EXP-401

ADVANCED WINDOWS EXPLOITATION

The Most Difficult Exploit Development Course

Advanced Windows Exploitation (AWE) is our most demanding Offensive Security Course, featuring a sophisticated hands-on computer lab environment challenging you to bring out your best penetration testing skills.

Modern exploits for Windows-based platforms require modern bypass methods to circumvent Microsoft's defenses. In Advanced Windows Exploitation (EXP-401), OffSec challenges students 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 precision heap spraying to DEP and ASLR bypass techniques to 64-bit kernel exploitation.

AWE is a particularly demanding penetration testing course. It requires a significant amount of student-instructor interaction. Therefore, we limit AWE courses to a live, hands-on environment at Black Hat USA in Las Vegas, NV.

BENEFITS:

- Analyze vulnerable software
- Find problematic code
- Develop a functioning exploit for various modern Windows operating systems.

LEARN:

- NX/ASLR Bypass
- Function pointer overwrites
- Precision Heap Spraying
- Disarming EMET Mitigations to gain reliable code execution
- 64 and 32 Bit Windows Kernel Driver Exploitation
- Kernel Pool Exploitation

OFFENSIVE® security | QA

Learn more at
offensive-security.com