■ CLASSIFIED // CYBER WARFARE ACADEMY

SHADOWXLAB

CYBER • RANGE • ACADEMY

CEH v13

AI-POWERED ETHICAL HACKING

OFFICIAL SYLLABUS · TOC · LAB MANIFEST

20	221	44	AI v13
CORE MODULES	TOPICS	LIVE LABS	TRACK

doc-id: shadowx://syllabus/ceh-v13/0xA31F · rev 2026.05

■ DOCUMENT INDEX

Table of Contents

Program Overview

ShadowXLab's CEH v13 track aligns with EC-Council's official 20-module Certified Ethical Hacker v13 curriculum and adds a dedicated AI-Augmented Hacking module. Every topic below is reinforced inside the ShadowXLab

browser-based cyber range — no setup, fully isolated, MITRE ATT&CK; telemetry wired in.

■ CORE CURRICULUM

CEH v13 — 20 Official Modules

MOD 01 Introduction to Ethical Hacking — BEGINNER

■ TOPICS COVERED

- Information Security Overview
- Cyber Kill Chain & MITRE ATT&CK;
- Hacking Concepts & Phases
- Ethical Hacking Concepts & Scope
- Information Security Controls
- Laws, Standards & Compliance (GDPR, PCI-DSS, HIPAA)

■ HANDS-ON LABS

```
$ Lab 1.1 — Map an attack to MITRE ATT&CK; tactics
$ Lab 1.2 — Build a kill-chain diagram for a target org
```

MOD 02 Footprinting & Reconnaissance — BEGINNER

■ TOPICS COVERED

- Footprinting Concepts
- Search Engine & Advanced Google Hacking
- WHOIS, DNS & Network Footprinting
- Website & Email Footprinting
- OSINT via Social Networking
- Footprinting Countermeasures

■ HANDS-ON LABS

```
$ Lab 2.1 — Recon-ng full workspace recon
$ Lab 2.2 — theHarvester + Maltego pivot graph
$ Lab 2.3 — Google dorking for exposed assets
$ Lab 2.4 — Shodan / Censys attack surface map
```

MOD 03 Scanning Networks — INTERMEDIATE

TOPICS COVERED

- Network Scanning Concepts
- Host Discovery & Port Scanning
- Service & OS Fingerprinting
- Scanning Beyond IDS/Firewall
- Banner Grabbing
- Network Diagrams & Drawing

HANDS-ON LABS

```
$ Lab 3.1 — Nmap stealth + vuln scripts on /24
$ Lab 3.2 — Masscan internet-scale sweep
$ Lab 3.3 — Evade IDS with fragmentation & decoys
```

MOD 04 Enumeration — INTERMEDIATE

TOPICS COVERED

- NetBIOS, SNMP, LDAP, NTP, NFS Enumeration
- SMTP & DNS Enumeration
- IPsec, VoIP, RPC, Unix/Linux Enum
- SMB Enumeration
- Enumeration Countermeasures

HANDS-ON LABS

```
$ Lab 4.1 — enum4linux-ng against AD
$ Lab 4.2 — SNMPwalk → community string abuse
$ Lab 4.3 — LDAP anonymous bind enumeration
```

MOD 05 Vulnerability Analysis — INTERMEDIATE

TOPICS COVERED

- Vulnerability Assessment Concepts
- Classification & Assessment Types
- Assessment Tools & Reports
- CVSS Scoring
- Vulnerability Management Lifecycle

HANDS-ON LABS

```
$ Lab 5.1 — Nessus / OpenVAS full credentialed scan
$ Lab 5.2 — Triage CVEs with CVSS v4
```

MOD 06 System Hacking — ADVANCED

TOPICS COVERED

- Gaining Access (Password Cracking, Buffer Overflows)
- Privilege Escalation (Windows/Linux)
- Maintaining Access (Backdoors, Rootkits)
- Clearing Logs & Anti-Forensics
- Steganography

HANDS-ON LABS

```
$ Lab 6.1 — Hashcat GPU cracking of NTLM hashes
$ Lab 6.2 — Windows privesc via SeImpersonate (PrintSpoofer)
$ Lab 6.3 — Linux privesc — sudo / SUID chain
$ Lab 6.4 — Log clearing & artifact wiping
```

MOD 07 Malware Threats — ADVANCED

TOPICS COVERED

- Malware Concepts & APT
- Trojans, Viruses, Worms
- Fileless Malware
- Malware Analysis (Static / Dynamic)
- Anti-Malware Countermeasures

HANDS-ON LABS

```
$ Lab 7.1 — Static analysis with Ghidra
$ Lab 7.2 — Dynamic sandbox detonation (Cuckoo)
$ Lab 7.3 — Emotet traffic analysis
```

