UNSW CANBERRA | Cyber

Cyber Deception

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

Description

The need for awareness of cyber deception is growing. Cyber deception has been identified as one of the top 10 technologies businesses should be employing for cyber defence.

This 5-day course will provide students with hands-on experience of how to build, deploy and configure various cyber deception tools and technologies to protect computer networks and digital data. Students will use a combination of open source software, scripts and direct operating system configurations to create confusion, bait and trap intruders and unauthorised insiders.

The course has been designed for people with a beginner and intermediate level of technical IT skill and experience. Most of the course content is hands on activities. Students will configure and build cyber deceptions. Many of these will be using command line. The course will walk students through the basics of how to undertake each activity and provide them the means to complete the exercises. No academic or technical knowledge is assumed but the course can be challenging, in places if users are not familiar with basic IT and cyber security principles and tools.

Learning Outcomes

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

- Understand basic cyber deception tactics used in civilian businesses and defence environments.
- Understand how cyber deception tools and technologies protect computer networks and digital data.
- Understand and set up honeypots, sinkholes and covert network tunnels.
- Use open source software and command line tools to falsify web pages, web traffic and SSH services.
- Demonstrate the ability to plan and use best industry practices in cyber deception.

Who Should Attend

Managers, network security professionals and cyber security engineers.

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

Introduction to Cyber Deception

Day 1 starts with a comprehensive overview of the history of cyber deception and looks at how this concept fits into a cyber security framework. Students will be set up with VMWare environments and stepped through practical exercises.

Topics

VMWare Essentials, Linux Distributions, Command Line Basics, File System Navigation, Directories, Commands and Arguments.

Day 2

Hiding the Real

This session will cover the structure of deception and will look at methods for disrupting automated attacks. Students will be introduced to Steganography along with lab based exercises covering changing identity and modifying ports.

Topics

Hidden Partitions, Port Obfuscation, Covert Network Tunnels, Steganography Processes, Obfuscating Code, Masking and Repackaging Ports.

Day 3

Honeypots and other defensive tools

Day 3 will introduce students to the history of Honeypots and how they can be used to defend against cyber-attacks. The session will also look how to set up a convincing honeypot and will cover a number of other defensive tools.

Topics

SSH Honeypots, Elastichoney, HoneyNet Project, MHN Server.

Day 4

Showing the False

This session will look at techniques to disrupt automated attacks such as faking network traffic and services. Student will also be introduced to the requirements of building fake content in order to delay and confuse adversaries. Practical exercises include faking web pages & traffic and faking a SSH service.

Topics

Fake Services, Fake Traffic, Fake Content, Sinkholes, Labrea Tarpit, Tiny HP, SpiderTrap, Glastopf, Cowrie.

Day 5

Cyber Deception Limitations and Planning

The final day of the course will give an overview of the limitations of deceptive techniques and issues surrounding the legality of practices. Reasons and considerations to be aware of when planning to use deception will also be covered. Students will break into groups and complete a deception planning exercise.

Topics

Deception strategies, Tactics and Plan Architecture, Passive and Active Actions, Kill Chain.

"I would highly recommend this course. Well paced with good examples, exercises and labs."

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