TIER 1 · OFFENSIVE

Penetration Testing

Course syllabus · Prerequisite HRCF

HRCPT HackersRange Certified Penetration Tester

Offensive Security & Penetration Testing. Plan and execute an end-to-end assessment of networks, web applications and Active Directory — and report it to professional standard.

240 h	16	13	70%
TOTAL HOURS	WEEKS	MODULES	LABORATORY

ABOUT HACKERSEYE · HackersRange Academy

We are a working offensive and incident-response firm — and we teach the way we work.

HackersEye is an elite Israeli cyber-security firm, founded by senior operators from government, military and corporate security backgrounds. The same people who built their careers attacking and defending real networks today run live offensive engagements, incident response and security operations for organisations that cannot afford to be wrong.

HackersRange Academy is the training arm of that firm, built on one principle: you learn cyber security by doing the real work — not by watching slides or answering multiple-choice questions. Every learner operates a live, fully instrumented company network, with real adversary activity, and is assessed on the evidence they produce, exactly as they would be on the job.

The range is powered by our own technology. An **AI-driven content engine** builds and refreshes scenarios drawn from live engagements, and our proprietary **HackersRange Suite** provisions each learner an isolated, browser-reachable enterprise on demand. Behind it stands a **24/7 incident-response desk** and the operators who write and teach every module.

HackersEye operates to international standards and is **certified to ISO/IEC 27001** for information security management. The credentials earned here — the HRC certifications — map to the roles employers actually hire for, because they are built by the people already doing those roles.

WHY TRAIN WITH US

- **Assessed on real work** — evidence on a live range, never multiple choice.
- **Operators, not slideware** — the team that runs real engagements writes every module.
- **An always-on range** — your own isolated enterprise, ready in the browser, day or night.
- **Credentials employers trust** — HRC certifications mapped to real job roles.

HOW THE ACADEMY WORKS

1

Learn the discipline

Concise instruction frames each topic and the tradecraft behind it.

2

Work the live range

The majority of your hours are spent operating a real, instrumented enterprise.

3

Prove it on evidence

Every module and capstone is scored on what you do, not what you memorise.

COURSE OVERVIEW · Tier 1 · Offensive

Offensive Security & Penetration Testing. Plan and execute an end-to-end assessment of networks, web applications and Active Directory — and report it to professional standard.

WHO THIS IS FOR	Aspiring penetration testers and offensive-security professionals, plus defenders and IT staff who want to understand attacks by performing them under professional discipline.
PREREQUISITES Entry requirements	**HRCF** — HRCF (Intro to Cyber) or equivalent proven ability: confident Linux and Windows command-line use, a working grasp of TCP/IP and web requests, and the security fundamentals covered in the foundation track.
HOW IT IS DELIVERED Format	Instructor-led sessions frame each offensive discipline, then roughly seventy percent of your hours are spent attacking live, exploitable networks, web applications and Active Directory on the range under professional rules of engagement.
CERTIFICATION HRCPT · practical capstone	HRCPT is awarded on a hands-on capstone: a full external-to-domain-compromise assessment on the range, scored on the access you achieve, your methodology and a professional-standard report — never multiple choice.
PROGRESSION Next tracks	PT Expert · Red Team

240 h	**16**	**13**	**70**%
TOTAL HOURS	WEEKS	MODULES	ON THE RANGE

CURRICULUM · modules 1–2 of 13

PT-01 Methodology, Scoping & Ethics

12 HOURS

You learn how a real engagement is scoped, agreed and kept inside legal and ethical limits. This is the professional discipline that separates a tester from an attacker.

LEARNING OBJECTIVES

- [ ] By the end you can scope an engagement and agree clear rules of engagement.
- [ ] By the end you can operate inside the legal and ethical limits of authorised testing.
- [ ] By the end you can follow a recognised testing methodology from start to finish.
- [ ] By the end you can handle findings and client data responsibly.

TOPICS COVERED

- Engagement types and objectives
- Scoping and rules of engagement
- Legal authorisation and liability
- Ethics and professional conduct
- Methodologies: PTES, OWASP, OSSTMM
- Handling and protecting findings

RANGE LAB

You produce a scope and rules-of-engagement document for a range target, then plan an authorised assessment against a recognised methodology — the professional groundwork every later attack sits on.

ASSESSMENT You submit a scope, rules of engagement and methodology plan for a range engagement, graded on completeness, legal soundness and professional judgement.

PT-02 Reconnaissance & OSINT

15 HOURS

You gather everything a target reveals about itself in public before you touch a single system. You build the map of people, domains and services that guides the whole test.

LEARNING OBJECTIVES

- [ ] By the end you can gather open-source intelligence on a target's people and infrastructure.
- [ ] By the end you can enumerate an organisation's external attack surface.
- [ ] By the end you can distinguish passive reconnaissance from active footprinting.
- [ ] By the end you can turn raw findings into an attack map that guides the test.

