UNSW Course Outline

ZEIT8042 Introduction to Exploit Development - 2024

Published on the 27 Jun 2024

General Course Information

Course Code : ZEIT8042
Year : 2024
Term : Semester 2
Teaching Period : Z2
Is a multi-term course? : No
Faculty : UNSW Canberra
Academic Unit : School of Systems and Computing
Delivery Mode : Online
Delivery Format : Standard
Delivery Location : UNSW Canberra at ADFA
Campus : UNSW Canberra
Study Level : Postgraduate
Units of Credit : 6

Useful Links

Handbook Class Timetable

Course Details & Outcomes

Course Description

This course is designed to provide technically competent IT professionals with an accelerated introduction to exploit development in the modern environment. Starting with a theoretical overview of CPU technology and exploit development core concepts, the course quickly moves

into practical exercises to reinforce the key learning outcomes. By the end of the course, students will be able to formulate advanced exploitation strategies and begin to understand the core theory concepts which underpin the art and science of modern exploit development. This theoretical understanding will be reinforced with additional consolidation practical exercises and assessment.

Course Aims

This course is designed to provide technically competent IT professionals with an accelerated introduction to exploit development in the modern environment. Starting with a theoretical overview of CPU technology and exploit development core concepts, the course quickly moves into practical exercises to reinforce the key learning outcomes. By the end of the course, students will be able to formulate advanced exploitation strategies and begin to understand the core theory concepts which underpin the art and science of modern exploit development. This theoretical understanding will be reinforced with additional consolidation practical exercises and assessment.

into practical exercises to reinforce the key learning outcomes. By the end of the course, students will be able to formulate advanced exploitation strategies and begin to understand the core theory concepts which underpin the art and science of modern exploit development. This theoretical understanding will be reinforced with additional consolidation practical exercises and assessment.

Course Learning Outcomes

Course Learning Outcomes
CLO1 : Develop and implement exploitation strategies for use on endpoints.
CLO2 : Bypass modern exploit mitigation controls.
CLO3 : Understand modern vulnerabilities at a technical level.
CLO4 : Identify vulnerable coding structures by examining source and compiled code;
CLO5 : Analyse vulnerabilities and exploits through the proficient use of industry standard tools, and report on impact, mitigation effectiveness and root cause.
CLO6 : Understand the inter-related nature of exploit mitigation controls in a modern endpoint and be able to identify weak points in the overall system of mitigations.

Course Learning Outcomes	Assessment Item
CLO1 : Develop and implement exploitation strategies for use on endpoints.	• Assessment 3: Technical Report • Assessment 2: Major Exploitation Task • Assessment 1: Quiz and Report
CLO2 : Bypass modern exploit mitigation controls.	• Assessment 4: Major Essay • Assessment 3: Technical Report • Assessment 2: Major Exploitation Task • Assessment 1: Quiz and Report
CLO3 : Understand modern vulnerabilities at a technical level.	• Assessment 4: Major Essay • Assessment 3: Technical Report • Assessment 2: Major Exploitation Task
CLO4 : Identify vulnerable coding structures by examining source and compiled code;	• Assessment 1: Quiz and Report • Assessment 3: Technical Report
CLO5 : Analyse vulnerabilities and exploits through the proficient use of industry standard tools, and report on impact, mitigation effectiveness and root cause.	• Assessment 4: Major Essay • Assessment 2: Major Exploitation Task • Assessment 3: Technical Report
CLO6 : Understand the inter-related nature of exploit mitigation controls in a modern endpoint and be able to identify weak points in the overall system of mitigations.	• Assessment 4: Major Essay • Assessment 2: Major Exploitation Task • Assessment 3: Technical Report

Learning and Teaching Technologies

Moodle - Learning Management System

Assessments

Assessment Structure

Assessment Item	Weight	Relevant Dates
Assessment 3: Technical Report Assessment Format: Individual Short Extension: Yes (1 day)	30%	
Assessment 2: Major Exploitation Task Assessment Format: Individual Short Extension: Yes (1 day)	30%	
Assessment 4: Major Essay Assessment Format: Individual Short Extension: Yes (1 day)	30%	
Assessment 1: Quiz and Report Assessment Format: Individual	10%	

Assessment Details

Assessment 3: Technical Report

Assessment Overview

Assessment 3: Technical Report

- Length not to exceed 2500 words.
- Students are to given a recent CVE which allows remote code execution.
- Prepare a technical report on the CVE, including:
  - Nature of vulnerability;
  - Trigger conditions;
  - Success of mitigation strategies;
  - Exploitability assessment;
  - Root cause analysis;
  - Analysis of exploitation pathways;
  - Recommendations for technical mitigations
  - Threat intelligence on current use of this CVE in malicious campaigns.
- Students may submit code samples in an appendix to their report in excess of the word limit without penalty.
- Marking criteria: 1) completeness, 2) quality of analysis, and 3) quality of report.

Course Learning Outcomes

- CLO1 : Develop and implement exploitation strategies for use on endpoints.
- CLO2 : Bypass modern exploit mitigation controls.
- CLO3 : Understand modern vulnerabilities at a technical level.
- CLO4 : Identify vulnerable coding structures by examining source and compiled code;
- CLO5 : Analyse vulnerabilities and exploits through the proficient use of industry standard

tools, and report on impact, mitigation effectiveness and root cause.
- CLO6 : Understand the inter-related nature of exploit mitigation controls in a modern endpoint and be able to identify weak points in the overall system of mitigations.

