DHCP, DNS, ports, services and the OSI model; proxy concepts and their limits.
- Set up or access isolated Kali/target VMs, use the terminal and authorised SSH access, and inspect the sample web-server architecture.
- Compare passive observation with active discovery; use selected Nmap/Zenmap or netdiscover examples within the supplied scope.
- Document discovered services and distinguish an open port from a proven vulnerability.

2. Day 2 — Traffic and application testing

- Inspect supplied Wireshark captures using filters, stream tracing and protocol dissection.
- Demonstrate ARP/DNS manipulation and a controlled intermediary scenario on lab traffic; compare detection and prevention.
- Distinguish readable plaintext from TLS-protected data. Wireshark decryption needs appropriate secrets or endpoint cooperation; passive capture does not reveal every password or bypass HTTPS universally.
- Use selected Burp Suite exercises to inspect intentionally vulnerable SQL injection, XSS, file-upload and command-execution behaviour.
- Review input handling, output encoding, authorisation and secure configuration as relevant mitigations; report evidence rather than assume every platform behaves identically.

3. Day 3 — Wireless, social engineering and defensive review

- Wireless bands, adapter/capture constraints, rogue-access-point risks and controlled packet examples; optional demonstrations use isolated authorised equipment.
- Treat WEP as obsolete historical context; explain the assumptions behind WPA/WPA2 password-guessing and WPS weaknesses without promising recovery of any network key.

- Introduce WPA3 and protected management frames and their effect on password guessing and spoofed management-frame attacks.
- Recognise phishing and impersonation using benign examples and discuss consent-based simulation, response and account protection.
- Introduce reverse-engineering/forensic observations using a benign supplied artifact; advanced malware development and arbitrary tracking are not course outcomes.
- Review Metasploit or other testing-tool roles through a supplied demonstration, not a promise to master more than 20 tools.
- Consolidate wireless settings, segmentation, secure protocols, endpoint protections and suspicious-traffic detection into a small remediation/reporting exercise.