HACKERS EYE ©

HACKERSRANGE ACADEMY

TIER 0 · FOUNDATION

Intro to Cyber

Course syllabus · Open enrolment

HRCF HackersRange Certified, Foundations

Cyber Foundations. The computing, networking and security baseline every other track depends on — taken with no prior security knowledge.

120 h	8	8	50%
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 0 · Foundation

Cyber Foundations. The computing, networking and security baseline every other track depends on — taken with no prior security knowledge.

WHO THIS IS FOR	Career-changers and complete beginners entering cybersecurity with no prior security background, and IT or helpdesk staff who want a rigorous, hands-on technical baseline before specialising.
PREREQUISITES Entry requirements	None. Basic computer literacy is assumed — you should be comfortable using a laptop and a web browser. No programming, networking or security knowledge is required.
HOW IT IS DELIVERED Format	Instructor-led sessions frame each discipline, then the majority of your hours are spent in self-paced hands-on labs on a live, browser-reachable company network. Roughly half of all contact hours are spent operating real machines rather than reading.
CERTIFICATION HRCF · practical capstone	HRCF is awarded on a hands-on capstone, not a multiple-choice exam: a guided two-sided intrusion on the live range, scored on how cleanly you operate and how completely you document every step.
PROGRESSION Next tracks	SOC Analyst · Penetration Testing

120 h	8	8	50%
TOTAL HOURS	WEEKS	MODULES	ON THE RANGE

CURRICULUM · modules 1–2 of 8

FND-01 Computing & Operating System Fundamentals

12 HOURS

You learn how a computer really works underneath — files, processes, memory and user accounts — by driving a live machine yourself. This gives you the mental model every security task later depends on.

LEARNING OBJECTIVES

- [ ] By the end you can navigate a running operating system to inspect files, processes and user accounts from first principles.
- [ ] By the end you can explain how the CPU, memory and disk cooperate to load and run a program.
- [ ] By the end you can identify which user or process owns a resource and why that ownership matters for security.
- [ ] By the end you can distinguish volatile from persistent state on a live machine.

TOPICS COVERED

- The boot process and the role of the kernel
- Processes, threads and the process tree
- Virtual memory, RAM and paging
- File systems, inodes and file metadata
- User accounts, groups and privilege levels
- Volatile versus persistent state

RANGE LAB

On a live workstation you enumerate running processes, map open files back to their owning process, and trace how an executable is loaded into memory — building the mental model every later attack and investigation relies on.

ASSESSMENT Evidence-based worksheet on the range: you capture and annotate the process tree, memory map and file ownership of a running target, graded on accuracy of interpretation.

FND-02 Networking Essentials

15 HOURS

You follow real traffic across a small network and see how data actually moves between machines, ports and services. By the end you can read an IP address, a port and a packet and say what is happening.

LEARNING OBJECTIVES

- [ ] By the end you can trace a connection through the TCP/IP stack from application down to the wire.
- [ ] By the end you can read an IP address, subnet mask and port number and state what each identifies.
- [ ] By the end you can analyse a packet capture to reconstruct which hosts talked and over which services.
- [ ] By the end you can distinguish normal protocol behaviour from something anomalous.

TOPICS COVERED

- The OSI and TCP/IP models
- IP addressing, subnets and routing basics
- TCP versus UDP and the three-way handshake
- Common ports and the services behind them
- DNS, DHCP and ARP in practice
- Reading packets in Wireshark

RANGE LAB

You capture live traffic on a small range network with Wireshark, follow a TCP stream end to end, and identify the hosts, ports and protocols in play — separating routine chatter from a connection worth questioning.

ASSESSMENT You are handed an unlabelled packet capture on the range and must reconstruct the conversation — hosts, services and intent — graded on the correctness of your written analysis.

CURRICULUM, CONTINUED · modules 3–4 of 8

FND-03 Linux for Security

16 HOURS

You work entirely from the Linux command line to move files, manage permissions and automate tasks with short Bash scripts. This is the daily working environment for almost every security tool you will meet.

LEARNING OBJECTIVES

- [ ] By the end you can operate a Linux host entirely from the command line to navigate, search and manipulate files.
- [ ] By the end you can configure file and directory permissions and reason about who can access what.
- [ ] By the end you can write a short Bash script to automate a repetitive task.
- [ ] By the end you can inspect processes, services and logs on a running Linux system.

TOPICS COVERED

- The Linux file-system hierarchy
- Core commands, pipes and redirection
- Users, groups and permission bits
- Package management and services
- Bash scripting fundamentals
- System and authentication logs

● RANGE LAB

You are dropped onto a headless Linux server on the range and must configure a user, lock down a set of permissions, and write a Bash script that automates a housekeeping task — all from the shell, with no GUI.

ASSESSMENT Timed command-line challenge on a live Linux host, scored on completing a set of administration and scripting tasks and on the correctness of your permission model.

FND-04 Windows for Security

16 HOURS

You drive Windows the way a professional does — through PowerShell, the registry and the event logs rather than the desktop. You learn where Windows records what happened, which matters for both attack and defence.

LEARNING OBJECTIVES

- [ ] By the end you can administer a Windows host from PowerShell rather than the graphical interface.
- [ ] By the end you can navigate the registry and explain how it stores configuration and persistence.
- [ ] By the end you can read Windows event logs to reconstruct what happened on a system.
- [ ] By the end you can locate the artefacts Windows creates when a program runs or a user logs in.

TOPICS COVERED

- PowerShell cmdlets, objects and the pipeline
- The Windows registry structure
- Windows services, tasks and processes
- The Windows event log architecture
- Authentication and logon events
- Where Windows records execution

● RANGE LAB

You investigate a Windows workstation on the range using only PowerShell and the event logs — enumerating services, querying the registry and reconstructing a sequence of logons and program launches from the recorded evidence.

