

Certified Ethical Hacker (CEH v13)

3-Month Practical Training Programme

3 classes per week · 1 hour per class · 36 classes total

36 instruction hours + 4–6 hours per week lab practice

Live online · taught in English · open worldwide

A hands-on route through the CEH v13 syllabus. Every class ends with something you built, broke or captured yourself in your own lab — not a slide you watched.

WEEK 1

Build the Lab and Learn the Ground

Stand up a working attack lab and get fluent in the two operating systems you will live in.

CLASS	TOPIC	TOOLS USED	WHAT YOU BUILD
1	Build your hacking lab Install VirtualBox, Kali Linux, a Windows 10 victim VM and Metasploitable 2 on one NAT network.	VirtualBox, Kali Linux, Windows 10, Metasploitable 2	→ A 3-machine lab where every VM can ping the others.
2	Linux and Windows for attackers The commands you will actually type all course: files, users, services, processes, networking.	bash, PowerShell, netstat, ps, systemctl	→ Enumerate users, services and open ports on both VMs from the terminal.
3	Networking the way an attacker sees it IP, ports, TCP vs UDP, the OSI model and what a three-way handshake looks like on the wire.	Wireshark, ipconfig/ifconfig, ping, traceroute	→ Capture a live TCP handshake and label every packet in it.

WEEK 2

Footprinting and OSINT

Gather everything about a target without ever touching it.

CLASS	TOPIC	TOOLS USED	WHAT YOU BUILD
4	Passive reconnaissance WHOIS, DNS records, subdomain discovery and certificate transparency — all without sending a packet to the target.	whois, dig, dnsrecon, Sublist3r, crt.sh	→ Produce a full footprint of a domain you own, including every subdomain.
5	Google Dorking and Shodan Search operators that surface exposed panels, config files and devices the owner forgot about.	Google dorks, Shodan, Censys	→ Find exposed login panels and unsecured devices with Shodan filters.
6	OSINT on people and organisations Harvesting emails, usernames and staff structure, and drawing the relationships.	Maltego, theHarvester, Sherlock, Hunter.io	→ Build a Maltego graph of a company from a single domain name.

WEEK 3

Scanning Networks

Find live hosts, open ports and exactly what software is listening.

CLASS	TOPIC	TOOLS USED	WHAT YOU BUILD
7	Host discovery and port scanning Finding what is alive on a subnet, and TCP scan types including stealth SYN scans.	Nmap, netdiscover, Angry IP Scanner	→ Map every live host and open port in your lab subnet.
8	Service detection and NSE scripts Version fingerprinting and Nmap's scripting engine for automated checks.	nmap -sV -sC, NSE scripts, Netcat	→ Fingerprint every service on Metasploitable and script a vulnerability check.
9	Vulnerability scanning Running a real scanner, then reading the report critically instead of trusting it.	Nessus Essentials, OpenVAS, Nikto	→ Scan Metasploitable with Nessus and rank the findings by real risk.

WEEK 4

Enumeration

Turn open ports into usernames, shares and attack paths.

CLASS	TOPIC	TOOLS USED	WHAT YOU BUILD
10	SMB and NetBIOS enumeration Pulling shares, users and policies out of Windows file sharing.	enum4linux, smbclient, smbmap, CrackMapExec	→ List every share and local user on the Windows VM.
11	SNMP, LDAP, NFS and SMTP enumeration The forgotten services that hand over a user list for free.	snmpwalk, ldapsearch, showmount, smtp-user-enum	→ Extract a valid user list through SNMP and SMTP.
12	Web server and directory enumeration Finding the pages nobody linked to: admin panels, backups, .git folders.	Gobuster, Dirb, WhatWeb, Wappalyzer	→ Brute-force hidden directories on DVWA and fingerprint its stack.

WEEK 5

System Hacking — Gaining Access

Get your first shell, by guessing credentials and by exploiting a service.

CLASS	TOPIC	TOOLS USED	WHAT YOU BUILD
13	Online password attacks Brute force, dictionary and credential-stuffing attacks against live services.	Hydra, Medusa, Ncrack, rockyou.txt	→ Break into SSH and FTP in your lab with a targeted wordlist.
14	Offline hash cracking Where password hashes live, how to identify them and how fast a GPU really is.	John the Ripper, Hashcat, hashid, hashcat rules	→ Dump Windows NTLM hashes and crack them offline.
15	Gaining Windows system access Exploiting a vulnerable SMB service to land a SYSTEM-level shell on Windows.	Metasploit, EternalBlue (MS17-010), msfconsole	→ Exploit the Windows VM and prove SYSTEM access with whoami.

WEEK 6

Post-Exploitation and Privilege Escalation

Turn a foothold into full control of the machine.

CLASS	TOPIC	TOOLS USED	WHAT YOU BUILD
16	Meterpreter post-exploitation What to do in the first five minutes after a shell: situational awareness and stability.	Meterpreter, migrate, hashdump, screenshot, keyscan	→ Take a screenshot, log keystrokes and migrate to a stable process.
17	Windows privilege escalation Unquoted service paths, weak permissions, stored credentials and token abuse.	WinPEAS, PowerUp, Mimikatz, accesschk	→ Escalate a standard user to SYSTEM and dump credentials from memory.
18	Linux privilege escalation SUID binaries, sudo misconfigurations, cron jobs and writable paths.	LinPEAS, GTF0Bins, pspy, linux-exploit-suggester	→ Escalate to root three different ways on the same box.