TOPICS COVERED

- Passive versus active reconnaissance
- OSINT sources and techniques
- DNS and subdomain enumeration
- Discovering people and credentials
- External attack-surface mapping
- Building the target picture

RANGE LAB

You footprint a range organisation from the outside — enumerating its domains, services and people from public sources — and assemble the attack-surface map that will guide every stage that follows.

ASSESSMENT You deliver a reconnaissance report and attack-surface map for a range target, graded on thoroughness, accuracy and how well it sets up the engagement.

CURRICULUM, CONTINUED · modules 3–4 of 13

PT-03 Scanning & Enumeration

16 HOURS

You use Nmap and related tools to find live hosts, open ports and running services across the range. You turn a raw network into a clear list of things worth attacking.

LEARNING OBJECTIVES

- [ ] By the end you can discover live hosts and open ports across a network with Nmap.
- [ ] By the end you can fingerprint services and versions accurately.
- [ ] By the end you can enumerate services deeply to reveal attackable detail.
- [ ] By the end you can turn scan output into a prioritised target list.

TOPICS COVERED

- Host discovery and port scanning
- Nmap scan types and timing
- Service and version fingerprinting
- Nmap scripting engine
- Enumerating SMB, web and other services
- From scan data to a target list

RANGE LAB

You scan and enumerate a range network end to end with Nmap and supporting tools, fingerprinting every service and turning the raw output into a clear, prioritised list of the systems and services worth attacking.

ASSESSMENT You deliver a full enumeration of a range network with a prioritised target list, graded on completeness, accuracy of service identification and prioritisation.

PT-04 Vulnerability Analysis

16 HOURS

You match the services you found to known weaknesses and judge which are real and which are noise. You learn to prioritise by impact, not by scanner score.

LEARNING OBJECTIVES

- [ ] By the end you can map discovered services to their known vulnerabilities.
- [ ] By the end you can verify a vulnerability manually rather than trusting a scanner.
- [ ] By the end you can prioritise findings by real-world impact and exploitability.
- [ ] By the end you can separate a genuine weakness from a false positive.

TOPICS COVERED

- Vulnerability research and CVE mapping
- Automated scanning and its limits
- Manual verification techniques
- Exploitability versus severity
- Prioritising by impact, not score
- Identifying false positives

RANGE LAB

You take the enumerated services from a range network, research their weaknesses, and manually verify which are genuinely exploitable — producing a prioritised list driven by real impact rather than scanner severity.

ASSESSMENT You deliver a verified, prioritised vulnerability analysis for a range network, graded on accuracy, manual verification and the soundness of your prioritisation.

CURRICULUM, CONTINUED · modules 5–6 of 13

PT-05 Exploitation Fundamentals

18 HOURS

You get your first real foothold, using Metasploit and manual techniques to turn a weakness into access. You learn what a working exploit actually looks like on a live host.

LEARNING OBJECTIVES

- [ ] By the end you can turn a verified vulnerability into a working foothold.
- [ ] By the end you can use Metasploit to select, configure and launch an exploit.
- [ ] By the end you can run a manual exploit where a framework module does not fit.
- [ ] By the end you can stabilise and maintain an initial shell.

TOPICS COVERED

- Exploitation concepts and payloads
- The Metasploit Framework
- Manual exploitation techniques
- Reverse and bind shells
- Stabilising and upgrading shells
- Post-exploitation basics

RANGE LAB

You gain your first real foothold on a range host, using Metasploit and manual techniques to turn a verified weakness into an interactive shell — then stabilise it into a working session you can operate from.

ASSESSMENT You demonstrate a documented foothold on a range target, graded on successful exploitation, methodology and a reproducible account of how you got in.

PT-06 Web Application Pentesting I

18 HOURS

You attack web applications with Burp Suite, exploiting injection, broken access and authentication flaws. You learn the OWASP-style weaknesses that dominate real reports.

LEARNING OBJECTIVES

- [ ] By the end you can find and exploit injection flaws such as SQL injection and XSS.
- [ ] By the end you can exploit broken access control and authentication weaknesses.
- [ ] By the end you can drive Burp Suite to intercept, manipulate and automate web attacks.
- [ ] By the end you can map a web application's attack surface systematically.

TOPICS COVERED

- The OWASP Top 10
- SQL injection and command injection
- Cross-site scripting
- Broken access control and IDOR
- Authentication and session flaws
- Attacking with Burp Suite

RANGE LAB

You attack a vulnerable web application on the range with Burp Suite, exploiting injection, broken access control and authentication flaws to reach data and functionality you should never be able to touch.

ASSESSMENT You exploit and document a set of web vulnerabilities on a range application, graded on successful exploitation, methodology and clarity of the write-up.

