UNSW CANBERRA | Cyber

Cyber Offence

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

Description

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 (TTP) involved with offensive cyber operations, and to develop competence in addressing strategic, operational and tactical issues of cyber operations. Students will be walked through the various stages of the Cyber Kill Chain, which is an industry-accepted methodology for understanding how an attacker will conduct the activities necessary to cause harm to an organisation. For every stage, students will get hands-on experience with various TTPs as employed by cyber threat actors.

Topics covered include:

- Enumeration
- Exploitation
- Escalation
- Netcat and Wireshark
- OSINT
- OS Fingerprinting
- Vulnerability Scanning
- Social Engineering
- Avoiding Attribution

Learning Outcomes

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

- Conduct simple computer network operations by defining the suitable operation goals and outcomes.
- Identify opportunities in defeating cyber threat actor tradecraft by understanding the full spectrum of offensive activities.
- Improve an organisation's security by understanding and acting on artefacts and signatures generated by cyber offensive activities.
- Provide advice to policy makers on strategic issues regarding cyber capabilities, doctrine, and partnerships.
- Plan computer network operations using industry and government best practices.

Who Should Attend

This course is well suited to experienced IT professionals who wish to further specialise in offensive and defensive tactical cyber operations.

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

Cyber Offence Basics

The first day of the course will introduce the Cyber Kill Chain and the legal aspects of Cyber Offence. We will then look at Windows and Kali Linux File System navigation and manipulation, and go through basic computer networking principles. Students will utilise virtual machines to do exercises with Netcat and Wireshark.

Topics

Command Line, Standard input/output, Pipes, IP Addresses, Ports, Network Commands, Services, Netcat, Wireshark.

Day 2

Reconnaissance

Day 2 of the course will introduce the main reconnaissance techniques, including Social Engineering, OSINT, network enumeration, vulnerability scanning, email harvesting, OS (and service) fingerprinting. Practical exercises include passive recon on real targets and active recon on the virtual machines.

Topics

SMTP, SMB, SNMP and DNS Enumeration, nmap, nikto, SET, phishing, OpenVAS, the Harvester.

Day 3

Access and Exploitation

Day 3 of the course will introduce students to Searching for Exploits, Execution Techniques and Transfer Methods. Practical exercises include creating a reverse shell using msfvenom, outputting and executing payloads and detecting them with Metasploit.

Topics

Exploit Sources, Bind vs Reverse, Staged vs Stageless, Executable Formats, Metasploit, Msfvenom, Catching Shells.

Day 4 & Day 5

Perseverance and Exfiltration

This session will cover basic Windows and Linux escalation techniques such as Kernel Exploits, Privileged Exploits, Attacking Hashes, and Pivoting. Students learn to understand password hacking using Meterpreter and Medusa. We will also look at avoiding detection, website attacks, and exfiltration.

Topics

Kernel Exploits, High Privileged Programs Credential Theft, Insecure Configurations, Privileged Exploits, Metasploit, Proxytunnels.

"The course was very informative and provided a very good broad understanding of offensive strategies."

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