Introducing Our New Security Training Courses

In the new year, we're launching a hands-on training service that will help you learn more about offensive security. Let us train you to develop your cybersecurity knowledge by thinking like a hacker. Sound interesting to you? Read on for more information on our security training courses.

Over the past few months, we've been busy developing our Hacking & Defending training courses and we're very pleased to announce they're now available to book for January 2021. At Secarma, we're known for our ethical hacking capabilities, and now we want to pass a little bit of our knowledge on to you, to help you keep security at the forefront of your organisation, or to take your first step into a career in penetration testing.

About the Course

Our Hacking & Defending security training courses consist of a full-day session, hosted by our cybersecurity experts. For the time being, our sessions will be delivered remotely, but stay tuned for in-person training once lockdown restrictions ease. These courses are designed to teach candidates how to think like a hacker by taking them through the process of a penetration test step by step.

We'll show you the methodology that we use, the tools and techniques, and talk you through how pentesting is delivered. You'll learn what security vulnerabilities to look out for, how testing works, the pros and cons of each exploit, and much more. Through these courses, you'll gain practical experience breaking security systems through our hands-on labs, then learn how to build them in a more resilient way.

Currently, our training service consists of two comprehensive courses:

- **Hacking & Defending Networks:** designed to teach systems administrators the tools and techniques we use when targeting network infrastructure during real world penetration tests. You'll learn how to map a network and break into an organisation's infrastructure, then how to secure one against similar attacks.
- **Hacking & Defending Web Applications:** designed to teach web application developers the tools and techniques we use when targeting web apps during real world penetration tests. You'll learn how to spot application vulnerabilities and exploit them, then how to ensure the apps you build are protected against threat actors.

Designed with You in Mind

Our security training courses are designed for organisations and their security teams, as well as individuals who are interested in developing a security testing capability. If you have a technical understanding or are looking to break into penetration testing, we can give you the hands-on experience you need to expand your skills and further your pentesting journey.

What You'll Gain

Many security flaws can be subtle or difficult to spot if you're not well versed in common vulnerability types and testing methods; the more you and your team understand about pentesting, the more you'll be able to do with it. This includes in-house re-testing and building on external remediation advice.

Aspects of security remediation advice can be complicated, and sometimes too convoluted for your business needs, but instead of having an external party come in to help you, we'll train you so you can help yourself. We're not saying that you'll no longer need external pentesting – 3rd party validation is still an important part of robust security. However, with the extra knowledge you'll gain via our courses, you'll be much more confident that any issues that did arise during a pentest can be remediated.

What to Expect

This full day-long course will begin by mapping the attack surface, approaching the work like a real work threat actor, before hunting for vulnerabilities. Once vulnerabilities are discovered (and false positives are eliminated), we'll walk you through the exploitation process, demonstrating the real-world risk of these issues. Next, we'll analyse the vulnerabilities you've discovered and let you step into the shoes of a hacker for the day by exploiting them. Finally, we'll provide guidance on how systems and applications could be hardened. This will make exploitation action more difficult, and attack detection easier.

You can expect the session to follow these steps:

1. Mapping and intelligence gathering
2. Vulnerability discovery
3. Proof of concept and confirmation
4. Exploitation
5. Remediation

Don't worry if you've never done a penetration test before, we'll guide you through the process. You won't become an expert overnight, but it's a great way to understand what we do and develop your skills from there.

Training with us means you benefit from the knowledge of our experienced testers, so we'll help you get more out of your offensive security strategy, or develop your own personal pentesting skills. If these courses sound interesting to you, or beneficial for your organisation, make sure you reach out and register your interest. Be sure to look out for two other training courses that are due to be announced in the new year too, so it's safe to say there's plenty to look forward to in 2021.

If you're interested in our Hacking & Defending Networks or Hacking & Defending Web Applications courses, be sure to check out our events page for specific dates, or contact us directly for more information.