EXP-301

Windows User Mode Exploit Development

OFFENSIVE security

ABOUT THE COURSE

Windows User Mode Exploit Development (EXP-301) is an intermediate-level course which teaches students the fundamentals of modern exploit development.

It starts with basic buffer overflow attacks and builds into learning the skills needed to crack the critical security mitigations protecting enterprises.

Those who complete the course and pass the 48-hour exam earn the **Offensive Security Exploit Developer (OSED) certification.**

COURSE TOPICS

Topics include:

- Exploiting SEH overflows
- Overcoming space restrictions: Egghunters
- Shellcode from scratch
- Reverse-engineering bugs
- Stack overflows and DEP/ASLR bypass
- Format string specifier attacks
- Custom ROP chains and ROP payload decoders

OFFENSIVE® security

THE STUDENT EXPERIENCE

Ronald Ocubillo | OSCP, OSCE^3, CRTO

w00tw00t!! I've almost lost my own sanity at this until I popped that shell which barely passed the exam. **It was so tough that you have to combine everything that has been taught on the course: stack/SEH overflow, reverse engineering, custom shellcode, egghunter, ASLR/DEP bypass, and custom ROP chain.**

Overall, that was a hell of a challenge that kept me awake for 48 hours with almost no sleep but it's all worth it. Thank you Offensive Security and I'll be seeing you again for the next couple of weeks for the OSEP exam.

Jorge Giménez Duro | Ethical Hacker at Security Research Labs

Finally OSED! After 36 hours of no sleep I finally succeed. This is, by far, the most challenging (and fun) exam of Offensive Security I have done so far, but It was worth the time; **the content is extremely well structured** :)

OSED + OSWE + OSEP = OSCE^3

Eugene Lim | Cybersecurity Specialist

I'm delighted to pass the Offensive Security Exploit Development course, and in so doing, achieved the Offensive Security Certified Expert (OSCE3)! OSCE3 holders must have passed all three of Offensive Security's 300-level courses: Windows User Mode Exploit Development (EXP-301), Evasion Techniques and Breaching Defenses (PEN-300), and Advanced Web Attacks and Exploitation (WEB-300).

This was the hardest exam I've taken so far. **It was truly a beast of a challenge but it demonstrated all the hallmarks of the OffSec "try harder" rigour.** On to the next!

OFFENSIVE security

THE OFFSEC TRAINING LIBRARY

Learn One

Ready to enroll? Enjoy more flexibility and go at your own pace with a **Learn One** subscription.

A subscription includes an entire year of access to the course lab and Proving Grounds Practice.

Learn One also includes:

- **2 exam attempts**
- New content, added monthly
- Access to OffSec Wireless Attacks (PEN-210)
- Access to Kali Linux Certified Professional

OFFENSIVE® security