InfoSect

ABN: 59615281706
2/9 Beaconsfield
Fyshwick, 2609, ACT
Australia
courses@infosectcbr.com.au

Exploit Development

In this 5 day course, students will learn how to exploit 32-bit stack-based buffer overflows in Linux and Windows applications without the presence of strong mitigations.

Specifically, students will:

1. Learn about the process of vulnerability discovery.
2. Learn how to develop x86 assembly and shellcode.
3. Learn how the stack works on the x86 architecture.
4. Exploit classic stack-based buffer overflows on Linux and Windows.
5. Exploit Linux stack-based buffer overflows on NX/DEP using ret2libc techniques.
6. Defeat ASLR on Linux.
7. Exploit Windows stack-based buffer overflows using SEH.
8. Defeat NX/DEP using ROP on Linux and Windows.
9. Use Windows and Linux debuggers including GDB and Immunity.

Prerequisites: Proficiency in general programming. Some competency in Python.
Format: Lectures and Labs.
Time: 9am – 5pm.
Duration: 5 days.
Catering: Provided.
Cost: $4000 (inc GST).