POWERED BY AI · ZERO TO HERO

THE CYBER ACADEMIA

ETHICAL HACKING ZERO TO HERO

A modern, fully hands-on 3-month cybersecurity program — built around the tools, attacks, and defenses that matter in 2026 and mapped to real industry practice and the MITRE ATT&CK framework.

LEARN | CERTIFY | ENGAGE | COMPETE

12 WEEKS · 48 LECTURES · 220+ LAB HOURS

12	4/wk	48	20+	100%
WEEKS	LECTURES	SESSIONS	MODULES	HANDS-ON

Complete Curriculum & Syllabus · 2026 Edition · Beginner → Job-Ready Practitioner

Build a Real Cybersecurity Career — From Zero to Hero

This is a 12-week intensive built for people starting from scratch. Four lectures a week, more than half of every session spent in a live lab. You begin with the absolute fundamentals — how networks and operating systems actually work — and finish running a full simulated red-team engagement against a modern enterprise, cloud, and AI stack. By the end you don't just know the theory; you can do the job.

Who This Is For

- Absolute beginners with no security background
- IT / networking / dev professionals pivoting into security
- Final-year CS / IT students targeting SOC, pentest, or red-team roles
- Anyone preparing for PenTest+, eJPT, or OSCP-style certifications

What Makes It "2026"

- AI & LLM attack/defense woven through every phase, not bolted on
- Cloud-native, container, and Kubernetes exploitation
- Zero Trust, identity-first attacks, and modern EDR/XDR evasion
- Post-quantum crypto, deepfakes, and supply-chain threats

Every Week Has 4 Lectures

- **Lecture 1 — Concept:** theory, attack surface, how it breaks
- **Lecture 2 — Tooling / Deep Dive:** the modern toolkit, hands-on walkthrough
- **Lecture 3 — Lab:** guided end-to-end exploitation on live targets
- **Lecture 4 — Defense + Challenge:** countermeasures & a graded CTF-style task

> **The AI edge.** Every week you'll use AI assistants (ShellGPT-style copilots, LLM recon, automated report writing) to work faster — and you'll also learn to **attack** AI systems using the OWASP LLM Top 10.

By the Numbers

12 Weeks, in 3 monthly phases	**48** Live lectures (4 per week)	**20+** Core modules, industry-aligned
550+ Attack techniques practiced	**4000+** Industry hacking & security tools	**1** Full capstone red-team engagement

Three Months, Three Phases

Each month builds on the last. You never move forward without proving you can apply what came before.

Phase	Weeks	Focus & Outcome
Month 1 Foundations & Recon	1 – 4	Networking, Linux, and the hacker mindset. Set up your attack lab (Kali/ Parrot), master reconnaissance, scanning, enumeration, and vulnerability analysis. **Outcome:** you can map any target and find its weak points.
Month 2 Exploitation & Access	5 – 8	Gaining access: system hacking, web & API exploitation, malware concepts, social engineering, network attacks, and wireless. **Outcome:** you can exploit a vulnerability end-to-end and maintain access.
Month 3 Modern & Advanced	9 – 12	Cloud, containers, IoT/OT, AI/LLM hacking, cryptography, Active Directory, evasion, and a full capstone engagement + reporting. **Outcome:** you can run and document a professional assessment.

Prerequisite check (Week 0, self-paced): basic computer literacy is all you need coming in. A short primer on binary, IP addressing, and command-line basics is provided before Week 1 so nobody is left behind.

MONTH 1 · WEEKS 1–4

FOUNDATIONS, LAB SETUP & RECONNAISSANCE

Understand how systems work before you break them. Build your arsenal, then learn to see a target the way an attacker does.

W1 Cyber Foundations & The Hacker Mindset

Goal: understand the landscape, the law, and how networks & operating systems actually work.

L1 — CONCEPT

Introduction to Ethical Hacking

The **CIA triad** (confidentiality, integrity, availability); difference between threat, vulnerability, risk, and exploit; hacker types (white / black / grey hat) and real threat actors including APTs; the **five phases of hacking** and the cyber kill chain; scope, written authorization, and the laws that separate ethical hacking from crime.

