UNSW CANBERRA | Cyber

Reverse Engineering

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

Description

In this short course students will learn how malware interacts with the underlying Operating System, how to go about identifying the functionality of malware, and how to perform large scale data analysis of malware. The course is an even mix of set lectures and laboratory work. In the laboratories students will use tools to apply the concepts of static and dynamic analysis, data analytics, and manual reverse engineering.

Over the course students will come to understand:

- The underlying Operating System
- Object file formats and their use as containers of object code
- How malware tries to evade analysis and detection
- How malware obfuscates analysis by the use of code packing
- Anti-emulation, anti-debugging, anti-VM, anti-sandbox, and anti-disassembly tricks that malware uses
- How dynamic analysis can analyse malware
- The process of static disassembly and decompilation
- How to identify similar malware through the use of program similarity
- How to classify programs as malicious using machine learning

Learning Outcomes

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

- Conduct the main approaches to analysing malware, including static and dynamic analysis.
- Conduct malware analysis automation including malware variant detection and malware classification.
- Discuss program analysis, including program representation and static program analysis.
- Conduct static reverse engineering including the ability to transform disassembly into descriptions of program functionality.

Who Should Attend

Reverse engineers, malware analysts, anti-malware engineers, tool writers for malware analysis.

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

Malware Fundamentals

The session starts with an overview of the history of malware, the motivations behind malware attacks and the different types of malware programs. We will then look at how malware is delivered to the victim and analyse common attacks used to propagate malware.

Topics

Malicious Actions, Malware Delivery and Exploitation, Malware C2, Persistence and Evading Detection, Side Channel Attacks and Jumping Airgaps, Reverse Engineering Firmware and Embedded Devices, Interfacing with UART.

Day 2

Reverse Engineering Malicious Code

Day 2 begins with an introduction to object file formats, common properties of object files, recognising object file formats and how malware modifies object files. We will then discuss the role of the operating system in executing programs, linking and loading processes and look at machine models and commonalties between Instruction Set Architectures.

Topics

Object File Formats – ELF, PE & Java CLASS, Linking and Loading, Object Code and Instruction Set Architectures, Debuggers.

Day 3

Malware Analysis

We will cover the different types of program representation and basic program analysis techniques including binary, data flow, optimisation, program, static and dynamic analysis. The role of automation and machine learning in the identification and prevention of malware attacks will also be discussed.

Topics

Program Representation, Dynamic Analysis, Program Analysis, Binary Program Analysis, Static Reverse Engineering.

Day 4 & Day 5

Malware Classification & Analysis Labs

The session will give an overview of malware detection and how to identify the origin of outbreaks. We will cover how statistical machine learning enables us to learn what malicious behaviour looks like and how benign or malicious behaviour is classified.

Topics

Program Similarity, Program Classification and Clustering, Malware Obfuscation and Evasion, Code Packing Transformations and Unpacking, Malware Classification Using Weka.

“The content was very high level and provided an in-depth look at malware.”

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