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

Updated 04/19/2024

Sign up

OSED™ Certification Training

ALL-IN-ONE: EXAM INCLUDED IN PRICE WITH EXP-301 COURSE

3 days (21 hours)

PRESENTATION

Learning exploit development in Windows user mode is possible with our OSED™ preparation training to teach you the basics of modern exploit development.

During our OSED™ training, you'll perform basic buffer overflow attacks to bypass the critical security mitigation measures that protect businesses. An excellent way to prevent vulnerabilities present in a computer system.

You'll be challenged to write Windows shellcode by hand. What's more, you'll also be asked to design custom exploits.

You'll need to learn all the fundamentals of reverse engineering, so that you'll be able to adapt older techniques to more modern versions of Windows.

After completing our preparation, you'll be eligible to pass OSED™ certification.

OBJECTIVES

- Develop the skills needed to circumvent security mitigation measures
- Write your own shellcode
- How to use WinDbg
- Learn the fundamentals of reverse engineering
- OffSec Exploit Developer (OSED) certification

TARGET AUDIENCE

- Web intrusion testers
- Safety researchers
- Developers
- Analysts

Prerequisites

- Familiarity with debuggers (ImmunityDBG, OllyDBG)
- Familiarity with basic 32-bit operating concepts
- Familiarity with writing Python 3 code
- Ability to read and understand C code at a basic level
- Ability to read and understand 32-bit Assembly code at a basic level

Software requirements

- **Kali Linux** --> Download here

Note: Ambient IT does not own OSED™, this certification belongs to OffSec ® Services LLC.

OSED™ CERTIFICATION TRAINING PROGRAM

User-mode exploit development

- About the EXP-301 course
- Discover general strategies for dealing with EXP-301
- Definition of examination details
- Summary

WinDbg and x86 architecture

- Introduction to x86 architecture
- Introduction to the Windows debugger
- Accessing and manipulating memory from WinDbg
- Control program execution in WinDbg
- Additional features

Exploiting pile overflows

- Introduction to stack overflow
- Installing the Sync Breeze Crash application
- Sync Breeze application crash
- Exploiting a Win32 buffer overflow

SEH overflow exploitation

- Sync Breeze crash
- Crash analysis in WinDbg
- Introduction to structured exception management
- Structured exception handler overflows

Introduction to IDA Pro

- IDA Pro 101
- Working with IDA Pro Wrapp

Overcoming space restrictions: Egghunters

- Web server crash
- Analyzing crashes in WinDbg
- Detecting bad characters
- Get code execution
- Storing large pads
- Find your stamp: Egghunters approach
- Improving Egghunter portability
- Improve SEH

Creating custom Shellcode

- Calling conventions on x86
- System call problem
- Find kernel32.dll
- Solving symbols
- NULLFree Position-Independent Shellcode (PIC)
- Reverse Shell

Reverse engineering of bugs

- Installation and enumeration
- Interaction with Tivoli Storage Manager
- Protocol reverse-engineering
- Find more bugs

Stack overruns and bypassing the PED

- Data execution prevention
- Return-oriented programming
- Selection of gadgets
- DEP bypass

Stack overruns and ASLR bypass

- Introduction to ASLR
- Searching for hidden gems
- Developing our exploit
- Bypassing ASLR
- DEP bypass with WriteProcessMemory

Companies concerned

This training 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 training to come, 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 course: 60% Practical, 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 verifies the correct acquisition of skills.

Sanction

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