SYSTEMS · TAUGHT WITH HACK THE BOX

Cybersecurity

Threat modelling, applied cryptography, web vulnerabilities and detection. You test authorized lab targets, write findings that actually get fixed, and build the monitoring that catches the next attempt.

Foundational | 4 phases | 20 sessions | 30 contact hours

Syllabus

4 phases, 20 sessions. Each phase ends in something you have built.

1 Ground Truth

Get the legal boundary and the systems fundamentals in place before touching a target.

5 sessions
$72 alone

1.1 Authorization First

Define scope, write rules of engagement, follow coordinated disclosure, and name the laws you can be charged under.

FREE PREVIEW

1.2 Linux for People Who Have Never Used It

Move around a shell and read users, permissions, processes, services, and the logs they leave behind.

1.3 Windows and Active Directory, Briefly

Read accounts, privileges, and event logs, and explain why most enterprise intrusions start with identity.

1.4 Networks You Can Read

Trace TCP/IP, DNS, HTTP, and TLS, and pull a story out of a packet capture in Wireshark.

1.5 Threat Modeling

Draw trust boundaries, apply STRIDE, map attack surface, and rank what actually matters.

By the end: **A signed rules-of-engagement document plus a threat model and network map for a lab environment you did not build.**

2 Code, Crypto, and Identity

Write the small amount of code this work needs, and understand the primitives every control rests on.

4 sessions
$72 alone

2.1 Python and Bash You Will Actually Use
Send HTTP requests from code, parse tool output, loop over hosts, and automate the boring half of a test.

2.2 Crypto You Use, Not Crypto You Invent
Pick the right hash, symmetric cipher, and signature, and recognize the failure modes behind A04:2025.

2.3 TLS, Certificates, and Trust
Explain what a certificate proves, how a chain is validated, and what a browser warning page really means.

2.4 Passwords, Sessions, and Identity
Store credentials with Argon2, reason about MFA, and follow an OAuth and OIDC login end to end.

By the end: **A password, session, and TLS audit of a lab web app, with a script that proves each fix holds.**

3 Authorized Testing

Find real vulnerabilities on deliberately vulnerable lab targets and write the fix for every one.

6 sessions
$72 alone

3.1 Recon and Enumeration, In Scope
Map an authorized target with Nmap, fingerprint its services, and stop cleanly where scope ends.

3.2 Broken Access Control
Test authorization per object and per function against A01:2025, which now absorbs SSRF and the API BOLA and BFLA cases.

3.3 Misconfiguration and the Supply Chain
Hunt default credentials and exposed admin surfaces for A02:2025, then read an SBOM and triage dependency risk for A03:2025.

3.4 Injection and Insecure Design
Exploit and then patch SQL injection, command injection, and XSS, and name the design flaws no input filter fixes.

3.5 Getting a Shell on a Lab Box
Work a Hack The Box Starting Point machine from foothold to Linux privilege escalation, documenting every command as you go.

3.6 Writing the Report
Turn evidence into CVSS v4.0 scores, business impact, and remediation a developer will actually act on.

By the end: **A findings report on an authorized lab target: reproduction steps, evidence, CVSS score, and a working patch per issue.**

4 Defense and Response

Detect the attacks you just practiced, work one incident end to end, and stop the bug class from shipping again.

5 sessions
$72 alone

4.1 Logs, Telemetry, and the SOC
Choose log sources, normalize events, and work a triage queue the way an analyst does on a normal Tuesday.

4.2 Detection Engineering
Map attacker behavior to MITRE ATT&CK, write Sigma rules for it, and tune out the false positives you create.

4.3 Incident Response
Run triage, containment, and a forensic timeline, then write a postmortem that blames the system and not a person.

4.4 Cloud and Identity Security
Audit IAM policies, public storage, and logging in a cloud account you inherited, under the shared responsibility model.

4.5 Securing AI Systems
Test for prompt injection, improper output handling, and excessive agency, then constrain what an agent is allowed to do.

By the end: **A detection rule set mapped to MITRE ATT&CK plus an incident response runbook and a written postmortem.**

Tools you will use

Hack The Box Academy | PortSwigger Web Security Academy | OWASP Juice Shop | Burp Suite Community | Wireshark | Nmap | Semgrep | Elastic Security

What you will build

1. **Juice Shop Teardown**
   Every finding mapped to OWASP Top 10:2025 and shipped with a patch
2. **Starting Point Writeup**
   One authorized lab box, documented command by command
3. **Mini-SOC**
   Detect the attack you ran, then write the runbook for it

Registration

Phase 1: Ground Truth	$72
Phase 2: Code, Crypto, and Identity	$72
Phase 3: Authorized Testing	$72
Phase 4: Defense and Response	$72
Whole track, all 4 phases	**$240**

Buying every phase separately costs $288, so the whole track saves $48.

No payment is taken online. Registering creates an order and payment instructions are sent with it. Access opens once payment is confirmed.