

OSEP — Evasion Techniques & Breaching Defenses Preparation Training

Delivered from Hacky Security's own curriculum, by instructors who also work our security operations centre. Classroom, online live, or at your office.

EXPERT

At a glance

COURSE	OSEP — Evasion Techniques & Breaching Defenses	WHAT IS INCLUDED ✓ Instructor-led delivery by practitioners who also work our SOC ✓ Hands-on lab access for the duration of the course ✓ Course materials and lab guides ✓ Hacky Security certificate of completion ✓ Post-course support by email
TRACK	OffSec	
DOMAIN	Cyber Security	
LEVEL	Expert	
DURATION	On request	
DELIVERY	Classroom · Online live · On-site at your office	
LANGUAGE	English	
CLASS SIZE	Small cohorts — everyone gets lab time	

Who this is for

This is an expert course. It suits people already working in or moving into Cyber Security who want structured, hands-on preparation rather than a video library. If you are unsure whether the level fits your team, send us the job titles and we will tell you honestly — including if a different course would serve you better.

Course outline

About this course map

OSEP is the evasion exam. Where OSCP proves you can break in, OSEP proves you can break in *where someone is watching* — past antivirus, past application whitelisting, past the EDR that is supposed to catch exactly what you are doing. It is the penetration-testing half of OffSec's OSCE³ certification, and it is aimed squarely at the gap between "I got a shell in the lab" and "I got a shell in a hardened enterprise and nobody's console lit up."

The course behind it, PEN-300 (Evasion Techniques and Breaching Defenses), assumes you can already do everything OSCP covers. This preparation programme is built for people who have passed OSCP, or who work as penetration testers already, and now need the tradecraft that keeps an operation quiet. The teaching is lab-heavy and Windows-heavy, because that is where the defences you are evading actually live.

The exam is a 48-hour practical against a hardened Active Directory environment, followed by 24 hours to write the report. There is no multiple choice. You either reached the objective without tripping the defences, or you did not.

Module 01 — Operating inside a mature defence

The mindset shift before any technique. What a modern enterprise actually deploys, and how each control decides whether to flag you.

- The defensive stack you are up against: antivirus, EDR, application control, network monitoring, and how they share signal
- Signature, heuristic and behavioural detection — and why evading one does nothing for the others
- Building a lab that mirrors a defended environment rather than an open one
- The operational cost of noise: why every extra process, file and connection is a risk

Module 02 — Client-side code execution

Getting the first execution when the easy paths are closed, using the formats users open without thinking.

- Weaponising Office documents: VBA macros, and why the naive version is caught instantly
- Staged versus stageless payloads, and the trade-off each makes with detection
- Windows Script Host, JScript and HTA delivery
- Living with Protected View, Mark-of-the-Web and macro-blocking policies

Module 03 — Antivirus evasion

Understanding how AV actually inspects a binary, then defeating each mechanism deliberately rather than by trial and error.

- On-disk versus in-memory scanning, and the Antimalware Scan Interface (AMSI)
- Bypassing AMSI at the PowerShell and .NET layers
- Encoding, encryption and packing — what still works and what is now itself a signature
- Testing evasion safely without burning your payloads to cloud sample-sharing

Module 04 — Application whitelisting

Executing code on a host that only allows approved binaries to run.

- How AppLocker and Windows Defender Application Control make their decisions
- Trusted binaries that run untrusted code — the "living off the land" binaries
- PowerShell Constrained Language Mode and getting out of it
- Enumerating a whitelisting policy before you try to beat it

Module 05 — Bypassing network filtering

Getting your traffic out of an environment that inspects and restricts what leaves it.

- Egress filtering, proxies and how outbound command-and-control is spotted

- DNS, HTTPS and domain-fronting-style channels
- Shaping traffic so it looks like the noise around it
- When to go slow: beaconing intervals and jitter as an evasion control

Module 06 — Process injection and migration

Running your code inside a process that is already trusted, and moving between them without being obvious.

- Classic and modern injection techniques, and which ones EDR now watches for
- Reflective loading and running managed code from memory
- Migrating to blend in, and the telemetry migration itself generates
- Why the textbook technique is often the caught one

Module 07 — Antimalware Scan Interface and PowerShell

The specific, recurring fight with PowerShell in a defended environment.

- How AMSI hooks PowerShell and .NET, in detail
- Patching and bypassing AMSI in memory
- Obfuscation that survives logging and script-block inspection
- Executing without touching disk

Module 08 — Kiosk and application breakouts

Escaping the restricted environment a user is handed, into the operating system underneath.

- Breaking out of locked-down desktops and kiosk applications
- Abusing legitimate application features to reach a shell
- Escalating from a constrained user context

Module 09 — Microsoft SQL attacks

Turning database access into host and domain compromise.

- Enumerating and abusing SQL Server from a foothold
- Command execution through the database
- Linked servers and lateral movement across a SQL estate

Module 10 — Active Directory exploitation and lateral movement

The heart of the exam: moving through a hardened domain quietly and reaching the objective.

- Enumeration that does not light up the defenders
- Credential theft and reuse in an environment that is watching for it
- Kerberos attacks — delegation, ticket abuse — under monitoring
- Lateral movement techniques ranked by how loud each one is
- Domain privilege escalation and reaching the goal without a detection

Module 11 — Combining the tradecraft under exam conditions

The chained operation, start to finish, which is what the exam actually tests.

- Building a full attack path from initial access to objective
- Time and noise management across a 48-hour operation

- Recovering when a technique is caught mid-engagement
- Writing the report: what a client needs to know about how you stayed hidden

Sitting the official exam

Exam voucher sold separately. We buy it from the certification body on your behalf and send you the code — you book your own exam date. This course is Hacky Security's own preparation training. The certification itself is awarded by the certification body, not by us.

Investment

Priced per cohort. Tell us how many people and which delivery mode and we will send a quote the same working day.

Book this course

Tell us how many people, where, and when — we will come back with dates and a quote within one working day.

+91-8091900310 • info@hackysecurity.com

<https://hackysecurity.com/courses/osep/>

CHANDIGARH • SHIMLA • DELHI • DUBAI • LONDON

Independent preparation training delivered from Hacky Security's own curriculum. Hacky Security Private Limited is not affiliated with or endorsed by the certification body named in this document. Certification names and codes are the trademarks of their respective owners and are used only to describe what this course prepares you for. Prices, durations and outlines are indicative and may change; the quotation we send you is the binding one. Issued 19 September 2026.