ASSESSMENT You reconstruct a short activity timeline on a live Windows host from its logs and registry, graded on completeness and on correct use of PowerShell to gather the evidence.

CURRICULUM, CONTINUED · modules 5–6 of 8

FND-05 Security Fundamentals & the Threat Landscape

14 HOURS

You learn the core ideas of security — risk, controls and how real attacks unfold — using plain language and current examples. This gives you the vocabulary to talk about threats with any team.

LEARNING OBJECTIVES

- [ ] By the end you can explain the CIA triad and apply it to a real system.
- [ ] By the end you can describe how a typical attack unfolds using the cyber kill chain.
- [ ] By the end you can classify security controls as preventive, detective or corrective.
- [ ] By the end you can reason about a risk in terms of likelihood, impact and mitigation.

TOPICS COVERED

- Confidentiality, integrity and availability
- Threat actors, motivations and capabilities
- The cyber kill chain and attack lifecycle
- Preventive, detective and corrective controls
- Risk, likelihood and impact
- The current threat landscape and common attack types

RANGE LAB

You map a small range environment against the cyber kill chain, identifying where an attacker could act at each stage and which control would catch or block them — producing a plain-language risk view of the estate.

ASSESSMENT You produce a written threat-and-control assessment of a range environment, graded on the soundness of your reasoning about risk and the correctness of your kill-chain mapping.

FND-06 Web & Application Basics

14 HOURS

You take apart how websites and applications work by inspecting requests and responses with Burp Suite. You see where common weaknesses live before you ever try to exploit or defend one.

LEARNING OBJECTIVES

- [ ] By the end you can dissect an HTTP request and response and explain each part.
- [ ] By the end you can use an intercepting proxy to observe and modify web traffic.
- [ ] By the end you can describe how a client, server and database fit together in a web application.
- [ ] By the end you can point to where common web weaknesses tend to live.

TOPICS COVERED

- HTTP methods, headers and status codes
- Cookies, sessions and authentication
- Client-server-database architecture
- Intercepting traffic with Burp Suite
- How forms and parameters reach the server
- An introduction to the OWASP Top 10

RANGE LAB

You proxy a deliberately simple web application on the range through Burp Suite, intercept and alter a request, and map how user input travels from the browser to the server — seeing first-hand where a weakness would sit.

ASSESSMENT You document the request-response flow of a range web application and identify its trust boundaries, graded on the accuracy of your analysis and your correct use of the proxy.

CURRICULUM, CONTINUED · modules 7–8 of 8

FND-07 Offensive vs Defensive Foundations

15 HOURS

You watch the same event from both sides — the attacker's action and the defender's trace of it — on the live range. This shows you why offensive and defensive work are two views of one story.

LEARNING OBJECTIVES

- [ ] By the end you can describe a single attacker action and the defensive evidence it leaves behind.
- [ ] By the end you can adopt an attacker mindset to reason about how a system could be abused.
- [ ] By the end you can adopt a defender viewpoint to reason about what a log would reveal.
- [ ] By the end you can connect an offensive technique to its corresponding detection.

TOPICS COVERED

- The attacker mindset and defender mindset compared
- Mapping attacker actions to the kill chain
- Telemetry: what each action leaves behind
- Indicators of compromise versus indicators of attack
- Detection as the mirror of exploitation
- How red and blue teams collaborate

● RANGE LAB

You run a simple, guided attack against a monitored range host, then switch seats and find your own footprints in the defender's logs — proving that every offensive step is also a detection opportunity.

ASSESSMENT You submit a paired attack-and-detection narrative for the same event on the range, graded on how accurately you connect each offensive action to its defensive trace.

FND-08 Tooling, Lab Discipline & Documentation

18 HOURS

You set up a clean working lab and complete a guided two-sided intrusion, recording every step as you go. The graded capstone scores how well you work and document, not what you memorised.

LEARNING OBJECTIVES

- [ ] By the end you can stand up and organise a clean, repeatable working environment.
- [ ] By the end you can keep contemporaneous notes that let someone else reproduce your work.
- [ ] By the end you can complete a guided two-sided intrusion from both attacker and defender seats.
- [ ] By the end you can assemble your evidence into a coherent write-up.

TOPICS COVERED

- Building and organising a working lab
- Command logging and evidence capture
- Structured note-taking and screenshots
- Reproducibility and chain of work
- Walking a guided intrusion end to end
- Turning notes into a report

● RANGE LAB

The foundation capstone: you configure your lab, then carry a guided intrusion through from initial access to detection on the live range — attacking a target and then finding the evidence — documenting every command and decision as you go.

ASSESSMENT Graded capstone scored on the cleanliness of your operation and the completeness and reproducibility of your documented evidence trail, not on recall.

OUTCOMES & CERTIFICATION

YOU WILL GRADUATE ABLE TO

- [ ] Reason about security at the OS, file-system, process and network level.
- [ ] Operate confidently on the Linux and Windows command lines and script in Bash and PowerShell.
- [ ] Capture and interpret network traffic, and complete a guided two-sided intrusion on a live range.
- [ ] Aligns to CompTIA Security+, Network+ and ISC2 CC.

TOOLS YOU WILL WORK WITH

Wireshark · Kali Linux · PowerShell · Bash · Burp Suite · VirtualBox

PREREQUISITE	None — open enrolment, no prior security knowledge required.
CERTIFICATION	**HRCF** — HackersRange Certified, Foundations, awarded on the practical capstone.
NEXT TRACKS	SOC Analyst · Penetration Testing

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**.