UNSW CANBERRA | CYBER

CYBER SECURITY CAREER PATHWAY

LEVEL 1 INTRODUCTION

- CYBER SECURITY BOOT CAMP
- INTRUSION ANALYSIS AND RESPONSE
- INTRO TO PEN TESTING
- CYBER DECEPTION

LEVEL 2 FUNDAMENTALS

- WIRELESS, MOBILE AND INTERNET OF THINGS SECURITY
- CYBER OFFENCE
- CYBER DEFENCE
- CRITICAL INFRASTRUCTURE CYBER SECURITY (SCADA)
- PYTHON FOR CYBER SECURITY PRACTITIONERS

LEVEL 3 SPECIALISED

- EXPLOIT DEVELOPMENT
- ADVANCED EXPLOIT DEVELOPMENT
- REVERSE ENGINEERING
- CODE REVIEW

STANDALONE

- RED VS BLUE
- CISSP
- CYBER WAR 101

LEVEL 1: INTRODUCTION

CYBER SECURITY BOOT CAMP

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 at the moment, how they work and how to protect yourself and your organisation against them.

INTRUSION ANALYSIS AND RESPONSE

The 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.

INTRO TO PEN TESTING

This course covers the OWASP and OSTINT content. It provides an introduction to penetration testing and works through the difference between vulnerability assessments and actual penetration tests. The course will take the participants into the world of the attackers and the lengths they will go to gain foothold in the networks of their victims.

CYBER DECEPTION

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

LEVEL 2: FUNDAMENTALS

WIRELESS, MOBILE AND INTERNET OF THINGS SECURITY

Wireless technologies are ubiquitous in modern systems yet pose unique challenges. This course covers current wireless network protocols and the systems typically deployed in network environments, their weaknesses, practical attack methodologies and mechanisms for their defence.

CYBER OFFENCE

This course provides the foundation for offensive and defensive tactical cyber operations. It also seeks to develop the participants knowledge and skills of the tools, techniques and procedures involved with cyber offence. The course will increase the competence of participants in addressing strategic, operational and tactical issues of cyber offence.

CYBER DEFENCE

This course provides in-depth understanding of the technical and policy used in computer and network defence. Numerous cyber defence technologies and their effectiveness against modern threats are discussed.

CRITICAL INFRASTRUCTURE CYBER SECURITY (SCADA)

This is a technical course, designed to use simulation tools and equipment to replicate the potential threats against Critical Infrastructure Services (CIS) utilising real life SCADA models.

PYTHON FOR CYBER SECURITY PRACTITIONERS

This course introduces participants to the Python programming language in a security context. Participants are shown core Python language structures before applying these to security problems. Key libraries are introduced, along with common design patterns for security applications.

LEVEL 3: SPECIALISED

EXPLOIT DEVELOPMENT

This course will introduce participants to the art and science of exploit development. Core concepts involving debuggers, stack based overflows, disassemblers and some defence mitigation will be taught in a largely practical delivery style. Instruction will commence with an overview of core concepts, and will then quickly dive into the intricacies of modern x86 CPUs. Finally, mitigations such as DEP and ASLR will be investigated.

ADVANCED EXPLOIT DEVELOPMENT

This course takes participants with a strong foundation in exploit development and exposes them to the more recent operating system defences. In this interactive course, participants will learn and apply techniques to bypass or weaken a range of modern security controls such as Address Space Layout Randomisation (ASLR), Data Execution Protection (DEP/NX) and Stack Cookies on x86 and x86 64 processors.

REVERSE ENGINEERING

This course provides an introduction to reverse engineering. Participants will do exercises to gain familiarity with the tools and techniques necessary to reverse engineer software.

CODE REVIEW

This course will look at reviewing C/C++ code for security issues. The course is heavily based around practical auditing of actual C/C++ programs. Common coding bugs will be identified in set lectures and then students will apply the theory by reviewing real programs and identifying vulnerabilities. In addition to manual code review, automated means of vulnerability discovery will be briefly discussed, including fuzz testing and static analysis.

STANDALONE

RED VS BLUE

The intent of the Red vs Blue exercise is to expose practitioners to a simulated cyber combat operation in order to provide foundation skills in and an appreciation for the complexity and friction of combat in cyberspace. Learning focus will be on collective command, control and communication (C3) and individual technical abilities.

CISSP

Led by an (ISC)² authorised instructor, this training course provides a comprehensive review of information security concepts and industry best practices, covering the 8 domains of the CISSP CBK. This training course will help candidates review and refresh their information security knowledge and help identify areas they need to study for the CISSP exam.

CYBER WAR 101

Participants will gain insights into key concepts of cyber military operations at the strategic level of war. The course will enable participants to adjust pre-existing notions of combat management or, in the civil sector, risk management, to take account of the likely impacts of complex multi-vector, multi-phase cyber attacks on Australia, including on its deployed forces.

UNSW.ADFA.EDU.AU/STUDY/PROFESSIONAL-EDUCATION-COURSES/PROGRAMS

cyber@adfa.edu.au

+61 2 6868 8350

UNSW Canberra, PO Box 7916, Canberra BC ACT 2610