EXP-401:

Advanced Windows Exploitation

THE MOST RIGOROUS IN-PERSON EXPLOIT DEVELOPMENT COURSE

EXP-401: Advanced Windows Exploitation is OffSec's most intense course, featuring a sophisticated hands-on computer lab environment challenging learners to bring out their best penetration testing skills.

Modern exploits for Windows-based platforms require modern bypass methods to circumvent Microsoft's defenses. In EXP-401, OffSec challenges learners to develop creative solutions that work in today's increasingly difficult exploitation environment.

The case studies in AWE are large, well-known applications that are widely deployed in enterprise networks. The course dives deep into topics ranging from security mitigation bypass techniques to complex heap manipulations and 64-bit kernel exploitation.

EXP-401 is a particularly demanding penetration testing course. It requires a significant amount of learner-instructor interaction. Therefore, we limit these courses to a live, hands-on environment at one of our live training at the Black Hat conference.

This course can qualify learners for 40 $(ISC)^2$ CPE Credits at the end of the training course or after passing the certification challenge.

Learners who complete EXP-401 and pass the exam will earn the **Offensive Security Exploitation Expert (OSEE) certification**.

BENEFITS:

- Put your team's skills to the test with intense in-person training
- Enrich your team's penetration testing learning journey with advanced exploit development skills
- Improve your team's preparedness for the OSEE certification exam
- Benchmark your team's skill level for increased confidence around securing your IT infrastructure through industry-recognized certifications

LEARN:

- Bypass and evasion of user mode security mitigations such as DEP, ASLR, CFG, ACG and CET
- Advanced heap manipulations to obtain code execution along with guest-to-host and sandbox escapes
- Disarming WDEG mitigations and creating version independence for weaponization
- 64-Bit Windows Kernel Driver reverse engineering and vulnerability discovery
- Bypass of kernel mode security mitigations such as kASLR, NX, SMEP, SMAP, kCFG and HVCI

OffSec™ Partner Program