Lumify Work EXP-301 Windows Exploit Development Instruction Manual

Home » Lumify Work » Lumify Work EXP-301 Windows Exploit Development Instruction Manual

CYBER SECURITY
EXP-301 – Windows User Mode Exploit Development (OSED) – Self-paced

Contents

EXP-301 Windows Exploit Development

INCLUSIONS	LENGTH	PRICE (Incl.
OSED exam	90 days access	

OFFSEC AT LUMIFY WORK
Security professionals from top organisations rely on OffSec to train and certify their personnel. Lumify Work is an Official Training Partner for OffSec.

OffSec™ Partner | Gold Channel

WHY STUDY THIS COURSE

Learn the fundamentals of modern 32-bit exploit development with this intermediate-level Windows User Mode Exploit Development (EXP-301) course, designed for those who want to learn about exploit development skills.
EXP-301 expands on many of the concepts covered in CT P, and prepares students to take on AWE and the OSEE. EXP-301 is an intermediate course that teaches the skills necessary to bypass DEP and ASLR security mitigations, create advanced custom ROP chains, reverse-engineer a network protocol and even create read and write primitives by exploiting format string specifiers.
Students who complete the course and pass the exam earn the OffSec Exploit Developer (OSED) certification, demonstrating their ability to create custom exploits.
T he OSED is one of three certifications making up the OSCE³ certification, along with the **OSWE** for web application security and the **OSEP** for advanced penetration testing.
T his self-paced course includes:

- 15+ hours of video
- 600+ page course guide
- Active student forums
- Access to virtual lab environment
- OSED exam voucher

“ My instructor was great being able to put scenarios into real world instances that related to my specific situation.
I was made to feel welcome from the moment I arrived and the ability to sit as a group outside the classroom to discuss our situations and our goals was extremely valuable.
I learnt a lot and felt it was important that my goals by attending this course were met.
Great job Lumify Work team.
AMANDA NICOL
IT SUPPORT SERVICES MANAGER – HEALT H WORLD LIMIT ED
Introducing Windows User Mode Exploit Development About the OSED exam:

- T he EXP-301 course and online lab prepares you for the OSED certification
- 4 8-hour exam
- Proctored

Learn more about the exam.

WHAT YOU’LL LEARN

- Learn the fundamentals of reverse engineering
- Create custom exploits
- Develop the skills to bypass security mitigations
- Write handmade Windows shellcode
- Adapt older techniques to more modern versions of Windows

Lumify Work Customised Training

We can also deliver and customise this training course for larger groups saving your organisation time, money and resources.
For more information, please contact us on 1 800 853 276.

COURSE SUBJECTS

The course covers the following topics:

- WinDbg tutorial
- Stack buffer overflows
- Exploiting SEH overflows
- Intro to IDA Pro
- 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

View the full syllabus **here**.

WHO IS THE COURSE FOR?

Job roles such as penetration testers, exploit developers, security researchers, malware analysts, and software developers working on security products, could benefit from this course.

PREREQUISITES

All students are required to have:

- Familiarity with debuggers (ImmunityDBG, OllyDBG)
- Familiarity with basic exploitation concepts on 32-bit
- Familiarity with writing Python 3 code

  The following are optional but recommended:
- Ability to read and understand C code at a basic level
- Ability to read and understand 32-bit Assembly code at a basic level

https://www.lumifywork.com/en-au/courses/exp-301-windows-user-mode-exploit-development-osed-self-paced/

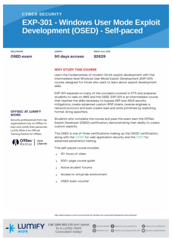
twitter.com/LumifyWorkAU

lumifywork.com

linkedin.com/company/lumify-work

youtube.com/@lumifywork

Documents / Resources

 CYBER SECURITY EXP-301 - Windows User Mode Exploit Development (OSED) - Self-paced INCLUSIONS OSED exam LENGTH 90 days access PRICE (incl. GST) $2629 WHY STUDY THIS COURSE Learn the fundamentals of modern 32-bit exploit development with this intermediate-level Windows User Mode Exploit Development (EXP-301) course, designed for those who want to learn about exploit development skills. EXP-301 expands on many of the concepts covered in CTP, and prepares students to take on AWE and the OSEE. EXP-301 is an intermediate course that teaches the skills necessary to bypass DEP and ASLR security mitigations, create advanced custom ROP chains, reverse-engineer a network protocol and even create read and write primitives by exploiting format string specifiers. Students who complete the course and pass the exam earn the OffSec Exploit Developer (OSED) certification, demonstrating their ability to create custom exploits. The OSED is one of three certifications making up the OSCE³ certification, along with the OSWE for web application security and the OSEP for advanced penetration testing. This self-paced course includes: • 15+ hours of video • 600+ page course guide • Active student forums • Access to virtual lab environment • OSED exam voucher OFFSEC AT LUMIFY WORK Security professionals from top organisations rely on OffSec to train and certify their personnel. Lumify Work is an Official Training Partner for OffSec. OffSec Partner | Gold Channel https://www.lumifywork.com/en-au/courses/exp-301-windows-user-mode-exploit-development-osed-self-paced/ LUMIFY work Call 1800 853 276 and speak to a Lumify Work Consultant today! [email protected] facebook.com/LumifyWorkAU twitter.com/LumifyWorkAU lumifywork.com linkedin.com/company/lumify-work youtube.com/@lumifywork	Lumify Work EXP-301 Windows Exploit Development [pdf] Instruction Manual EXP-301 Windows Exploit Development, EXP-301, Windows Exploit Development, Exploit Development, Development

References

- Lumify Work \| Lumify Work AU
- Lumify Work \| Lumify Work AU
- EXP-301 - Windows User Mode Exploit Development (OSED) - Self-paced \| Lumify Work AU
- PEN-300 - Evasion Techniques and Breaching Defenses (OSEP) - Self-paced \| Lumify Work AU
- WEB-300 - Advanced Web Attacks and Exploitation (OSWE) - Self-paced \| Lumify Work AU
- User Manual