L2 — CONCEPT

How Networks Really Work

The **OSI & TCP/IP models** and data encapsulation; IP addressing and subnetting basics, MAC vs IP; core protocols (HTTP/S, DNS, DHCP, ARP, ICMP); ports and services; the **TCP three-way handshake** — the foundation everything else builds on.

L3 — LAB

Linux Command Line + Traffic Analysis

Linux filesystem, users & permissions, and essential bash; networking commands (**ip, ss, netstat, dig**); capturing and reading live packets in **Wireshark** — apply filters, follow a TCP stream, and watch a handshake happen in real time.

L4 — DEFENSE + CTF

Security Controls & Ethics

Defense-in-depth and control types (preventive / detective / corrective); responsible disclosure and bug-bounty ethics; **first mini-CTF:** analyze a provided packet capture to recover a hidden flag.

Lab environment: install & configure Kali/Parrot, VirtualBox/VMware, and an isolated lab network.

W2 Footprinting & OSINT Reconnaissance

Goal: gather everything about a target without ever touching it directly.

L1 — CONCEPT

Reconnaissance Fundamentals

Passive vs active recon and why the distinction matters legally; footprinting methodology; mapping the attack surface across three angles — network, organization, and people; what information leakage looks like in the real world.

L2 — TOOLING

The OSINT Toolkit

WHOIS and DNS enumeration; subdomain discovery (Amass, subfinder); **Shodan & Censys** for exposed devices; advanced Google dorking; email/username harvesting with theHarvester; relationship mapping in **Maltego**; social-media and metadata OSINT.

L3 — LAB

Build a Full Target Profile

Compile a complete passive profile of an authorized target — domains, hosts, emails, tech stack, and leaked data; then use an **LLM assistant** to correlate and summarize scattered findings into a briefing at speed.

L4 — DEFENSE + CTF

Anti-Recon & Reporting

Reducing your organization's digital footprint and OSINT hygiene; **graded task:** deliver a footprinting report on a sandbox company.

2026 edge: using LLMs to correlate and summarize large volumes of scattered OSINT.

W3 Scanning & Enumeration

Goal: discover live hosts, open ports, running services, users, and shares.

L1 — CONCEPT

Network Scanning Theory

Host discovery techniques; scan types (**SYN, Connect, UDP**) and how TCP flags drive them; service/version and OS fingerprinting; how firewalls and IDS see your scans.

L2 — DEEP DIVE

Nmap Mastery & Service Enumeration

Nmap flags, timing templates, output formats, and the **NSE scripting engine**; enumerating the services that matter — **SMB, SNMP, LDAP, NFS, SMTP, RPC** — to pull users, shares, and versions.

L3 — LAB

Map an Entire Network

Run discovery across the lab range, identify every live host and open service, and build a **topology & asset inventory** you'll attack in later weeks.

L4 — DEFENSE + CTF

Evasion & Timed Challenge

Scan detection, rate-limiting, and IDS-aware scanning; **timed CTF:** find a deliberately hidden service and enumerate it for the flag.

Tools: Nmap, Masscan, RustScan, enum4linux-ng, NetExec.

W4 Vulnerability Analysis & Assessment

Goal: turn discovered services into a prioritized, validated list of weaknesses.

L1 — CONCEPT

Vulnerability Management

The vulnerability lifecycle; reading **CVE** entries and **CVSS** scores; using **EPSS** and the **KEV catalog** to prioritize what actually gets exploited; true vs false positives.

L2 — TOOLING

Vulnerability Scanners

Driving **Nessus, OpenVAS, and Nuclei**; authenticated vs unauthenticated scans; interpreting scanner output and separating signal from noise.

L3 — LAB

Assess & Validate Findings

Scan the lab network, triage results, and **manually confirm** top findings; map vulnerabilities to public exploits with searchsploit / Exploit-DB.

L4 — CAPSTONE

Month 1 Capstone Report

Deliverable: a complete recon → scan → vulnerability-assessment report with risk ratings and prioritized remediation — your first professional artifact.

Milestone: you can independently profile a target and produce a findings report.

MONTH 2 · WEEKS 5–8

EXPLOITATION, WEB, MALWARE & ACCESS

This is where you go from finding weaknesses to exploiting them. Systems, web apps, humans, and networks — end to end.

