HACKERS EYE ©

HACKERSRANGE ACADEMY

TIER 2 · EXPERT CAPSTONE

PT Expert · Red Team

Course syllabus · Prerequisite HRCPT

HRCRTO HackersRange Certified Red Team Operator

Advanced Offensive Operations & Red Teaming. Full adversary emulation against a defended enterprise — advanced AD, evasion, C2 and exploit development against production EDR and a live monitoring team.

320 h	20	11	75%
TOTAL HOURS	WEEKS	MODULES	LABORATORY

+972 52-425-7718 · Emergency@hackerseye.com

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 2 · Expert capstone

Advanced Offensive Operations & Red Teaming. Full adversary emulation against a defended enterprise — advanced AD, evasion, C2 and exploit development against production EDR and a live monitoring team.

WHO THIS IS FOR

Experienced penetration testers moving into red-team operations and adversary emulation, and offensive professionals who must operate against production defences and a live blue team.

PREREQUISITES

Entry requirements

HRCPT — HRCPT (Penetration Testing) or equivalent professional experience: fluent exploitation of networks, web applications and Active Directory, confident lateral movement and privilege escalation, and professional reporting.

HOW IT IS DELIVERED

Format

Instructor-led sessions cover advanced tradecraft, then the majority of your hours are spent running full-scope operations against a defended enterprise on the range — production EDR, real logging and a live monitoring team hunting you in real time.

CERTIFICATION

HRCRTO · practical capstone

HRCRTO is awarded on a hands-on capstone: a full-scope red-team engagement against a live monitoring team on the range, scored on objectives achieved, operational security, evasion and both red- and purple-team reporting.

320 h	20	11	75%
TOTAL HOURS	WEEKS	MODULES	ON THE RANGE

CURRICULUM · modules 1–2 of 11

PTX-01 Red Team Operations & Adversary Emulation

24 HOURS

You plan a full red team engagement that copies how a chosen real-world attacker behaves. You learn to run an operation with clear goals, rules and OPSEC rather than just breaking in.

LEARNING OBJECTIVES

- [ ] By the end you can plan a full-scope red-team engagement with defined objectives.
- [ ] By the end you can build an adversary-emulation plan from real threat intelligence.
- [ ] By the end you can maintain operational security throughout an operation.
- [ ] By the end you can run an engagement as a controlled operation rather than an ad-hoc break-in.

TOPICS COVERED

- Red teaming versus penetration testing
- Objectives, rules of engagement and deconfliction
- Adversary emulation from threat intelligence
- Operational security for operators
- Attack-lifecycle planning
- Engagement command and control

RANGE LAB

You build an adversary-emulation plan for a defended range enterprise, selecting a real-world threat actor to emulate and turning its known tradecraft into an operation with objectives, rules of engagement and an OPSEC plan.

ASSESSMENT You submit an adversary-emulation engagement plan for a range operation, graded on realism, fidelity to the emulated actor and the soundness of your OPSEC and objectives.

PTX-02 Advanced Active Directory Attacks

28 HOURS

You attack hardened and multi-domain Active Directory setups that the basic techniques no longer beat. You learn the trust and delegation abuses that lead to cross-forest control.

LEARNING OBJECTIVES

- [ ] By the end you can attack hardened Active Directory where basic techniques fail.
- [ ] By the end you can abuse trusts to move across domains and forests.
- [ ] By the end you can exploit constrained and resource-based delegation.
- [ ] By the end you can achieve cross-forest domain dominance.

TOPICS COVERED

- Attacking hardened AD
- Domain and forest trust abuse
- Constrained and resource-based delegation
- Active Directory Certificate Services abuse
- Cross-forest attack paths
- Bypassing AD hardening controls

RANGE LAB

You attack a hardened, multi-domain Active Directory forest on the range where the standard techniques are blocked — abusing trusts and delegation to move between domains and reach cross-forest control.

ASSESSMENT You achieve cross-domain or cross-forest compromise against hardened range AD, graded on the sophistication of the path and a documented, reproducible method.

CURRICULUM, CONTINUED · modules 3–4 of 11

PTX-03 Advanced Kerberos & Ticket Attacks

28 HOURS

You forge and abuse Kerberos tickets with Rubeus and Mimikatz to move and persist unseen. You learn the ticket attacks that quietly grant lasting access to a domain.

LEARNING OBJECTIVES

- [ ] By the end you can forge golden and silver tickets to impersonate any principal.
- [ ] By the end you can abuse Kerberos delegation for lateral movement.
- [ ] By the end you can operate Rubeus and Mimikatz for ticket attacks.
- [ ] By the end you can use ticket attacks to persist quietly in a domain.

TOPICS COVERED

- Kerberos protocol internals
- Golden and silver ticket forging
- Pass-the-ticket and overpass-the-hash
- Delegation abuse for movement
- Rubeus and Mimikatz tradecraft
- Ticket-based persistence

RANGE LAB

You forge and wield Kerberos tickets on a range domain with Rubeus and Mimikatz — impersonating privileged principals, moving laterally with stolen tickets, and planting ticket-based persistence that survives a password reset.

