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 2 certification training

ALL-IN-ONE : EXAM INCLUDED IN PRICE

4 days (28 hours)

Presentation

Red Team Ops 2 (RTO) is an advanced offensive cybersecurity program that immerses you in realistic adversary emulation scenarios, from deploying a Command & Control infrastructure to evading defenses (EDR, WDAC, ASR) and developing customized tools.

You'll learn to operate with rigorous OPSEC, manipulate Windows APIs, perform stealth process injections and produce reports that can be exploited by decision-makers.

At the end of the course, you'll be ready to run an end-to-end Red Team campaign and aim for RTO II certification, on the latest stable release available.

Like all our training courses, this one uses the latest tools and techniques from Zero-Point Security.

Objectives

- Master advanced offensive cybersecurity tactics
- Deploy and secure a C2 infrastructure
- Design and use customized offensive tools
- Bypass modern defenses (EDR, WDAC, ASR)
- Conduct a simulation aligned with MITRE ATT&CK
- Prepare for RTO II certification

Target audience

- Offensive cybersecurity consultants
- Red Team analysts
- Experienced Pentesters
- SOC / Blue Team professionals
- Security experts

Prerequisites

- Previous Red Teaming / pentesting experience
- Operational knowledge of Windows & Active Directory

Red Team Ops 2 certification training program

Advanced foundations & infrastructure

- RTO II objectives and scope; advanced OPSEC posture
- Targeted reminders: adversary emulation, MITRE ATT&CK, kill chain
- Overview of tools: Cobalt Strike, redirectors, malleable profiles
- C2 architecture choices (on?prem / cloud) and resilience models
- Workshop: setting up a basic C2 infrastructure (listener, profile, redirector)

Hardened C2 infrastructure and network camouflage

- Configuring Apache/Nginx redirectors and TLS certificates
- Camouflage by URI, User-Agent, cookies, front-end hosts
- Traffic management (staging/beacon) and IOC rotation
- Minimal logging and OPSEC hygiene
- Workshop: deploying an HTTPS redirector with filtering rules

Windows APIs & offensive development

- C# / C++ interop; Windows API calls, D/Invoke, ordinals
- Injection models (CreateRemoteThread, APC, MapViewOfFile)
- PPID spoofing, command masking, handle management
- Memory cleaning and detection area reduction
- Workshop: coding a simple loader based on WinAPI

Defense evasion

- EDR/AV operation (ETW, user/kernel hooks)
- Memory offuscation, direct/indirect syscalls
- AMSI bypass and beacon hardening
- Controlled tests and noise measurement
- Workshop: evaluating a payload against a lab EDR

ASR & WDAC: understanding and bypassing

- Attack Surface Reduction (ASR) policies: logic, rules, telemetry
- Windows Defender Application Control (WDAC): catalogs, signatures
- LOLBAS abuse, signed hijacking and permissive loading
- Responsible escape scenarios and ethical limits
- Workshop: bypassing a WDAC policy in a simulated environment

Protected processes & Windows hardening

- Protected Processes model and offensive implications
- Constraint code signing, certificates and chains of trust
- Controlled access techniques and conditional execution
- Rollback strategies & clean disengagement
- Workshop: guided analysis of a protected process case study

Integrated attack chain

- End-to-end orchestration: infra, load, pivot, actions
- Artifact management and minimalist logging
- Real-time tactical adaptation
- Preparing a team playbook
- Workshop: controlled intrusion exercise

Adversary emulation & threat intel

- Modeling an adversary with ATT&CK (tactics/techniques)
- Mapping defensive controls and assumptions
- Enter objectives, preconditions and expected outputs
- Measuring impact and coverage
- Workshop: mapping an RTO II scenario on ATT&CK

Red Team executive & technical reporting

- Structure: executive summary, narrative, evidence, recommendations
- Traceability: timelines, captures, indicators, IOCs
- Editorial quality and actionability
- Preparing the presentation and multi-party debriefing
- Workshop: writing a structured mini-report

Preparing for certification

- RTO II test preparation & constraints
- Targeted review: C2, injections, escape, report
- Time and flags management strategy
- Pre-exam checklist
- Workshop: exam-style simulation

Post-simulation analysis & anchoring plan

- Review of successes and areas for improvement
- Consolidation of technical skills
- Progression plan (labs, readings, drills)
- Prepare for progression to related courses
- Workshop: feedback & continuous improvement

Closing & certification

- Valuing skills & deliverables
- Ethics and compliance
- Business projection and monitoring
- Post-certification roadmap
- Workshop: interview simulation & mission pitch

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 enabling 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 issued to each trainee who completes the training course.