ZEIT8020 Cyber Offence – Threats and Opportunities Distance Mode - Semester 1, 2023

Course Outline

Course Staff

A/Prof Frank den Hartog

Course Convener

Room 203, Building 15

Tel: (02) 5114 5138

Frank.den.Hartog@unsw.edu.au

Frank is available for consultation without appointment in his office or by phone every working day during semester from 9:00-9:30 am. However, making an appointment is strongly recommended, and can be done electronically at https://denhartog.youcanbook.me/ .

Mr Bevan Jones

Lecturer

B.D.Jones@unsw.edu.au

Bevan is available for consultation by appointment.

Course Details

Units of Credit (UOC): 6

The aim of this course is to provide the foundation for offensive tactical cyber operations, to develop knowledge and skills of various tools, techniques and procedures involved with offensive cyber operations, and to develop competence in addressing strategic, operational and tactical issues of cyber operations.

This course consists of eight weeks of theory mixed with practical sessions. The students will do the practical sessions by remotely accessing the UNSW Canberra's cloud Cyber Range. During this period students will be presented the entire course syllabus and assisted with preparation for the delivery on the major assessments, which are due in weeks 12 and 15. There is no mid-semester break for this course.

Course Description

Every person, business, organisation and government around the world is investing in cyber security. Information is increasing in value, the growth of devices online is exponential, and the complexity of systems is driving increasing opportunity for their subversion. Both software and security vendors strive to design, build and distribute technologies to protect information, plug software holes, and detect malicious activity.

The Cyber domain is an active arms-race where the attacking side has the inherent advantage: attackers need only discover a single vulnerability within a target's wilderness of code, architecture or configuration to successfully breach security. At the same time, defenders race to discover vulnerabilities and implement counter measures.

Combating attacker tools using technical mitigation and detection measures is an incomplete strategy. New thinking in the realm of cyber security focusses more and more on defeating cyber threat actor behaviour rather than just their technology. Hack-back, active-defence, and infiltration of cyber threat actor networks, are examples of targeting the people behind the keyboard.

Essential to combating cyber threat actor behaviour is understanding it. The tactics, techniques and procedures (TTPs) employed by a cyber threat actor are also known as 'tradecraft'. It is this tradecraft, which is the focus of this course.

Students will be walked through the various stages of the Cyber Kill Chain. The Cyber Kill Chain is an industry-accepted methodology for understanding how an attacker will conduct the activities necessary to cause harm to an organisation.

Course assumed knowledge

Students will need a good understanding of, and basic practical experience with:

- computer and software architecture;
- basic security engineering;
- network engineering;

- Linux operating system command-line interfaces;
- VMware virtualisation technologies.

Students’ successful completion of the course will depend largely on the ability to design, configure and operate offensive security tools. Thus, students experienced in conducting online technical research to troubleshoot problems will be greatly advantaged.

It is also strongly recommended that students have access to a computer with at least 8 gigabytes of memory to undertake the final assessment, and to a stable Internet connection of at least 1 Mbps symmetric.

Student Learning Outcomes

On successful completion of this course, students will be able to:

LO1. Conduct simple cyber offensive operations by defining the suitable operation goals and outcomes, conducting reconnaissance against a target, identifying suitable vulnerabilities for access opportunities, selecting and packaging computer exploits, understanding and applying strategies to penetrate network defences, installing network backdoors for access assurance, and expanding network access to reach target systems.

LO2. Identify opportunities in defeating cyber threat actor tradecraft by understanding the full spectrum of offensive activities.

LO3. Improve an organisation’s security by understanding and acting on artefacts and signatures generated by cyber offensive activities.

LO4. Provide advice to policy makers on strategic issues regarding cyber capabilities, doctrine, and partnerships.

Resources for Students

Week 0 and Week 1 of the course will provide a wealth of background information which students can use to refresh their basic knowledge of Linux, security, and computer networks. Weeks 2-8 will be guided by slides and the exercise book. The exercises are additional to the slides, and it is expected that, by doing the exercises, students learn how to find information about relevant tools and techniques on the Internet, like real offense teams do. During the course, also various recommended readings will be provided. The relevance of those depends on the direction the students choose to take with their essays and practical projects.

Teaching Strategies

The course is delivered as a combination of lecturing consolidated with practical laboratory exercises to be undertaken by students under supervision of the lecturers. The intensive teaching of theory and related practical skills prepares the student optimally to achieve the stated learning outcomes. The first eight weeks also fully prepare students for the expectations of the two major assessments, to be undertaken in the remaining weeks of the semester.

Every week, students will be provided a list of activities to undertake, including reading, watching videos, doing exercises, etc. All lectures will be provided by recorded video, which can be downloaded (but may not be distributed further), or directly streamed from Moodle. In addition, students are encouraged to discuss the matter and the exercises via the course forum on the Moodle page. Frank and Bevan will actively contribute to those discussions. In addition, various live Q&A sessions will be organized via Collaborate on the Moodle page, teachers are responsive to emails, and students are encouraged to organize one-to-one sessions with Frank or Bevan when they are struggling.

Course Schedule

Week	Dates	Topic
1	27 Feb – 3 Mar	Introductory readings
2-3	6 – 17 Mar	Module 1: Basics, Research and Targeting
4-5	20 - 31 Mar	Module 2: Reconnaissance Tools and Resources
6-7	3 - 14 Apr	Module 3: Exploitation, Shells, Exploitation Tools
8	17-21 Apr	Module 4: Cover and Pivot
8-9	17-28 Apr	Work on Theoretical Presentation
10-12	1-19 May	Work on Discussion Essay
9-15	24 Apr – 9 Jun	Work on Practical Project

Both Frank and Bevan will be involved in all modules.

