USYD Cybersecurity Boot Camp

Course Structure

You can think of this boot camp as six modules that each focus on an important piece of the vast cybersecurity landscape:

Module 1: Security Fundamentals (Units 1-2)

- The first two weeks of the program will be largely conceptual. This week, you will learn how to think like a security professional, look at the cybersecurity career landscape, and get an introduction to certifications in the space.
- Next week, we will look at governance, risk, and compliance. You will look at security from an organizational perspective via governance, risk, and compliance, and how these topics affect security controls and other decisions.

Module 2: System Administration (Unit 3-7)

- Beginning in Unit 3, we will start using technical lab environments to complete activities. You will get comfortable using the command line and hone your systems administration skills in the several units that follow.
- We will cover both Linux and Windows systems, and dive into programming with both Bash and PowerShell. You will configure and audit servers, and harden them from malicious attacks.

Module 3: Networks and Network Security and Project 1 (Units 8-13)

- Security professionals are expected to have a strong foundation in networking. In this module we'll cover topics such as network configuration, design, ports, protocols, and data communication.
- We'll get hands-on practice analyzing data packets on the wire and investigating network security attacks and hardening, and cover a variety of topics in cryptography. This module will also look at cloud virtualization and security, and you will complete your first project.

Module 4: Offensive Security (Units 14-17)

- With our networking foundation now established, we'll look at a variety of offensive topics in security.
- We'll start with web architecture and dive into common web vulnerabilities and the hardening techniques associated with them. We'll then cover ethical hacking and penetration testing, and will use tools like Metasploit.

Module 5: Defensive Security and Project 2 (Units 18-21)

- We'll now look at defensive security monitoring and spend a few weeks diving into SIEM with Splunk. We will set up security monitoring, and create alerts, dashboards, and custom reports.
- You will gain an understanding of the incident response framework, and how to respond to breaches and incidents. We'll also spend a unit on forensics, and will use tools to recover deleted data and solve a sample forensics case.

Module 6: Review and Final Projects (Units 22-24)

- At this point, we've covered a lot! It's time for some focused certification and career prep and review. We will focus primarily on the Security+ exam but will also spend one day of our Certification unit on the CISSP and CEH exams.
- There will also be a short unit on career prep, where we will hone our resumes, sharpen our networking skills, and get practice with both behavioral and technical interviewing.
- We will finish the program with a final project.