W5 System Hacking & Gaining Access

Goal: exploit a vulnerability, get a shell, escalate privileges, and persist.

L1 — CONCEPT

Exploitation Fundamentals

How exploits and payloads work; **bind vs reverse shells**, staged vs stageless; the Metasploit framework model (msfconsole, modules, Meterpreter); finding and adapting public exploits safely.

L2 — CONCEPT

Privilege Escalation & Password Attacks

Windows & Linux privesc vectors — misconfigurations, SUID binaries, weak services, token abuse; password attacks (brute force, dictionary, spraying); **hash cracking** with John and Hashcat.

L3 — LAB

Full Kill Chain on a Live Box

Exploit → get a shell → **escalate to root/SYSTEM** → establish persistence → clear tracks; dump and crack credentials with Mimikatz.

L4 — DEFENSE + CTF

Logging Awareness & Boot-to-Root

How EDR and logging catch attackers, and evasion basics; **challenge:** a full boot-to-root CTF machine.

Tools: Metasploit, Hydra, John, Hashcat, Mimikatz, WinPEAS/LinPEAS.

W6 Web Application & API Hacking

Goal: exploit the OWASP Top 10 and modern API vulnerabilities end to end.

L1 — CONCEPT

Web Architecture & the OWASP Top 10

How HTTP, cookies, sessions, and same-origin policy work; the flaws that dominate real bugs — **SQL injection, XSS** (stored/reflected/DOM), **SSRF, IDOR, CSRF**, and broken authentication.

L2 — DEEP DIVE

Burp Suite & API Attacks

Burp Suite proxy, Repeater, and Intruder for intercepting and tampering; **JWT** attacks; abusing REST and **GraphQL** APIs; mass assignment and broken object-level authorization.

L3 — LAB

Exploit a Web App + API

Automated injection with **sqlmap**, working XSS payloads, and an SSRF pivot to an internal service; **chain multiple flaws** into a full application compromise.

L4 — DEFENSE + CTF

Secure Coding & Web CTF

Input validation, output encoding, security headers, and WAF concepts; **web CTF:** an SSRF + injection chain to capture the flag.

Tools: Burp Suite, OWASP ZAP, sqlmap, ffuf, Postman, PortSwigger Web Security Academy.

W7 Malware, Sniffing & Social Engineering

Goal: understand payloads, intercept traffic, and hack the human layer.

L1 — CONCEPT

Malware & Analysis Basics

Malware families — viruses, worms, trojans, RATs, **ransomware** — plus fileless and APT techniques; the difference between **static and dynamic analysis**; indicators of compromise (IOCs) and sandboxing.

L2 — CONCEPT

Sniffing & the Human Attack Surface

ARP/DNS spoofing and man-in-the-middle interception; the psychology of social engineering; phishing, vishing, and pretexting; running a campaign with a phishing framework.

L3 — LAB

Analyze a Sample & Simulate Phishing

Detonate a malware sample in a sandbox and extract IOCs; build and launch a **controlled phishing simulation** against consenting lab users with GoPhish.

L4 — DEFENSE + CTF

AI-Era Threats & Awareness

Deepfake video and AI-voice phishing — how they work and how to detect them; designing awareness training and social-engineering countermeasures.

Tools: Wireshark, bettercap, GoPhish, sandbox (any.run-style), Cuckoo.

W8 Network, Wireless & DoS Attacks

Goal: attack the network fabric and the wireless perimeter.

L1 — CONCEPT

Network Attacks & Evasion

Session hijacking; DoS/DDoS techniques and amplification; how firewalls, IDS/IPS, and honeypots work — and the fundamentals of evading them.

L2 — CONCEPT

Wireless Security

Wi-Fi standards and the security of **WEP / WPA2 / WPA3**; handshake and **PMKID** capture; **Evil Twin** and rogue access points; deauthentication attacks.

L3 — LAB

Crack Wi-Fi + Run a MITM

Capture and **crack a WPA2 handshake** with Aircrack-ng and Hashcat; perform an authorized man-in-the-middle on the lab network and harvest traffic.

L4 — CAPSTONE

Month 2 Capstone

Multi-stage attack: recon → exploit → establish a network foothold → loot — chaining everything from the last four weeks.