Assessment 2: Major Exploitation Task

Assessment Overview

Assessment 2: Major Exploitation Task

- Students are to write a non-trivially vulnerable program and then exploit it, demonstrating bypass techniques for at least 1 security control.
- Submission format is a narrated for the exploit and the source code for the vulnerable program.
- Marking criteria: Marks will be awarded for successful exploitation and bypass techniques, but also for the difficulty of the program.

If students choose to write a trivially exploitable program, then marks will be scaled down accordingly. Similarly, setting the bar too high and failing to exploit a locked-down binary will also result in loss of marks.

Course Learning Outcomes

- CLO1 : Develop and implement exploitation strategies for use on endpoints.
- CLO2 : Bypass modern exploit mitigation controls.
- CLO3 : Understand modern vulnerabilities at a technical level.
- CLO5 : Analyse vulnerabilities and exploits through the proficient use of industry standard tools, and report on impact, mitigation effectiveness and root cause.
- CLO6 : Understand the inter-related nature of exploit mitigation controls in a modern endpoint and be able to identify weak points in the overall system of mitigations.

Assessment 4: Major Essay

Assessment Overview

Assessment 4: Major Essay

- Length not to exceed 2500 words.
- Students are to examine the effectiveness of a modern exploit mitigation control at a technical level, specifically addressing current academic

and industry literature pertaining to the strengths and weaknesses of the control.

- Marking criteria: 1) research breadth and depth, 2) structure and coherence, 3) creativity and originality, and 4) accuracy and completeness

Course Learning Outcomes

- CLO2 : Bypass modern exploit mitigation controls.

- CLO3 : Understand modern vulnerabilities at a technical level.
- CLO5 : Analyse vulnerabilities and exploits through the proficient use of industry standard tools, and report on impact, mitigation effectiveness and root cause.
- CLO6 : Understand the inter-related nature of exploit mitigation controls in a modern endpoint and be able to identify weak points in the overall system of mitigations.

Assessment 1: Quiz and Report

Assessment Overview

Assessment 1 – Part A: Stack Overflow Theoretical Exploitation Task

- Students will be given **one hour** to complete a theoretical task.
- The examination will be based on the covered lectures' and labs' content.
- Marking criteria: 1) completeness, 2) structure and coherence, and 3) depth and accuracy.

Assessment 1 – Part B: Stack Overflow Practical Exploitation Task

- Students will be given **two hours** to complete stack overflow exploitation task.
- This task will be performed in a protected environment; no external tool use will be allowed.
- Students will be able to reference written notes in an open-book structure.
- Successful exploitation of the target binary within the constraints of the task is required to pass this assessment.
- Submission will be in the form of a commented Python script.

Marking criteria: 1) reliability of the exploitation, 2) creativity and originality, and 3) suitability and feasibility.

Course Learning Outcomes

- CLO1 : Develop and implement exploitation strategies for use on endpoints.
- CLO2 : Bypass modern exploit mitigation controls.
- CLO4 : Identify vulnerable coding structures by examining source and compiled code;

General Assessment Information

For all assessment tasks unless otherwise noted, you are permitted to use standard editing and referencing functions in word processing software. You must not use any functions that generate or paraphrase [or translate] passages of text, whether based on your own work or not. Please note that your submission will be passed through an AI-generated text detection tool. If your marker has concerns that your answer contains passages of AI-generated text you may be asked to explain your work. If you are unable to satisfactorily demonstrate your understanding of your submission you may be referred to UNSW Conduct & Integrity Office for investigation for academic misconduct and possible penalties.

Grading Basis

Standard

Course Schedule

Attendance Requirements

Students are strongly encouraged to attend all classes and review lecture recordings.

Course Resources

Prescribed Resources

None

Recommended Resources

None

Staff Details

Position	Name	Email	Location	Phone	Availability	Equitable Learning Services Contact	Primary Contact
Convenor	Pedram Hayati					No	Yes

Other Useful Information

School-specific Information

The Leaning Management System

Moodle is the Learning Management System used at UNSW Canberra. All courses have a Moodle site which will become available to students at least one week before the start of semester. Please find all help and documentation (including Blackboard Collaborate) at the Moodle Support page.

UNSW Moodle supports the following web browsers:
• Google Chrome 50+
• Safari 10+
Internet Explorer is not recommended. Addons and Toolbars can affect any browser's

performance.

Operating systems recommended are:

• Windows 10,

• Mac OSX Sierra,

• iPad IOS10

Further details:

Moodle System Requirements

Moodle Log In

If you need further assistance with Moodle:

For enrolment and login issues please contact:

IT Service Centre

Email: itservicecentre@unsw.edu.au

Phone: (02) 9385-1333

International: +61 2 9385 1333

For all other Moodle issues please contact:

External TELT Support

Email: externalteltsupport@unsw.edu.au

Phone: (02) 9385-3331

International: +61 2 938 53331

Opening hours:

Monday – Friday 7:30am – 9:30 pm

Saturday & Sunday 8:30 am – 4:30pm

Study at UNSW Canberra

Study at UNSW Canberra has lots of useful information regarding:

• Where to get help

• Administrative matters

• Getting your passwords set up

• How to log on to Moodle

• Accessing the Library and other areas.

UNSW Canberra Student Hub

For News and Notices, Student Services and Support, Campus Comminity, Quick Links,

Important Dates and Upcoming Events

School Contact Information

Deputy Head of School (Education): Dr Erandi Hene Kankanamge

E: e.henekankanamge@adfa.edu.au

T: 02 5114 5157

Syscom Admin Support: syscom@unsw.edu.au

T: 02 5114 5284

Syscom Admin Office: Building 15, Level 1, Room 101 (open 10am to 4pm, Mon to Fri)