Assessment Requirements

All marks obtained for assessment items during the session are provisional. The final mark as published by the university following the assessment review group meeting is **the only official mark.**

Students are not required to pass any one particular piece of assessment; they simply need to achieve at least 50 marks out of a total 100 marks to pass this course.

Assessment	Weight	Due Date

Practical Exercises	20%	Part 1 (5%):
		Sunday 19 March 11:55 pm (feedback provided by census date)
		Part 2 (15%):
		Sunday 23 April 11:55 pm

Theoretical Presentation	10%	Sunday 30 April 11:55 pm
Discussion Essay	30%	Sunday 21 May 11:55 pm
Practical Project	40%	**Friday** 9 June 11:55 pm

All assessments must be submitted using the appropriate upload links in Moodle. The marking criteria for the Practical Exercises will be 1) completeness, 2) quality of analysis, and 3) quality of documentation. The marketing criteria for the Theoretical Presentation will be 1) depth and breadth of research, 2) structure and coherence, and 3) discussion participation.

The Essay/Report must be an analytical research paper. The marking criteria for the Practical Project are 1) research breadth and depth, 2) structure and coherence, 3) creativity and originality, and 4) accuracy and completeness.

The Practical Project comprises a scenario walkthrough, which should be submitted via the Moodle submission link, and may include links to the storage location of the accompanying Virtual Machines (VMs). These VMs should be stored in respective students' allocated OneDrive storage. The marking criteria for the Practical Project are 1) complexity and diversity (targets, techniques, tools), 2) creativity and originality, and 3) suitability and feasibility.

Outcomes-Assessment Matrix

Assessment item	LO 1	LO 2	LO 3	LO 4
Practical Exercise	X		X	
Theoretical Presentation		X		X
Discussion Essay		X		X
Practical Project	X	X	X	X

Late Submission of Assessment

Unless prior arrangement is made with the lecturer or a formal application for special consideration is submitted, a penalty of 5% of the total available mark for the assessment will apply for each day that an assessment item is late up to a maximum of 5 days (120 hours) after which an assessment can no longer be submitted and a grade of 0 will be applied.

All requests for special consideration must be formally submitted via MyUNSW prior to the assessment due date. An appropriate extension of the deadline or a supplementary assessment (whatever is most appropriate) will be offered to any student if their request for special consideration is approved. If a supplementary assessment is offered, then the mark for the assessment task will be based solely on the supplementary assessment.

Developing Graduate Capabilities

Successful completion of this course contributes to the acquisition of UNSW graduate capabilities. UNSW aspires to develop globally focused graduates who are **rigorous scholars**, capable of **leadership** and **professional practice** in an **international** community.

The Learning 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

For further details about system requirements click here. Log in to Moodle here.

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

Course Evaluation and Development

One of the key priorities in the 2025 Strategy for UNSW is a drive for academic excellence in education. One of the ways of determining how well UNSW is progressing towards this goal is by listening to our own students. Students will be asked to complete the myExperience survey towards the end of this course.

Students can also provide feedback during the semester via: direct contact with the lecturer, the "On-going Student Feedback" link in Moodle, Student-Staff Liaison Committee meetings in schools, informal feedback conducted by staff, and focus groups. Student opinions really do make a difference. Refer to the Moodle site for this course to see how the feedback from previous students has contributed to the course development.

Important note: Students are reminded that any feedback provided should be constructive and professional and that they are bound by the Student Code of Conduct Policy

https://www.unsw.edu.au/content/dam/pdfs/governance/policy/2022-01-policies/studentcodepolicy.pdf

Other Information

This is a 6 UOC course, which means that students typically need to spend ~150 hours to pass it. Only a fraction of these hours will be spent during the first five weeks. The remainder will be needed to prepare the out-of-class assessments, and students should plan their time accordingly.

Students are bound to the UNSW ICT Acceptable Use Policy when on campus and making use of the UNSW ICT facilities. See https://my.unsw.edu.au/student/resources/ComputingCommunicationRule.html .

Further information, e.g. the SEIT Guide to Referencing, UNSW Graduate Capabilities, UNSW Assessment Policy, UNSW Canberra Assessment Procedures, and the policies and guidelines on Academic Honesty and Plagiarism, are available on the course's Moodle page.

Referencing

In this course, students are required to reference following the APA 6 referencing style. Information about referencing styles is available at: https://guides.lib.unsw.adfa.edu.au/c.php?g=472948&p=3246720 . Hint: Google Scholar provides references of all literature in APA style (click the "-sign).

Academic Integrity and Plagiarism

UNSW has an ongoing commitment to fostering a culture of learning informed by academic integrity. All UNSW staff and students have a responsibility to adhere to this principle of academic integrity. All students are expected to adhere to UNSW's Student Code of Conduct.

Plagiarism undermines academic integrity and is not tolerated at UNSW. It is defined as using the words or ideas of others and passing them off as your own, and can take many forms, from deliberate cheating to accidental copying from a source without acknowledgement.

For more information, please refer to the following:

https://student.unsw.edu.au/plagiarism

Study at UNSW Canberra

https://www.unsw.adfa.edu.au/study
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.

CRICOS Provider no. 00098G

The University of New South Wales Canberra.