UNSW CANBERRA | Cyber

Introduction to Exploit Development

Location	UNSW Canberra
Duration	5 days
Standard Price	$4,550.00
Defence Price	$4,095.00

Description

This course will introduce students to the art and science of exploit development. Core concepts involving debuggers, stack based overflows, disassemblers and some defence mitigation will be taught in a largely practical delivery style. Instruction will commence with an overview of foundational theory concepts, and will then quickly dive into the intricacies of modern x86 CPUs. Mitigations such as DEP and ASLR will be investigated, and students will have the opportunity to demonstrate their new skills in an extended capstone exercise on the final day.

Topics covered include:

- Core exploitation theory
- Stack based overflows on Linux and Windows
- Heap overflows (limited scope)
- Tool use
- Shellcode generation and modification
- Introduction to mitigations
- Mitigation bypass (limited scope)
- Capstone practical exercise

*Note: this course is a foundational course and will not teach 64 bit exploitation or advanced protection bypass techniques.

Learning Outcomes

On completion of this course, participants should be able to:

- Develop and implement basic exploitation strategies.
- Exploit stack-based overflows in Windows and Linux in the absence of strong mitigation controls.
- Use Structured Exception Handling (SEH) to exploit Windows stack-based overflows.
- Write basic ROP exploits to bypass DEP.
- Use tools such as gdb, Immunity Debugger, IDAPro, objdump, readelf, to perform static and dynamic analysis of simple binaries.

Who Should Attend

- Novice exploit developers
- Penetration testers
- Software architects

NICE Framework mapping

This course maps to the highlighted work categories:

Securely Provision | Oversee & Govern | **Analyse** | **Investigate**

Operate & Maintain | **Protect & Defend** | **Collect & Operate**

To find out more about the NICE Framework go to: niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework

Course Day Breakdown

Day 1

Core Exploitation Theory

The session starts with an overview of the history of models of computation and the different types of CPU architecture. We'll then move onto Program Representation and The Stack. Shellcoding Tips and exercises will be covered during the lab session.

Topics

Turing Model of Computation, x64/x86 Architectures, Compilation/Decompilation, Endianess, Stack Frames, Calling Conventions.

Day 2

Stack based Overflows on Linux and Windows

Day 2 covers Buffer Overflows for Linux and Windows environments. We'll then move onto executable binary formats, sharing code, linking shared libraries and stack cookies through lecture and lab components.

Topics

Executable Formats, Memory Layout, Buffer Overflows, Shellcoding – Bad Characters, Exploiting GOT, RELRO, Stack Cookies.

Day 3

Introduction to Mitigations

The session will introduce the concepts of Structured Exception Handling (SEH), Data Execution Prevention (DEP) and Return Oriented Programming (ROP). Labs will cover writing remote exploits using SEH and enabling DEP as a mitigation defeated with ROP.

Topics

SEH Exploitation, Mitigations, Protections, Return-to-libc, ROP Gadgets, ROP Chain.

Day 4 & Day 5

ASLR & Heap Overflows

Today's session lectures will discuss Address Space Layout Randomisation and heap Overflows. Students will run through a number of practical exercises including forcing and leveraging an info leak, understanding Heap Chunks, Allocations and writing exploits to learn more about Heap and how to control it.

Topics

ASLR, Heap Overflows, ASLR Bypasses, Non-rebased Modules, Info Leak, Stack Characteristics, Heap Characteristics, Operations, Management, Fragmentation, Managers and Integrity.

"Well-structured with great analogies and explanations of complex topics."

Course participant

UNSW Canberra Cyber

UNSW Canberra Cyber is a unique, cutting-edge, interdisciplinary research and teaching centre, working to develop the next generation of cyber security experts and leaders. The centre is based in Canberra at the Australian Defence Force Academy and provides professional, undergraduate and post graduate education in cyber security. Our air-gapped, state of the art cyber range offers a secure environment where we deliver a number of technical and highly specialised learning opportunities. Our courses are designed to give the next generation of cyber security professionals the skill sets needed to thrive in the industry. We can also create bespoke professional education programs tailored to your organisation's needs. Contact us at cyber@adfa.edu.au to discuss how.

Find out more

cyber@adfa.edu.au

unsw.adfa.edu.au/cyber