UNSW CANBERRA | Cyber

Intrusion Analysis and Response

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

Description

This course aims to develop knowledge and understanding of the strategies, techniques and technologies used in attacking and defending networks and how to design secure networks and protect against intrusion, malware and other hacker exploits.
Designed as either a standalone course or to flow from Introduction to Pen Testing, the course will explore the attackers' mindsets and methods, and work through the different ways of protecting the estate. The course will cover keystone technologies required in an effective security defence solution including an introduction to usable and effective policies that staff will follow and not be encouraged to work around.

Theoretical content includes

- Network security fundamentals
- Intrusion analysis and response
- Secure socket layer (SSL)
- IPSec
- Firewalls
- Intrusion analysis practices
- Legal, privacy and ethics issues

Learning Outcomes

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

- Understand the main functions of a Security Operations Centre.
- Understand and evaluate the key issues involved in designing secure networks.
- Understand the issues arising in the collection of computer evidence after network breach.
- Develop effective risk management plans to protect against malware and other hacking exploits.
- Formulate a range of strategies and solutions for testing and continuously improving the security of a network.

Who Should Attend

This course is designed for IT graduates entering the Cyber Security profession or those in junior Cyber Security roles. It is also useful for investigators who wish to develop a technical approach to their profession. Prior attendance at Cyber Security Boot Camp is recommended.

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

Network Security and Linux IAR Fundamentals

The first day of the course will look at Linux incident analysis and response processes, specifically Bash Shell scripting, permissions, shell expansion, functions and hashing. Students will then be introduced to network security fundamentals, looking at layers, services, protocols and common issues.

Topics

Linux Command Line, Shell Coding, Trustico, Networking, Traffic Management, Security Architecture, SSL Components, Firewall Principles, Intrusion Analysis Practices.

Day 2

Cryptography and Computer Networks

Day 2 of the course will introduce students to the principles of cryptography, properties of secure communication and methods of encryption/decryption. Students will then be stepped through the fundamentals of computer networks, covering transport-layer services, UDP/TCP and IP protocol.

Topics

Confidentiality, Authentication, Integrity, Digital Signatures, Access Control, Public Key Algorithms, Transport & Network Layer Protocols, Internet Routing.

Day 3

Introduction to MANET; Incident Analysis & Response Theory

The first half of the session will cover the characteristics of mobile ad hoc networks (MANET), their applications and common security vulnerabilities. The rest of the day will focus on the concepts and practical processes of incident analysis and response.

Topics

Security in MANET, Dynamic Source Routing, Attacks in MANET, DDoS, Incident Response Process, Electronic Evidence Collection and Analysis, Cyber Kill Chain techniques.

Day 4

Attacks, Counter Measures, Security Assessment and Testing

Day 4 will look at different types of attack vectors and methods of defence. Students will be given an introduction to security assessment, risk identification and evaluation techniques. We will also look at penetration testing methodologies, information gathering and flaw testing.

Topics

In-line Memory Attacks, Webshells, Dos Attack, Flood Attack, Smurf IP Attack, Asset Identification, Threat Assessment, Security Assessment Components, Probing the Network.

Day 5

Legal, Privacy and Ethical Aspects

The final day of the course will give an overview of the various governance issues involved with cybercrime and computer crime. Students will be introduced to the issues facing law enforcement, intellectual property and copyright implications, privacy concerns, and ethical codes of conduct

Topics

Types of Property, Patents, Trademarks, DMCA Copyright Act, Privacy Protections, Australian and Global Privacy Laws, Data Surveillance.

"The course provided a very good level of fundamental knowledge with a variety of practical, hands-on exercises."

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