AMBIENT-IT

+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated on 11/08/2025

Sign up

Red Team Ops (RTO) training

ALL-IN-ONE: EXAM INCLUDED IN PRICE

4 days (28 hours)

Presentation

Red Team Ops (RTO) is an offensive cybersecurity training course dedicated to adversary simulation to assess and improve the resilience of organizations.

This approach goes beyond traditional pentesting to cover the complete engagement cycle: intelligence, initial access, post-exploitation, lateral movement, exfiltration and reporting.

You will practice TTPs of realistic attackers in near-real environments, respecting rigorous OPSEC and rules of engagement.

On completion, you will be able to design, conduct and document an end-to-end Red Team operation, drawing on frameworks such as MITRE ATT&CK and modern C2s.

As with all our training courses, this one will introduce you to the latest update of Red Team Ops .

Objectives

- Conduct a Red Team engagement from planning to reporting
- Implement advanced TTPs (AD, Kerberos, lateral, exfiltration)
- Deploy and operate C2 with OPSEC (network profiles, redirectors)
- Translate results into actionable recommendations and detections

Target audience

- Pentesters and offensive security consultants
- Teams exposed to Red/Purple Team exercises

- Security engineers targeting adversary emulation

Prerequisites

- Knowledge of networks, Windows/AD and pentest tools
- Command-line fluency and virtualized environments
- Notions of OPSEC and offensive ethics

Red Team Ops (RTO) training

Red Team operational framework and methodology

- Differences between Red Team and Pentest, and the role of the Purple Team
- MITRE ATT&CK, Kill Chain, Adversary Emulation frameworks
- Defining mission objectives, ROE and scope
- Governance: ethics, legality, risk management and insurance
- Planning tools: threat profiles, OPSEC and activity logs
- Workshop: building a complete engagement plan

Intelligence and initial access

- Structured OSINT: people, infrastructure, technical footprints
- Targeted phishing, malvertising, watering hole, USB drop (simulation)
- External exploitation: vulnerabilities, credential stuffing, MFA fatigue
- Payload preparation and OPSEC rules (network profile, times, noise)
- Expected detection measures on the defense side (adversary hypotheses)
- Workshop: spearfish phishing campaign with indicators

Command & Control and persistence

- C2 selection (e.g. Cobalt Strike, Sliver) and redirector topologies
- Malleable C2 / network profiles, sleep/jitter, User-Agent & DNS
- Persistence: scheduled tasks, services, WMI, registry, LNK
- C2 OPSEC: traffic shaping, domains, certificates, minimal logs
- Basic evasion: AMSI, ETW, AppLocker, EDR exclusions
- Workshop: deploying an implant and establishing a C2 channel

Initial post-exploitation and elevation of privileges

- Artifact collection: tokens, credentials, cookies, sensitive files
- UAC bypass, local privileges, LSASS (ethics & safe-guards)
- Kerberos techniques (AS-REP roast, kerberoasting) and DPAPI
- Enhanced persistence: scheduled tasks, WMI Event Subscriptions
- OPSEC hygiene: cleaning, living-off-the-land (LOLBAS)
- workshop: controlled local privilege escalation

Active Directory: mapping and attack paths

- AD enumeration and access graphs (e.g. BloodHound)
- Abuse of ACL/ACE, shadow admins, kerberoastable accounts
- Delegations: Unconstrained/Constrained/RBCD
- Movement facilities: WinRM, SMB, PsExec, WMI
- OPSEC preparation: request rates, caches, network footprint
- workshop: exploiting an identified attack path

Controlled lateral movement

- Token impersonation, Pass-the-Hash/Ticket, S4U2Self/Proxy
- RDP/SMB/SSH techniques and pivoting via socks/proxychains
- Lateral evasion: process injection, in-memory
- Reinforce multi-node persistence and fallback points
- Defensive indicators (honey tokens, canaries, traps)
- workshop: scenario for lateral movement to a sensitive account

Advanced operations on Kerberos & Domain Attack

- Silver/Golden Tickets, KRBTGT hygiene, DC Sync
- Shadow Credentials and abuse of enterprise PKI
- NTLM relay and targeted delegation attacks
- OPSEC: timing, jitter, timeboxing, trace coverage
- Examples of IOCs and detection support
- workshop: Kerberos lab (roast ? ticket ? DC Sync)

Exfiltration and target-based actions

- Defining business objectives (BIA, crown jewels)
- Collection: local staging, compression, steganography

- Exfiltration: HTTPS, DoH, SFTP, controlled cloud
- Footprint reduction and DLP/SIEM testing
- Alert thresholds, rate limiting, diversion channels
- workshop: countermeasured exfiltration in the environment

Communication, coordination and operational security

- War-room, out-of-band channels, encrypted logbook
- Incident management (pause/stop/kill-switch)
- Coordination with sponsor and findings management
- Legal hold, evidence retention, confidentiality
- OPSEC assessment and remediation plan
- workshop: crisis exercise and communication

Reporting, storytelling and remediation

- Architecture of a risk-oriented Red Team report
- Narrative: kill chain, business impact, probability & severity
- Recommendations: techniques, processes, prioritization
- Appendices: IOCs, TTPs, artifacts & methodology
- Executive and technical presentation (two levels)
- workshop: drafting of an executive report + appendices

Feedback and defensive hardening

- Purple teaming: transforming TTPs into tests
- Déclinaison detections (SIEM/EDR) and TTP-based hunting
- N1/N2 playbooks, alerting, escalation runbooks
- Continuous simulation & baselining
- Gap mapping and continuous improvement plan
- Workshop: convert 3 TTPs into detection rules

Synthesis and preparation for production launch

- Pre- and post-commitment checklists
- Threat profile models and emulation scenarios
- Toolbox: C2, redirectors, infra as code
- Ethical and legal best practices
- Skills and resources development plan

- workshop: preparation of a reusable engagement kit

Companies concerned

This course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced computer technology, or to acquire specific business knowledge or modern methods.

Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire which enables us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives for the forthcoming course, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

Teaching methods

Practical training: 60% hands-on, 40% theory. Training material distributed in digital format to all participants.

Organization

The course alternates theoretical input from the trainer, supported by examples, with brainstorming sessions and group work.

Validation

At the end of the session, a multiple-choice questionnaire is used to check that skills have been correctly acquired.

Certification

A certificate will be awarded to each trainee who completes the training course.