UNSW CANBERRA | Cyber

Introduction to Pen Testing

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

Description

This course provides an introduction to Penetration Testing and works through the differences between Vulnerability Assessments and actual Penetration Tests. The course will take participants into the world of the attackers and the lengths they will go to gain a foothold in the networks of their victims.

Topics covered include:

- Pre-engagement interactions
- Reconnaissance
- Threat Modelling
- Vulnerability Analysis
- Exploitation
- Post Exploitation
- Reporting

Learning Outcomes

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

- Understand the different types of penetration testing and the industry standards that regulate the field.
- Understand how penetration testers utilise common attack vectors in exploits.
- Use software and command line tools for scanning, enumeration and exploitation.
- Understand how web based attacks affect penetration testing workflows.
- Understand how social engineering techniques are utilised in penetration testing strategies.

Who Should Attend

This course is designed for IT graduates entering the Cyber Security profession or those in junior and intermediate Cyber Security roles.

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

Pen Testing Introduction

The first section of the course gives a brief history and overview of the purpose and different types of penetration testing. We will also discuss the goals and outcomes of penetration testing, rules of engagement that govern the field, data collection and reporting methods.

Topics

Red teaming, Vulnerability scanning, Attack cycles, Change control, Testing frameworks, Exploit techniques, Stakeholder engagement.

Day 2

Scanning and Enumeration

On day 2 we start by looking at techniques and tools used in network scanning such as ARP sweeping, DNS scanning, DNS enumeration and port scanning. We will finish off by running through several practical lab based exercises utilising Ettercap and Kali Linux.

Topics

Networking scanning, Google hacking database vulnerability scanning, Netcat, Nikto, Golismero tool, Dnswalk, Dnsrecon, Fierce Script, Thehavester.

Day 3

Exploitation Techniques

We'll continue exploring network exploitation techniques utilising the Metasploit framework, modules and shellcode payloads. Afterwards we'll see how the framework integrates with Postgresql database within Kali Linux. We will end the day with a lab walkthrough on MSF3 Windows System.

Topics

Metasploit framework, Ruby programming, Exploit code, Auxiliary modules, Exploit modules, Post modules, Shellcode, Listeners, Encoders, Social Engineer Toolkit.

Day 4

Website Penetration Testing

This session is designed to broaden your knowledge of web based attacks and provide a greater understanding of how dangerous and difficult they are to identify and track. You will gain hands on experience using the same tools and processes attackers follow in simulated online scenarios.

Topics

Injection attacks, Scripting attacks, Sensitive information exposure, Cross site scripting, SQLi, SQLMAP, Web scanners, directory brute force tools.

Day 5

Internal Testing & Social Engineering

The final day of the course will focus on how social engineering (SE) campaigns are formed and will introduce some of the software and methods used for these attacks. We will touch on the use of SMB Protocol, MimiKatz, Responder Python Script and Social-Engineer Toolkit.

Topics

SMB Protocol with Kali Linux, MimiKatz Post exploit tool, Responder Python Script, Browser exploitation framework.

> *"Very good course - was very in-depth but allowed people with little prior knowledge to get up to speed quickly."*
>
> 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