Tools: Aircrack-ng, Wifite, hcxtools, Scapy, hping3.

MONTH 3 · WEEKS 9–12

CLOUD, AI, ADVANCED THREATS & CAPSTONE

The modern battlefield: cloud-native infra, AI systems, IoT/OT, and the enterprise identity plane — finished with a full engagement and pro report.

W9 Cloud & Container Security

Goal: attack and defend AWS/Azure/GCP, Docker, and Kubernetes.

L1 — CONCEPT

Cloud Attack Surface

Cloud service models and the **shared-responsibility model**; the flaws that cause real breaches — **IAM misconfigurations**, over-permissive roles, public storage buckets, leaked keys, and metadata-service SSRF.

L2 — CONCEPT

Containers & Kubernetes

Docker fundamentals, image vulnerabilities, and **container escapes**; Kubernetes attack surface — exposed API server, **RBAC abuse**, secrets exposure, and pod breakout.

L3 — LAB

Break the Cloud

Exploit a deliberately misconfigured cloud account with **Pacu / CloudGoat**; attack a vulnerable Kubernetes cluster with kube-hunter and escalate.

L4 — DEFENSE + CTF

Cloud Hardening & CTF

Least privilege, CSPM, and image scanning (Trivy); **challenge:** escalate privileges through a misconfigured IAM policy.

Tools: Pacu, ScoutSuite, Prowler, stratus-red-team, Kubescape, Peirates, Trivy, CloudGoat.

W10 Hacking AI Systems & Using AI to Hack

Goal: attack LLM/ML systems and weaponize AI copilots — responsibly.

L1 — CONCEPT

OWASP Top 10 for LLMs

Prompt injection (direct and indirect) and jailbreaks; training-data poisoning; insecure output handling; **model theft**, excessive agency, and sensitive-information disclosure — the vulnerabilities unique to AI systems.

L2 — CONCEPT

AI-Assisted Offense

Using LLM copilots for recon, payload generation, exploit drafting, and **automated report writing**; automating repetitive tasks to work faster; the ethics and limits of AI-assisted hacking.

L3 — LAB

Break a Vulnerable AI App

Use **prompt injection and jailbreaks** to bypass a chatbot's guardrails, leak its system prompt, and extract secrets; run an automated LLM red-team pass with **Garak, PyRIT, and Promptfoo**.

L4 — DEFENSE + CTF

Securing AI Applications

Guardrails, input/output filtering, allow-lists, and monitoring for AI apps; **AI red-team CTF.**

2026 edge: attacking and securing AI is the single most in-demand skill this year.

W11 Active Directory, IoT/OT & Cryptography

Goal: own the enterprise identity plane and understand edge & crypto attacks.

L1 — CONCEPT

Active Directory Attacks

AD structure, Kerberos, and NTLM; enumeration and attack-path mapping with **BloodHound CE**; **Kerberoasting, AS-REP roasting, pass-the-hash, lateral movement**, DCSync, and **AD Certificate Services (ESC) attacks** with Certipy — how modern enterprises actually fall.

L2 — CONCEPT

IoT/OT & Cryptography

IoT, OT, and **ICS/SCADA** architecture and threats; cryptography, hashing, and PKI/TLS in practice; the **quantum risk** to today's encryption and post-quantum cryptography readiness.

L3 — LAB

Own the Domain

Compromise a full lab Active Directory environment — from a single low-privilege user all the way to **Domain Admin** — using Impacket, Rubeus, and CrackMapExec.

L4 — DEFENSE + CTF

Zero Trust & Detection

Zero Trust architecture, tiered admin, and detection engineering; **challenge:** an AD attack-path CTF.

Tools: BloodHound CE, Impacket, Rubeus, Certipy, NetExec, Ligolo-ng, Hashcat.

W12 Capstone Engagement & Reporting

Goal: run a full assessment like a professional and deliver a client-grade report.

L1 — CONCEPT

Engagement Methodology

Industry methodologies — **PTES, OWASP, and MITRE ATT&CK**; rules of engagement and scoping; OPSEC and an evasion recap; how to run an assessment safely and professionally.