MOD 08 Sniffing — INTERMEDIATE

TOPICS COVERED

- Sniffing Concepts
- MAC Attacks, DHCP Attacks
- ARP Poisoning & DNS Poisoning
- Sniffing Tools (Wireshark, tcpdump)
- Sniffing Countermeasures & Detection

HANDS-ON LABS

```
$ Lab 8.1 — ARP spoof + credential capture
$ Lab 8.2 — DHCP starvation + rogue server
$ Lab 8.3 — DNS cache poisoning
```

MOD 09 Social Engineering — BEGINNER

TOPICS COVERED

- SE Concepts & Techniques
- Insider Threats
- Identity Theft
- Impersonation on Social Media
- SE Countermeasures
- Phishing Detection Tools

HANDS-ON LABS

```
$ Lab 9.1 — GoPhish phishing campaign
$ Lab 9.2 — Evilginx2 2FA bypass simulation
```

MOD 10 Denial-of-Service — INTERMEDIATE

TOPICS COVERED

- DoS / DDoS Concepts
- Attack Techniques (Volumetric, Protocol, Application)
- Botnets
- DoS Tools
- Detection & Countermeasures

HANDS-ON LABS

```
$ Lab 10.1 — SYN flood with hping3
$ Lab 10.2 — Slowloris application-layer DoS
$ Lab 10.3 — DDoS mitigation tuning
```

MOD 11 Session Hijacking — ADVANCED

TOPICS COVERED

- Application-Level Session Hijacking
- Network-Level Session Hijacking
- Token Theft & Replay
- TLS Stripping
- Countermeasures (HSTS, secure cookies)

HANDS-ON LABS

```
$ Lab 11.1 — Cookie theft via XSS → session replay
$ Lab 11.2 — TLS strip with bettercap
```

MOD 12 Evading IDS, Firewalls & Honeypots — ADVANCED

TOPICS COVERED

- IDS, IPS, Firewall Concepts
- Honeypot Detection
- Evasion Techniques
- Bypassing WAFs
- Detection Countermeasures

HANDS-ON LABS

```
$ Lab 12.1 — WAF bypass via encoding & HPP
$ Lab 12.2 — Snort rule evasion lab
```

MOD 13 Hacking Web Servers — ADVANCED

TOPICS COVERED

- Web Server Attacks (Misconfig, Directory Traversal, HTTP Smuggling)
- Web Server Attack Methodology
- Patch Management
- Hardening & Countermeasures

HANDS-ON LABS

```
$ Lab 13.1 — HTTP request smuggling on Nginx/Apache
$ Lab 13.2 — Tomcat manager RCE chain
```

MOD 14 Hacking Web Applications — ADVANCED

TOPICS COVERED

- OWASP Top 10 (2021)
- Injection (SQLi, NoSQLi, Command, LDAP)
- XSS / CSRF / SSRF
- Auth & Session Flaws
- API Security (REST / GraphQL)
- Web App Hacking Methodology

HANDS-ON LABS

```
$ Lab 14.1 — Boolean-blind SQLi with sqlmap
$ Lab 14.2 — DOM & stored XSS chain → account takeover
$ Lab 14.3 — SSRF → cloud metadata exfil
$ Lab 14.4 — GraphQL introspection & batching abuse
```

MOD 15 SQL Injection — ADVANCED

TOPICS COVERED

- SQLi Concepts & Types
- Error-based, Union-based, Blind, Time-based
- Out-of-band SQLi
- SQLi Tools (sqlmap)
- SQLi Countermeasures (Prepared Statements, WAF)

HANDS-ON LABS

```
$ Lab 15.1 — Union-based extraction lab
$ Lab 15.2 — Time-based blind to OOB exfil
```

MOD 16 Hacking Wireless Networks — INTERMEDIATE

TOPICS COVERED

- Wireless Concepts, Encryption (WEP/WPA/WPA2/WPA3)
- Wireless Threats
- Wireless Hacking Methodology
- Bluetooth Hacking
- Wireless Security Tools

HANDS-ON LABS

```
$ Lab 16.1 — WPA2 handshake capture + hashcat
$ Lab 16.2 — Evil twin captive-portal attack
$ Lab 16.3 — WPA3 Dragonblood-style downgrade
```

MOD 17 Hacking Mobile Platforms — INTERMEDIATE

TOPICS COVERED

- Android & iOS Attack Vectors
- Mobile Device Management
- Mobile Malware
- OWASP Mobile Top 10
- Mobile Security Tools

HANDS-ON LABS

```
$ Lab 17.1 — Android APK reversing with jadx + Frida
$ Lab 17.2 — iOS jailbreak + Objection runtime hooks
```