CURRICULUM, CONTINUED · modules 7–8 of 13

PT-07 Web Application Pentesting II

18 HOURS

You take on harder web targets — chained bugs, tricky logic flaws and modern app defences. You learn to think past the obvious and combine weaknesses into a real breach.

LEARNING OBJECTIVES

- [ ] By the end you can identify and exploit business-logic flaws.
- [ ] By the end you can chain multiple weaknesses into a single meaningful breach.
- [ ] By the end you can attack server-side flaws such as SSRF and deserialisation.
- [ ] By the end you can work around modern application defences.

TOPICS COVERED

- Business-logic vulnerabilities
- Server-side request forgery
- Insecure deserialisation
- Chaining vulnerabilities
- Bypassing input filters and WAFs
- Attacking APIs and modern frameworks

RANGE LAB

You take on a harder range web target, chaining a logic flaw and a server-side vulnerability into a full compromise — thinking past the obvious single bug to reach internal systems the application was meant to protect.

ASSESSMENT You exploit a chained, non-trivial web compromise on the range, graded on the sophistication of the chain, methodology and quality of the report.

PT-08 Password & Credential Attacks

16 HOURS

You capture and crack credentials with Hashcat and learn how stolen passwords open the next door. You see why weak and reused passwords are still the fastest way in.

LEARNING OBJECTIVES

- [ ] By the end you can capture credential material from hosts and traffic.
- [ ] By the end you can crack password hashes with Hashcat using appropriate strategies.
- [ ] By the end you can reuse recovered credentials to reach further systems.
- [ ] By the end you can explain why weak and reused passwords remain a primary risk.

TOPICS COVERED

- Hash types and where credentials live
- Capturing hashes from hosts and traffic
- Cracking with Hashcat: wordlists, rules and masks
- Password spraying and credential stuffing
- Credential reuse and lateral access
- Pass-the-hash fundamentals

RANGE LAB

You capture credential material from range hosts and traffic, crack the hashes with Hashcat, and reuse the recovered passwords to open the next door — proving how quickly weak and reused credentials cascade.

ASSESSMENT You recover and reuse credentials to extend access on the range, graded on successful cracking, effective reuse and a documented account of the method.

CURRICULUM, CONTINUED · modules 9–10 of 13

PT-09 Active Directory Fundamentals

18 HOURS

You learn how Windows Active Directory really works — users, groups, trusts and where it is weak. This is the backbone of almost every enterprise you will ever test.

LEARNING OBJECTIVES

- [ ] By the end you can explain how Active Directory structures users, groups and trusts.
- [ ] By the end you can describe how Kerberos and NTLM authentication work.
- [ ] By the end you can enumerate an AD domain to find weaknesses.
- [ ] By the end you can identify the misconfigurations that make AD attackable.

TOPICS COVERED

- Active Directory structure and objects
- Domains, forests and trusts
- Kerberos and NTLM authentication
- Group policy and delegation
- AD enumeration techniques
- Common AD misconfigurations

RANGE LAB

You enumerate a live Active Directory domain on the range — mapping its users, groups, trusts and delegation — and identify the misconfigurations that turn a normal domain into an attack path.

ASSESSMENT You deliver an enumeration of a range AD domain with identified weaknesses, graded on completeness, accuracy and correct identification of attackable misconfigurations.

PT-10 Active Directory Attacks

20 HOURS

You map an AD domain with BloodHound and Impacket and follow the paths that lead to full control. You learn the attacks that take a tester from one user to domain admin.

LEARNING OBJECTIVES

- [ ] By the end you can map attack paths in a domain with BloodHound.
- [ ] By the end you can execute Kerberoasting and AS-REP roasting attacks.
- [ ] By the end you can abuse Impacket to move laterally and dump credentials.
- [ ] By the end you can walk a path from a single user to domain admin.

TOPICS COVERED

- Attack-path analysis with BloodHound
- Kerberoasting and AS-REP roasting
- Impacket toolkit for lateral movement
- Credential dumping and DCSync
- Abusing ACLs and delegation
- Escalation to domain admin

RANGE LAB

You compromise a live Active Directory domain on the range, mapping it with BloodHound and following the shortest path from a single foothold user to full domain-admin control with Impacket and Kerberos attacks.

ASSESSMENT You achieve and document domain-admin compromise on a range AD environment, graded on the attack path taken, methodology and reproducibility.

CURRICULUM, CONTINUED · modules 11–12 of 13

PT-11 Privilege Escalation

17 HOURS

You turn a low-privilege foothold into full control on both Windows and Linux hosts. You learn to spot the misconfigurations that hand you the keys.