ASSESSMENT You demonstrate ticket forging, impersonation and persistence on the range, graded on technical execution, stealth and a documented account of each attack.

PTX-04 Evasion & Defense Bypass

30 HOURS

You rework your tools and techniques to slip past production EDR and logging. You learn what actually triggers a defender and how modern operators stay quiet.

LEARNING OBJECTIVES

- [ ] By the end you can modify payloads and techniques to evade production EDR.
- [ ] By the end you can bypass application-control and logging defences.
- [ ] By the end you can explain what telemetry a given action generates.
- [ ] By the end you can operate quietly against an instrumented estate.

TOPICS COVERED

- How EDR and modern defences work
- Payload obfuscation and packing
- AMSI, ETW and logging bypass
- Application-control bypass
- In-memory and fileless execution
- Understanding and minimising telemetry

RANGE LAB

You rework your tooling against production EDR on the range, testing payloads and techniques until they execute without tripping the sensors and logging — learning exactly which actions light up a defender's console and how to stay dark.

ASSESSMENT You demonstrate execution against a monitored range host with minimal detection, graded on evasion effectiveness and your documented analysis of the telemetry avoided.

CURRICULUM, CONTINUED · modules 5–6 of 11

PTX-05 Command & Control Infrastructure

28 HOURS

You stand up resilient C2 with Cobalt Strike, Sliver and Mythic and shape traffic to blend in. You learn to run and hide the channel that controls your implants.

LEARNING OBJECTIVES

- [ ] By the end you can stand up resilient command-and-control infrastructure.
- [ ] By the end you can shape C2 traffic to blend with legitimate activity.
- [ ] By the end you can deploy redirectors and domain fronting to hide the channel.
- [ ] By the end you can operate Cobalt Strike, Sliver and Mythic.

TOPICS COVERED

- C2 frameworks: Cobalt Strike, Sliver, Mythic
- Listener and profile configuration
- Malleable C2 and traffic shaping
- Redirectors and domain fronting
- Resilient and segmented infrastructure
- Operating and hiding the channel

RANGE LAB

You build resilient C2 infrastructure on the range with Cobalt Strike, Sliver and Mythic — configuring redirectors and shaping traffic profiles so the channel controlling your implants blends into ordinary network noise.

ASSESSMENT You stand up and operate a resilient, low-signature C2 setup on the range, graded on infrastructure design, traffic blending and operational resilience.

PTX-06 Initial Access & Social Engineering Operations

28 HOURS

You engineer a realistic way in — phishing, pretext and payloads that survive email and endpoint defences. You learn how modern intrusions actually start with a person, not a port.

LEARNING OBJECTIVES

- [ ] By the end you can plan and run a phishing operation with a credible pretext.
- [ ] By the end you can craft payloads that survive email and endpoint defences.
- [ ] By the end you can harvest credentials or gain execution through initial-access tradecraft.
- [ ] By the end you can model how a modern intrusion begins with a person.

TOPICS COVERED

- Initial-access tradecraft
- Pretext and campaign design
- Phishing infrastructure and delivery
- Payloads that bypass email and endpoint controls
- Credential harvesting and MFA-phishing
- Adversary-in-the-middle techniques

RANGE LAB

You engineer a realistic initial-access operation against the range enterprise — building the pretext, the delivery infrastructure and a payload that survives the mail gateway and endpoint controls to land your first foothold through a person.

ASSESSMENT You plan and execute an initial-access operation on the range, graded on pretext credibility, payload survivability and a documented, controlled campaign.

CURRICULUM, CONTINUED · modules 7–8 of 11

PTX-07 Advanced Web & API Exploitation

28 HOURS

You break modern web applications and APIs, chaining deep flaws to reach internal systems. You learn the server-side and logic attacks that a standard test misses.

LEARNING OBJECTIVES

- [ ] By the end you can exploit advanced server-side vulnerabilities to reach internal systems.
- [ ] By the end you can attack modern APIs and their authorisation models.
- [ ] By the end you can chain deep flaws into a full compromise.
- [ ] By the end you can find the logic and server-side bugs a standard test misses.

TOPICS COVERED

- Advanced SSRF and internal pivoting
- Deserialisation and template injection
- API and GraphQL exploitation
- Authorisation and access-control chains
- Request smuggling and cache attacks
- Chaining to internal compromise

RANGE LAB

You break a modern web and API stack on the range, chaining an advanced server-side flaw through to internal systems — reaching the network behind the application in ways a standard web test would never surface.

ASSESSMENT You exploit a chained web-to-internal compromise on the range, graded on the depth of the chain, technical execution and quality of the report.

PTX-08 Exploit Development Fundamentals

28 HOURS

You debug binaries with x64dbg and build a working exploit from a crash to code execution. You learn how memory-corruption bugs become the exploits that others just run.