MOD 18 IoT and OT Hacking — ADVANCED

TOPICS COVERED

- IoT Architecture & Protocols (MQTT, CoAP, Zigbee, BLE)
- IoT Attacks
- OT/ICS/SCADA Attacks
- Modbus, DNP3, S7 Protocol Exploitation
- IoT Security Tools

HANDS-ON LABS

```
$ Lab 18.1 — MQTT broker enumeration + control hijack
$ Lab 18.2 — Modbus PLC tag manipulation
```

MOD 19 Cloud Computing — ADVANCED

TOPICS COVERED

- Cloud Models & Threats
- Container & Kubernetes Security
- Serverless Security
- AWS / Azure / GCP Attack Techniques
- Cloud Security Controls & CSPM

HANDS-ON LABS

```
$ Lab 19.1 — AWS IAM privilege escalation with Pacu
$ Lab 19.2 — Kubernetes pod escape → node takeover
$ Lab 19.3 — Azure AD device-code phishing
$ Lab 19.4 — GCP service-account key pivot
```

MOD 20 Cryptography — INTERMEDIATE

TOPICS COVERED

- Cryptography Concepts (Symmetric / Asymmetric / Hashing)
- PKI & Certificates
- Email & Disk Encryption
- Cryptanalysis & Attacks
- Quantum-Resistant Cryptography
- Cryptography Tools

HANDS-ON LABS

```
$ Lab 20.1 — Padding-oracle attack on CBC
$ Lab 20.2 — Certificate transparency monitoring
```

■ DIFFERENTIATOR

AI Track — Exclusive to v13

The v13 release of CEH formally integrates artificial-intelligence offense and defense. ShadowXLab extends this with a full AI-warfare track running on production-grade GPU pods.

MOD
Module
Add-on

AI-Augmented Ethical Hacking (CEH v13)

ADVANCED

■ TOPICS COVERED

- AI / GenAI Threat Landscape
- LLM Recon & OSINT Automation
- AI for Vulnerability Triage
- Prompt Injection & Jailbreak Attacks (OWASP LLM Top 10)
- Adversarial ML & Model Poisoning
- Deepfake & Synthetic Media Threats
- AI-Driven SOC Triage & Threat Hunting
- Defensive AI: Detection Engineering with ML

■ HANDS-ON LABS

```
$ AI-Lab 1 — Build an autonomous recon agent (LangChain + nmap)
$ AI-Lab 2 — Prompt injection against a tool-using agent
$ AI-Lab 3 — Model extraction / membership inference
$ AI-Lab 4 — LLM-assisted log triage in Splunk
$ AI-Lab 5 — Deepfake voice phishing simulation
```

■ MANIFEST

Complete Lab List

All 49 hands-on labs delivered inside the ShadowXLab cyber range.

#	LAB	MODULE	DIFFICULTY
1	Lab 1.1 — Map an attack to MITRE ATT&CK tactics	M01 — Introduction to Ethical Hacking	Beginner
2	Lab 1.2 — Build a kill-chain diagram for a target org	M01 — Introduction to Ethical Hacking	Beginner
3	Lab 2.1 — Recon-ng full workspace recon	M02 — Footprinting & Reconnaissance	Beginner
4	Lab 2.2 — theHarvester + Maltego pivot graph	M02 — Footprinting & Reconnaissance	Beginner
5	Lab 2.3 — Google dorking for exposed assets	M02 — Footprinting & Reconnaissance	Beginner
6	Lab 2.4 — Shodan / Censys attack surface map	M02 — Footprinting & Reconnaissance	Beginner
7	Lab 3.1 — Nmap stealth + vuln scripts on /24	M03 — Scanning Networks	Intermediate
8	Lab 3.2 — Masscan internet-scale sweep	M03 — Scanning Networks	Intermediate
9	Lab 3.3 — Evade IDS with fragmentation & decoys	M03 — Scanning Networks	Intermediate
10	Lab 4.1 — enum4linux-ng against AD	M04 — Enumeration	Intermediate
11	Lab 4.2 — SNMPwalk → community string abuse	M04 — Enumeration	Intermediate
12	Lab 4.3 — LDAP anonymous bind enumeration	M04 — Enumeration	Intermediate
13	Lab 5.1 — Nessus / OpenVAS full credentialed scan	M05 — Vulnerability Analysis	Intermediate
14	Lab 5.2 — Triage CVEs with CVSS v4	M05 — Vulnerability Analysis	Intermediate
15	Lab 6.1 — Hashcat GPU cracking of NTLM hashes	M06 — System Hacking	Advanced
16	Lab 6.2 — Windows privesc via SeImpersonate (PrintSpoofer)	M06 — System Hacking	Advanced
17	Lab 6.3 — Linux privesc — sudo / SUID chain	M06 — System Hacking	Advanced
18	Lab 6.4 — Log clearing & artifact wiping	M06 — System Hacking	Advanced
19	Lab 7.1 — Static analysis with Ghidra	M07 — Malware Threats	Advanced
20	Lab 7.2 — Dynamic sandbox detonation (Cuckoo)	M07 — Malware Threats	Advanced
21	Lab 7.3 — Emotet traffic analysis	M07 — Malware Threats	Advanced
22	Lab 8.1 — ARP spoof + credential capture	M08 — Sniffing	Intermediate
23	Lab 8.2 — DHCP starvation + rogue server	M08 — Sniffing	Intermediate
24	Lab 8.3 — DNS cache poisoning	M08 — Sniffing	Intermediate
25	Lab 9.1 — GoPhish phishing campaign	M09 — Social Engineering	Beginner

