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

Updated on 12/08/2025

Sign up

Offensive Development Practitioner Certification

ALL-IN-ONE : EXAM INCLUDED IN PRICE

5 days (35 hours)

Presentation

Offensive Development Practitioner Certification (ODPC) is an advanced offensive development training course designed for professionals wishing to design custom tools and payloads for realistic Red Team operations.

During this program, you'll learn how to manipulate Windows APIs, implement stealth injection techniques and bypass modern defenses such as EDR, AMSI and ETW. You'll also learn how to set up encrypted and discrete C2 communications.

The course covers memory exploitation, advanced persistence, exfiltration and optimizing your tools for stealth and performance, with a strong emphasis on practice in a controlled environment.

At the end of the course, you'll be able to develop, test and document operational offensive tools, and prepare effectively for ODPC certification (daily workshops and mock exam included).

Like all our training courses, this one uses the latest resources from White Knight Labs.

Objectives

- Design customized payloads and loaders
- Master WinAPI, EDR/AMSI/ETW injections and bypasses
- Deploy encrypted and stealthy C2 channels
- Automate post-exploitation and exfiltration

- Produce a professional, actionable report
- Prepare for ODPC certification

Target audience

- Offensive security developers
- Experienced Pentesters
- Red Team analysts
- Automation-oriented security professionals

Prerequisites

- Basic knowledge of C/C++, C#, Python
- Knowledge of pentest/offensive security
- Proficiency in Windows and Linux environments

Offensive Development Practitioner Certification training program

Foundations of offensive development

- Role of the offensive developer, rules of engagement, scope
- OPSEC hygiene applied to code
- Environments and tools
- Local CI and organization
- Workshop: preparing the environment

Languages & Windows API

- C/C++, C#, Python, Go
- Windows API calls, interop
- Memory management, pointers
- I/O, registry, services
- Workshop: WinAPI utility

Payloads & discrete executions

- Stealth executables
- Shellcode encoding, packaging
- Simple persistence
- Signature, trust
- Workshop: basic payloads

Injection & evasion

- CreateRemoteThread, APC, hollowing
- PPID spoofing, handles
- Controlled elevation
- Post-exec cleaning
- Workshop: injection

Bypass EDR/AMSI/ETW

- EDR telemetry
- Bypass AMSI / ETW
- Anti-sandbox/debug
- Measurement & adjustment
- Encrypted loader workshop

C2 channels & communications

- HTTP/HTTPS channel
- Application encryption
- Network profiles & OPSEC
- IOC rotation
- Workshop: minimalist beacon

Automation & operation

- PowerShell / Python scripts
- Modularity, build
- Dynamic generation
- Offensive QA
- Workshop: scripted orchestrator

Exploitation & hooks

- Buffer overflow
- Hooks and API interception
- DLL injection
- Stability & performance
- Workshop: guided operation

Multi-platform

- Cross-compiling Windows/Linux
- Portable libs
- Packaging & distribution
- Compatibility/testing
- Workshop: porting to 2 OS

Post-exploitation & stealth

- Persistence (tasks, services, registry)
- Fileless approaches
- Clean rollback
- Minimal logging
- Workshop: stealth persistence

Exfiltration & staging

- Discrete channels
- Encryption, fragmentation
- Protocol hijacking
- Evidence & time stamping
- Workshop: exfiltration pipeline

Enhancement & quality

- Lab tests
- Stealth optimization
- Hardening
- Good release practices
- Workshop: tool audit

Certification preparation

- ODPC format & criteria
- Time management
- OPSEC checklist
- Deliverables
- Workshop: white session

Targeted review

- WinAPI, injections, EDR bypass
- C2 & exfiltration
- Traps & remedies
- Individual plan
- Workshop: multi-TTP challenge

Simulated passage & final validation

- Exam-style conditions
- Technical objectives

- Professional report
- Feedback & action plan
- Workshop: graded mock exam

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.