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

Updated 04/26/2024

Sign up

Training and preparation for OSEE™ Certification (EXP-401)

ALL-IN-ONE: EXAM INCLUDED IN PRICE WITH EXP-401 COURSE

5 days (35 hours)

PRESENTATION

Offensive Security Exploitation Expert (OSEE) certification is a crucial milestone in demonstrating your expertise in offensive exploitation and system security.

It testifies to your ability to identify, exploit and secure vulnerabilities in IT systems, as well as to develop effective exploits for any loopholes discovered.

The OSEE™ exam comprises several modules covering a wide range of topics, including.
:

- Creating custom shellcode
- VMware Workstation host-to-guest escape
- Advanced operation of Windows systems
- Analysis of type confusion in browsers
- Overwriting pilot recalls

Each module tests your knowledge and skills in specific areas of offensive operation and system security.

Our OSEE™ training offers comprehensive exam preparation, providing in-depth educational content and practical exercises to reinforce your understanding of the concepts.

We cover every aspect of the certification program, focusing on practical skills and industry best practices.

OSEE™ training is constantly updated to reflect the latest trends and developments in OffSec IT security.

OBJECTIVES

- Master the creation of custom shellcode for various architectures
- Acquire the skills needed to evade VMware Workstation security mechanisms
- Develop advanced Windows operating techniques
- Understanding and exploiting type confusion vulnerabilities in browsers
- Practicing pilot abseiling for privilege climbing

TARGET AUDIENCE

- Pentesters
- Safety researchers
- Analysts SOC

Prerequisites

- Previous experience in offensive operations or systems security
- Advanced knowledge of Windows and Linux operating systems
- Familiarity with common IT security tools
- Understanding of the basic concepts of reverse engineering and malware analysis

Technical requirements

- **Kali Linux** --> Download here
- A computer capable of running three virtual machines with ease
- VMware Workstation 15 or higher
- 64-bit processor with a minimum of 4 cores and support for NX, SMEP, VT-d/IOMMU and VT-x/EPT
- At least 160 GB of available hard disk space
- At least 16 GB RAM
- The only host operating system supported is Windows 10

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

OUR OSEE™ CERTIFICATION TRAINING PROGRAM

Introduction

- General introduction to the course
- Context and importance of custom shellcode creation
- Overview of exploitation techniques and vulnerabilities addressed
- Summary of prerequisite skills
- Training program presentation
- Learning objectives
- Training methodology

Custom Shellcode Creation

- 64-bit architecture and memory improvements
- Conventions for calling and using Win32 APIs
- Writing advanced operating code
- Position-independent shellcode creation techniques
- Using Visual Studio to develop exploits
- Creating a shellcode framework
- Case study : Reverse Shell

VMware Workstation Guest-To-Host Escape

- Vulnerability classes and introduction to data execution prevention (DEP)
- Advanced operating techniques :
  - Ret2Lib
  - ROP
  - Gadget location
- Address space randomization strategies (ASLR)
- Understanding the inner workings of VMware Workstation
- Case study: UaF vulnerability in VMware Workstation
- Analysis of UaF vulnerability case studies
- Bypassing advanced security protections

Advanced Windows Exploitation

- The inner workings of the Windows heap memory manager
- Case study: Triggering and in-depth analysis of UaF vulnerabilities
- Advanced operating techniques: Bypassing ASLR and DEP
- Analysis of UaF vulnerability case studies
- Strategies for restoring runtime flow after successful operation
- Using and executing shellcode in Windows environments
- Evaluation of advanced security protection provided by Windows Defender Exploit Guard (WDEG)

Microsoft Edge Type Confusion

- Analysis of the internal mechanisms of the Microsoft Edge browser
- Case study: Exploiting type confusion
- Advanced operating techniques: Bypassing CFG and ACG

- Analysis of Confusion vulnerability case studies
- Exploit remote procedure calls (RPC) and buffer analyses
- Bypassing security protections in a sandboxed browser environment
- Revision of techniques to make exploits version-independent

Driver Callback Overwrite

- Introduction to the Windows kernel and privilege levels
- Kernel-mode debugging techniques on Windows
- Interaction with the Windows kernel through native system calls and device drivers
- Kernel-mode vulnerability analysis and exploitation techniques
- Exploiting driver callbacks and controlling execution flow
- Methods for achieving operating system version independence
- Conclusion and review of acquired skills

Unsanitized User-mode Callback

- Creating Windows desktop applications and managing kernel pool memory
- Analysis of TagWND objects and callbacks in user mode
- Advanced exploitation techniques: Arbitrary memory overwriting and privilege escalation
- Case study analysis of callback operation in user mode
- Exploiting read/write primitives in the kernel
- Techniques for restoring execution flow after a successful operation
- Methods for making exploits version-independent

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.