#	LAB	MODULE	DIFFICULTY
26	Lab 9.2 — Evilginx2 2FA bypass simulation	M09 — Social Engineering	Beginner
27	Lab 10.1 — SYN flood with hping3	M10 — Denial-of-Service	Intermediate
28	Lab 10.2 — Slowloris application-layer DoS	M10 — Denial-of-Service	Intermediate
29	Lab 10.3 — DDoS mitigation tuning	M10 — Denial-of-Service	Intermediate
30	Lab 11.1 — Cookie theft via XSS → session replay	M11 — Session Hijacking	Advanced
31	Lab 11.2 — TLS strip with bettercap	M11 — Session Hijacking	Advanced
32	Lab 12.1 — WAF bypass via encoding & HPP	M12 — Evading IDS, Firewalls & Honeypots	Advanced
33	Lab 12.2 — Snort rule evasion lab	M12 — Evading IDS, Firewalls & Honeypots	Advanced
34	Lab 13.1 — HTTP request smuggling on Nginx/Apache	M13 — Hacking Web Servers	Advanced
35	Lab 13.2 — Tomcat manager RCE chain	M13 — Hacking Web Servers	Advanced
36	Lab 14.1 — Boolean-blind SQLi with sqlmap	M14 — Hacking Web Applications	Advanced
37	Lab 14.2 — DOM & stored XSS chain → account takeover	M14 — Hacking Web Applications	Advanced
38	Lab 14.3 — SSRF → cloud metadata exfil	M14 — Hacking Web Applications	Advanced
39	Lab 14.4 — GraphQL introspection & batching abuse	M14 — Hacking Web Applications	Advanced
40	Lab 15.1 — Union-based extraction lab	M15 — SQL Injection	Advanced
41	Lab 15.2 — Time-based blind to OOB exfil	M15 — SQL Injection	Advanced
42	Lab 16.1 — WPA2 handshake capture + hashcat	M16 — Hacking Wireless Networks	Intermediate
43	Lab 16.2 — Evil twin captive-portal attack	M16 — Hacking Wireless Networks	Intermediate
44	Lab 16.3 — WPA3 Dragonblood-style downgrade	M16 — Hacking Wireless Networks	Intermediate
45	Lab 17.1 — Android APK reversing with jadx + Frida	M17 — Hacking Mobile Platforms	Intermediate
46	Lab 17.2 — iOS jailbreak + Objection runtime hooks	M17 — Hacking Mobile Platforms	Intermediate
47	Lab 18.1 — MQTT broker enumeration + control hijack	M18 — IoT and OT Hacking	Advanced
48	Lab 18.2 — Modbus PLC tag manipulation	M18 — IoT and OT Hacking	Advanced
49	Lab 19.1 — AWS IAM privilege escalation with Pacu	M19 — Cloud Computing	Advanced
50	Lab 19.2 — Kubernetes pod escape → node takeover	M19 — Cloud Computing	Advanced
51	Lab 19.3 — Azure AD device-code phishing	M19 — Cloud Computing	Advanced
52	Lab 19.4 — GCP service-account key pivot	M19 — Cloud Computing	Advanced
53	Lab 20.1 — Padding-oracle attack on CBC	M20 — Cryptography	Intermediate
54	Lab 20.2 — Certificate transparency monitoring	M20 — Cryptography	Intermediate

#	LAB	MODULE	DIFFICULTY
55	AI-Lab 1 — Build an autonomous recon agent (LangChain + nmap)	AI Track (v13 add-on)	Advanced
56	AI-Lab 2 — Prompt injection against a tool-using agent	AI Track (v13 add-on)	Advanced
57	AI-Lab 3 — Model extraction / membership inference	AI Track (v13 add-on)	Advanced
58	AI-Lab 4 — LLM-assisted log triage in Splunk	AI Track (v13 add-on)	Advanced
59	AI-Lab 5 — Deepfake voice phishing simulation	AI Track (v13 add-on)	Advanced

■ END OF DOCUMENT // SHADOWXLAB CYBER RANGE ACADEMY