secarma®
CYBERSECURITY EXPERTS

SECURITY TRAINING OVERVIEW

Hacking & Defending Networks

The Secarma training team regularly run hands-on security training courses across the UK and remotely. With labs to allow you to get practical experience breaking security systems, before teaching you how to build systems in a more resilient way. Learn how to compromise network infrastructure, from zero access to Domain Admin.

WHO IS IT FOR?

Our infrastructure hacking course is designed to teach systems administrators the tools and techniques we use when targeting network infrastructure during real world penetration tests.

It's also a useful course for those looking to break into Penetration Testing who want a first step on the journey.

HOW CAN WE HELP?

System Administrators often focus on building a network to deliver IT functions. They're often tied to strict deadlines and therefore ensuring everything is secure is sometimes not the first priority.

Additionally, many security flaws can be subtle or difficult to spot if you're not well versed in common vulnerability types and testing methods.

By using the "hackers" point-of-view throughout the training course we allow those interested in developing a security testing capability to get started on that journey.

HANDS ON - Labs

Our training course includes the following hands-on labs to ensure you gain practical understanding as well as getting to grips with our testing methodology:

- **Kerberos Attacks**

Leveraging common Kerberos attacks including party tricks, kerberoasting, overpassing the hash, and more.

- **Interception Attacks**

Abusing link-local multicast name resolution, as well as address resolution protocol spoofing for credential theft and code execution.

- **Vulnerability Exploitation**

Automating exploitation through common testing frameworks, as well as looking at the wider vulnerability lifecycle.

- **Privilege Escalation**

Escalating from a low privileged foothold account up to a highly privileged account through credential extraction and token impersonation.

FEATURES

- Detail remediation guidance for every vulnerability type covered.
- Multiple challenges for each lab, for beginner to intermediate skill levels.
- Guidance on the Penetration Testing methodology.
- Covers the full path from foothold to full compromise.

0161 513 0960
secarma.com
enquiries@secarma.com

secarma
CYBERSECURITY EXPERTS

SECURITY TRAINING OVERVIEW

Hacking & Defending Networks

This course steps you through the common phases of an Infrastructure Penetration Test and allows you to gain an understanding of how hackers hack.

COURSE OVERVIEW

This course teaches candidates about infrastructure security vulnerabilities by stepping them through the process of a Penetration Test.

We'll map a network and approach the work like a real threat actor before hunting for vulnerabilities. Once vulnerabilities are discovered, we walk through exploitation to demonstrate the real-world risk of issues.

At the end of each section we'll review the discovered vulnerability and offer guidance on remediation.

At the end of the day we'll review all of the findings and give guidance on how systems and networks could be hardened to make exploitation action more difficult and attack detection easier.

Mapping and Intelligence Gathering

Before the engagement begins, we will map the attack surface to discover alive hosts, services, and versions. As well as mapping application functionality.

Vulnerability Discovery

We'll demonstrate methods of finding and confirming vulnerabilities to minimise false positives being highlighted.

Proof of Concept and Confirmation

Where vulnerabilities are discovered a proof of concept exploit will be created to demonstrate the potential business risk. This ensures that false positives are removed by manually confirming and demonstrating all discovered vulnerabilities.

Exploitation

Exploitation involves discovering weaknesses within exposed applications and leveraging those weaknesses to demonstrate as much business risk as possible.

OTHER COURSES

HACKING & DEFENDING WEB APPS

From injection vulnerabilities to abusing file handling functions, we look at how to hack web applications and how to make them more secure.

HACKING & DEFENDING NETWORKS

We run your team through breaking into internal corporate networks and teach them about attack mitigations and defence in depth.

SECURITY AWARENESS

We teach your staff how we compromise organisations and how they can stay safer online, at work and at home.

BESPOKE TRAINING

Looking for something specific? Need something not covered on this page? Talk to us about our bespoke training course development.

WHY SECARMA?

Secarma are a cybersecurity consultancy that specialises in security testing. We're not a training company trying to talk about security testing; we're penetration testers teaching your team what we do every single day.

We aim to combine instructor-led training with hands-on labs, to help your team build stronger software and to help you reduce your organisational risk.

0161 513 0960 secarma.com enquiries@secarma.com