UNSW CANBERRA | Cyber

Cyber Security Boot Camp

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

Description

This is a 101 IT cyber security short course designed to teach you about IT security issues, looking at the types of attacks that are happening now, how they work and how to protect yourself and your organisation against them.

This is an intensive, zero to hero, five day course covering:

- Overview of Computer Science/IT
- Networking Fundamentals
- Open Source Intelligence
- Cyber Security Knowledge Domains
- Roles in Industry
- Cyber Security Threat Modelling using STRIDE methodology
- Real world case studies
- Information resources for staying current

The course is centred around the crucial and relevant cyber security skills and techniques needed to protect and defend your organisation's business assets and information systems. Training is delivered in a boot camp style format and with integrated hands-on lab exercises designed to give you the chance to test your newly acquired skills.

Learning Outcomes

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

- Understand the cyber threats and vulnerabilities of computer networks, protocols, applications and network equipment.
- Understand basic cybersecurity issues, privacy principles and organisational requirements relating to data confidentiality, integrity, and availability.
- Understand common attack vectors, different classes of attacks and types of cyber attackers.
- Understand basic cryptography and cryptographic key management concepts.
- Use Linux command line tools to determine network content, passwords and vulnerabilities.

Who Should Attend

This is an entry level course for potential cyber security professionals who are competent computer users and assumes no Cyber Security knowledge and basic skills in Windows.

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

Computer networks

Day 1 of the course gives an overview of the history of cyber security before diving into computer networks: what components they are comprised of, how they physically and virtually connect to the internet and the limitations that make them susceptible to attacks.

Topics

Computer and PLCs, Internet of Things (IoT), IP Addresses, Computer Networks, OSI Model, Cables, Switches & Modems, Cloud Computing.

Day 2

The IT and Cyber Industries; Threats and Countermeasures - Theft

The first part of the session focuses on the IT profession in general and looks at the various work roles within the industry. We will then move onto Cyber Security roles and disciplines and how these relate to attack and response processes. Fundamental security frameworks, theft attacks and countermeasures will also be discussed.

Topics

IT roles and disciplines, Cyber roles and disciplines, Social Engineering, Security Fundamentals, Cyber Attacks, Cryptography, Encryption.

Day 3

Threats and Countermeasures – Coding, Denial of Service

Day 3 will focus on malicious code, denial of service attacks and relevant countermeasures. An overview of threat modelling and identification methodologies will be covered and students will participate in a practical threat modelling exercise.

Topics

Flawed Code, Malware, PenTesting, Firewalls, IDS/IPS, White Listing, Proxy Listing, Denial of Service Attacks, Threat Modelling and STRIDE.

Day 4

Interceptions, Impersonation; Cybercrime, Actors and Stuxnet

The day will start off with a rundown of the different methods of interception and social engineering techniques employed during attacks as well as encryption and authentication based countermeasures. We will discuss key players involved in cybercrime activities and look at several attack case studies.

Topics

Threats of Interception, Asymmetrical Cryptography, Countermeasure of Authentication, Passwords, Keyloggers, Cyber Actors, Stuxnet.

Day 5

Practical Cyber Security Exercises

The final day of the course will give students the opportunity to put their newly acquired skills and knowledge into practice. Hands on lab based exercises will cover scanning and banner grabbing, SMB & SMTP enumeration with Kali Linux, hacking FTP Telnet and SSH, password cracking in penetration testing and vulnerability assessment with OpenVAS.

Topics

Metasploitable, SMB/SMTP Enumeration with Kali Linux, Hacking FTP Telnet & SSH, Penetration testing, OpenVAS.

"Provided a good introduction to cyber security. The instructor translated technical information into easier to understand concepts."

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