L2 — CONCEPT

Professional Reporting

Report structure and the difference between **executive and technical** sections; assigning risk ratings; writing clear evidence, remediation, and retest guidance; communicating findings to non-technical stakeholders.

L3 — LAB

Live Capstone Engagement

A **full engagement** against a modern emulated organization spanning network, web, cloud, and Active Directory — applying the entire five-phase kill chain against a real, live lab environment.

L4 — FINAL

Submit, Defend & Plan Ahead

Submit and **defend your final penetration-test report**; then a career and certification roadmap session — PenTest+, eJPT, OSCP, and building a portfolio.

Final deliverable: a complete penetration-test report — your portfolio centerpiece.

The 2026 Toolkit You'll Actually Use

Industry-standard tools and current AI-driven tooling, mapped to what practitioners reach for on real engagements today.

Recon & Scanning

› Nmap · › Masscan · › RustScan · › naabu · › httpx · › katana

› Shodan · › theHarvester · › Maltego · › Amass · › Nuclei

Exploitation & Post-Exploitation

› Metasploit · › Impacket · › NetExec · › Mimikatz · › BloodHound CE

› Certipy · › Rubeus · › Ligolo-ng · › Sliver · › Havoc

Web & API

› Burp Suite · › Caido · › OWASP ZAP · › sqlmap · › ffuf · › Autorize

› Postman

Cloud, Container & Wireless

› Pacu · › ScoutSuite · › Prowler · › stratus-red-team · › Kubescape

› Peirates · › Trivy · › Aircrack-ng · › Wifite

AI & Automation

› AI shell copilots · › PentestGPT · › Garak · › PyRIT · › Promptfoo

› Burp AI · › Nuclei AI templates

New in 2026 › The toolkit stays current: **PyRIT & Promptfoo** for AI red-teaming, **Certipy** for AD Certificate Services (ESC) attacks, **Ligolo-ng** for modern pivoting, **stratus-red-team & Kubescape** for cloud-native attack simulation, and the **ProjectDiscovery** suite (naabu, httpx, katana, Nuclei) for automated recon.

Attack platform: Kali Linux or Parrot OS in an isolated, 100%-virtualized lab. Every attack you learn is performed only against provided, authorized targets — ethics and legal scope are reinforced every single week.

What You Can Do After 12 Weeks

MAP ANY TARGET

Perform recon, scanning, enumeration, and vulnerability analysis on networks, web apps, and cloud.

EXPLOIT END-TO-END

Chain vulnerabilities from initial access to privilege escalation, lateral movement, and persistence.

HACK MODERN STACKS

Attack cloud, containers, Kubernetes, Active Directory, wireless, and AI/LLM systems.

THINK LIKE A DEFENDER

Recommend real countermeasures — hardening, Zero Trust, detection, and EDR/XDR tuning.

USE AI AS A FORCE MULTIPLIER

Accelerate recon, exploitation, and reporting with AI — and secure AI apps against attack.

REPORT LIKE A PRO

Deliver a client-grade penetration-test report with risk ratings and remediation guidance.

Career Roles This Prepares You For

1. Penetration Tester
2. Ethical Hacker / Red Teamer
3. SOC Analyst (L1 / L2)
4. Vulnerability Assessment Analyst
5. Web Application Pentester
6. Cloud Security Analyst
7. Cybersecurity Analyst
8. Threat Hunting Analyst
9. AI / ML Security Engineer
10. Security Consultant
11. Incident Responder
12. Exploitation Analyst

Certifications You'll Be Ready For

- › CompTIA Security+
- › CompTIA PenTest+
- › eJPT / eCPPT
- › OSCP (foundation)
- › CRTP / CRTO

Assessment & Grading

- Weekly graded lab challenges (CTF-style flags)
- 3 monthly capstone assessments
- Final capstone engagement + written report
- Knowledge checks & a mock certification exam

WE DON'T JUST TEACH HACKING — WE BUILD CYBER CAREERS

The Cyber Academia · 12 weeks · Zero to Hero · Powered by AI, grounded in real practice.

This syllabus is an independent training curriculum by The Cyber Academia, built around current 2026 industry practice and the MITRE ATT&CK framework. All offensive techniques are taught strictly for authorized, ethical, and defensive purposes only.