LEARNING OBJECTIVES

- [ ] By the end you can debug a binary and analyse a crash with x64dbg.
- [ ] By the end you can develop a working exploit from a memory-corruption bug.
- [ ] By the end you can reason about modern exploit mitigations and their bypasses.
- [ ] By the end you can turn a crash into reliable code execution.

TOPICS COVERED

- Memory-corruption fundamentals
- Debugging with x64dbg
- Stack-based buffer overflows
- Bypassing DEP and ASLR
- Return-oriented programming basics
- From crash to code execution

RANGE LAB

You take a crashing binary on the range, analyse it in x64dbg, and build a working exploit from the memory-corruption bug up to reliable code execution — understanding first-hand how the exploits others simply run are actually made.

ASSESSMENT You develop and demonstrate a working exploit against a range binary, graded on reliability of code execution and a documented account of the development.

CURRICULUM, CONTINUED · modules 9–10 of 11

PTX-09 Cloud & Hybrid Identity Attacks

26 HOURS

You attack cloud tenants and the identity that links them to on-premises Active Directory with Certipy. You learn how attackers pivot between the network and the cloud.

LEARNING OBJECTIVES

- [ ] By the end you can attack a cloud tenant's identity and access model.
- [ ] By the end you can pivot between on-premises Active Directory and the cloud.
- [ ] By the end you can abuse certificate services and federation with Certipy.
- [ ] By the end you can compromise hybrid identity across the network-cloud boundary.

TOPICS COVERED

- Cloud identity and access models
- Hybrid identity and directory sync
- AD Certificate Services abuse with Certipy
- Federation and token abuse
- Pivoting between on-prem and cloud
- Cloud persistence techniques

RANGE LAB

You attack a hybrid range environment, abusing certificate services and federated identity with Certipy to pivot from on-premises Active Directory into the cloud tenant — and back — following the trust that links the two.

ASSESSMENT You demonstrate a hybrid identity compromise crossing the on-prem and cloud boundary, graded on the attack path and a documented, reproducible method.

PTX-10 Lateral Movement, Persistence & Domain Dominance

28 HOURS

You spread across a defended estate, plant durable persistence and take full domain control. You learn to hold access quietly while a live team hunts for you.

LEARNING OBJECTIVES

- [ ] By the end you can move laterally across a defended estate without being caught.
- [ ] By the end you can establish durable, stealthy persistence.
- [ ] By the end you can achieve and hold full domain dominance.
- [ ] By the end you can maintain access while a live team actively hunts for you.

TOPICS COVERED

- Stealthy lateral movement
- Advanced persistence mechanisms
- Defence-aware credential access
- Domain dominance techniques
- Evading active threat hunting
- Long-haul access and OPSEC

RANGE LAB

You spread through a defended range estate against a live monitoring team, moving laterally with care, planting durable persistence, and taking full domain control while staying below the threshold that would give you away.

ASSESSMENT You achieve and hold domain dominance against an actively hunted range estate, graded on depth of access, stealth and durability of persistence.

CURRICULUM, CONTINUED · modules 11–11 of 11

PTX-11

Red Team Reporting & Purple Teaming

44 HOURS

You turn the operation into a report defenders can act on and run a purple-team debrief with them. The graded capstone scores a full-scope engagement against a live monitoring team.

LEARNING OBJECTIVES

- [ ] By the end you can write a red-team report that improves the defence, not just lists wins.
- [ ] By the end you can run a purple-team debrief that maps attacks to detections.
- [ ] By the end you can present an operation to technical and executive audiences.
- [ ] By the end you can run a full-scope engagement against a live monitoring team end to end.

TOPICS COVERED

- Red-team report structure and narrative
- Mapping the operation to ATT&CK
- Detection and control gap analysis
- Running a purple-team debrief
- Executive and board communication
- The end-to-end operation workflow

RANGE LAB

The red-team capstone: you run a full-scope engagement against a live monitoring team on the range — from initial access to domain dominance under active defence — then deliver the report and run the purple-team debrief that makes the blue team better.

ASSESSMENT Graded capstone scored on a full-scope engagement against a live blue team: objectives achieved, operational security and evasion, and the quality of your red- and purple-team reporting.

OUTCOMES & CERTIFICATION

YOU WILL GRADUATE ABLE TO

- [ ] Plan and run a full-scope red team engagement with adversary emulation and OPSEC.
- [ ] Evade and operate against EDR and a live monitoring team using current tradecraft.
- [ ] Achieve cross-forest domain dominance and deliver red and purple-team reporting.
- [ ] Aligns to OffSec OSEP, Zero-Point CRTO, OSWE and Altered Security CRTP/CRTE.

TOOLS YOU WILL WORK WITH

Cobalt Strike | Sliver | Mythic | Certipy | Rubeus | Mimikatz | x64dbg

PREREQUISITE	**HRCPT** — completed before starting this track.
CERTIFICATION	**HRCRTO** — HackersRange Certified Red Team Operator, awarded on the practical capstone.

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**.