WEEK 7

Malware, Payloads and Persistence

Build your own payloads, keep access, and understand how defenders catch them.

CLASS	TOPIC	TOOLS USED	WHAT YOU BUILD
19	Creating malware payloads Generating reverse shells and backdoored executables, and how encoders change the file.	msfvenom, Veil, Shellter, multi/handler	→ Build an EXE reverse shell, deliver it in the lab and catch the callback.
20	Trojans, backdoors and persistence Surviving a reboot: registry run keys, scheduled tasks, services and startup folders.	Metasploit persistence, schtasks, reg, Autoruns	→ Install persistence, reboot the victim and regain your shell automatically.
21	Antivirus evasion and malware triage Why a payload gets flagged, basic obfuscation, and how an analyst picks it apart.	VirusTotal, PEStudio, strings, obfuscation	→ Analyse your own payload the way a defender would, and note what gave it away.

WEEK 8

Sniffing, Spoofing and Man-in-the-Middle

Get between two machines and read what passes.

CLASS	TOPIC	TOOLS USED	WHAT YOU BUILD
22	Packet sniffing Capturing traffic, filtering it properly, and pulling credentials out of plaintext protocols.	Wireshark, tcpdump, tshark, display filters	→ Capture FTP and HTTP logins from lab traffic in cleartext.
23	ARP spoofing and MITM Poisoning the ARP cache to sit between a victim and the gateway.	Ettercap, Bettercap, arpspoof, sslstrip	→ Run a MITM between two lab VMs and read their traffic live.
24	DNS spoofing and denial of service Redirecting a victim by answering DNS first; volumetric, protocol and app-layer DoS.	Bettercap, dnsspoof, hping3, Slowloris	→ DNS-spoof a lab host to your page, then simulate a SYN flood.

WEEK 9

Web Application Hacking

Break the applications that hold the data.

CLASS	TOPIC	TOOLS USED	WHAT YOU BUILD
25	Burp Suite and web recon Proxying your browser, intercepting requests, and mapping an application properly.	Burp Suite, OWASP ZAP, Burp Repeater/Intruder	→ Intercept a request, change a hidden field and watch the app accept it.
26	SQL Injection From a single quote to a full database dump, manually and then automated.	SQLMap, Burp, DVWA, bWAPP	→ Dump the entire DVWA database through an injectable parameter.
27	XSS, CSRF, file upload and LFI/RFI Stealing sessions, forcing actions, and uploading a shell through a file field.	Burp, DVWA, bWAPP, BeEF	→ Steal a session cookie with stored XSS and upload a web shell.

WEEK 10

Wireless, Mobile and Active Directory

The three attack surfaces every real engagement touches.

CLASS	TOPIC	TOOLS USED	WHAT YOU BUILD
28	WiFi hacking Monitor mode, capturing the WPA2 four-way handshake, and cracking it offline.	Aircrack-ng, airodump-ng, aireplay-ng, Wifite, hcxdumpool	→ Capture a WPA2 handshake from your own router and crack it.
29	Android hacking and RAT payloads Building a malicious APK, binding it, and controlling a device you own.	msfvenom (APK), Metasploit, AndroRAT, Android Studio emulator	→ Build an APK payload and control your own emulator from Meterpreter.
30	Active Directory attacks How a single domain user becomes Domain Admin: Kerberoasting, AS-REP roasting, DCSync.	BloodHound, SharpHound, Rubeus, Impacket, Kerbrute, Mimikatz	→ Map an attack path in BloodHound and Kerberoast a service account.

WEEK 11

Social Engineering, Cloud and IoT

Attack the human, the tenant and the device.

CLASS	TOPIC	TOOLS USED	WHAT YOU BUILD
31	Social engineering and phishing Cloning a login page, crafting a pretext, and running a measured phishing simulation.	SET (Social-Engineer Toolkit), GoPhish, Zphisher	→ Clone a login page in the lab and capture test credentials.
32	Cloud and container misconfiguration Public buckets, over-permissive IAM, exposed metadata and vulnerable images.	ScoutSuite, Prowler, Trivy, AWS/Azure CLI	→ Audit a free-tier cloud account you own and fix what you find.
33	IoT, OT and session hijacking Default credentials, exposed protocols, and taking over a live session.	Shodan, Burp, Wireshark, Routersploit	→ Hijack a session using a stolen cookie and explain the fix.

Full Engagement, Reporting and Exam

Do the whole job end to end and write it up like a professional.

CLASS	TOPIC	TOOLS USED	WHAT YOU BUILD
34	Full engagement — part 1 Recon through to exploitation against an unseen lab target, on the clock.	Everything from weeks 1–11	→ Compromise a target you have not seen before, documenting as you go.
35	Full engagement — part 2 and reporting Post-exploitation, evidence capture, CVSS scoring and client-grade writing.	CVSS calculator, report template, Markdown/Word	→ Produce a full penetration-test report with findings, evidence and fixes.
36	CEH exam preparation and capstone Exam format, question strategy, and presenting your engagement.	Mock exam bank	→ Sit a mock CEH exam and present your capstone findings to the class.

Lab and conduct. Every technique in this programme is practised inside a lab you build yourself, on machines and networks you own. Students are never asked to touch a third-party system. The same techniques are illegal without written authorisation from the system owner, and the course teaches the authorisation and scoping process alongside the tooling.

Requirements. A computer with 8 GB RAM or more and roughly 100 GB free disk space, plus a stable internet connection. Every tool used in this outline is free or has a free tier — there is no additional software cost.