LEARNING OBJECTIVES

- [ ] By the end you can escalate privileges on a Windows host from a low-privilege foothold.
- [ ] By the end you can escalate privileges on a Linux host to root.
- [ ] By the end you can enumerate a host systematically for escalation vectors.
- [ ] By the end you can recognise the misconfigurations that lead to escalation.

TOPICS COVERED

- Local enumeration for privilege escalation
- Windows escalation: services, tokens, unquoted paths
- Linux escalation: SUID, sudo, cron, capabilities
- Kernel and software exploits
- Credential harvesting on the host
- Automated enumeration tooling

RANGE LAB

You start with a low-privilege shell on Windows and Linux range hosts and systematically enumerate each for the misconfiguration that hands you full control — escalating to SYSTEM and to root.

ASSESSMENT You escalate to full privilege on Windows and Linux range hosts, graded on successful escalation, systematic enumeration and a documented method.

PT-12 Post-Exploitation & Pivoting

18 HOURS

You use one compromised host to reach deeper into the network and pivot toward hidden systems. You learn how attackers spread from a single foothold to the whole estate.

LEARNING OBJECTIVES

- [ ] By the end you can establish persistence on a compromised host.
- [ ] By the end you can pivot through a compromised host to reach segmented networks.
- [ ] By the end you can move laterally across an estate with harvested credentials.
- [ ] By the end you can collect and stage loot from compromised systems.

TOPICS COVERED

- Post-exploitation objectives
- Persistence techniques
- Pivoting and port forwarding
- Lateral movement methods
- Reaching segmented networks
- Data collection and staging

RANGE LAB

You use a single compromised range host as a pivot into a segmented internal network, moving laterally with harvested credentials to reach systems that were never exposed — spreading from one foothold across the estate.

ASSESSMENT You pivot and move laterally to reach otherwise-unreachable range systems, graded on the depth of access achieved and a documented account of the movement.

CURRICULUM, CONTINUED · modules 13–13 of 13

PT-13 Reporting & Remediation

38 HOURS

You write a clear, professional report that a client can actually act on, with practical fixes. The graded capstone scores a full external-to-domain-compromise assessment on the range.

LEARNING OBJECTIVES

- [ ] By the end you can write a professional penetration-test report a client can act on.
- [ ] By the end you can rate findings and recommend practical, prioritised remediation.
- [ ] By the end you can communicate technical risk to a non-technical audience.
- [ ] By the end you can execute a full external-to-domain-compromise assessment end to end.

TOPICS COVERED

- Professional report structure
- Writing findings and evidence
- Risk rating and CVSS
- Practical, prioritised remediation
- Executive summaries and client communication
- The end-to-end engagement workflow

> **RANGE LAB**
> The pentest capstone: you run a full assessment on the range from external foothold to domain compromise, then deliver the professional report — findings, evidence, risk ratings and remediation — a paying client would receive.

ASSESSMENT Graded capstone scored on a complete external-to-domain-compromise assessment: the access achieved, your methodology and the professional quality of your report.

OUTCOMES & CERTIFICATION

YOU WILL GRADUATE ABLE TO

- [ ] Scope an engagement and operate within legal and ethical constraints.
- [ ] Exploit network, web-application and Active Directory weaknesses to escalate access.
- [ ] Move from external foothold to domain compromise and write a professional report.
- [ ] Aligns to OffSec OSCP, TCM PNPT, INE eJPT/eCPPT and PenTest+.

TOOLS YOU WILL WORK WITH

Nmap · Burp Suite · Metasploit · BloodHound · Impacket · Hashcat · CrackMapExec

PREREQUISITE	**HRCF** — completed before starting this track.
CERTIFICATION	**HRCPT** — HackersRange Certified Penetration Tester, awarded on the practical capstone.
NEXT TRACKS	PT Expert · Red Team

PLANS & ENROLMENT · individual membership

CURRENT INDIVIDUAL-PLAN PRICING

Full access to HackersRange Academy on an individual membership. Prices shown are for individual enrolment and are current at publication — they may be updated over time. Every plan includes your own always-on range and progress scored on real work.

Recruit

$29 / month

$24/mo billed yearly · $290/yr

- Guided career paths & core scenarios
- Community, leaderboard & skill map
- Your own always-on range
- Progress scored on real work

MOST POPULAR

Operator

$59 / month

$49/mo billed yearly · $590/yr

- **Everything in Recruit**
- Full scenario & machine library, all disciplines
- CISO Room executive tabletops
- Larger range, priority spin-up
- Path to an HRC certification

Elite

$99 / month

$82/mo billed yearly · $990/yr

- **Everything in Operator**
- HRC certification exams included
- Highest range capacity
- Mentor check-ins & new content first

7-day free trial · no card required · cancel anytime. Start on any plan and switch whenever you like.

Training a team? Enterprise, government, universities and partners run on dedicated ranges, priced per seat. Talk to us at **hackerseye.com**.