PATHWAY TO PENTESTING

A COMPREHENSIVE TRAINING PROGRAM TO LAUNCH YOUR CYBER SECURITY CAREER

WELCOME TO THE COURSE

We are excited to have you with us!

Over the next 12 weeks, we are going to jump into the world of pentesting. Whether you are just starting out or looking to take your current skills and learn how to use them for offensive security, this course is designed to give you everything you need to succeed.

The course starts with the basics of what pentesting is, laws to be aware of, Linux, and networking. Then we will get into the fun stuff, building up to real-world scenarios such as breaking into systems, compromising high value accounts, and identifying vulnerabilities in web applications. By the end of the course, you will conduct a complete penetration test from start to finish and produce a report just like in the real world.

Our instructors are not just trainers, they are seasoned professionals who have been in the weeds and know what its really like to have this as a career. They are here to guide you and make sure you get as much hands on experience as possible.

This course isn't about memorising tools or commands - instead it's about learning to think like a hacker and how to apply that skill in a legal, ethical way that will make you excited to go work.

CONTENTS **PAGE**

COURSE **OVERVIEW**

Throughout this course, you'll gain a solid foundation in the tools, techniques, and mindset needed to become a successful penetration tester. But this isn't a tick list of knowledge, we will build your confidence, capability, and give you the practical skills needed for the real world.

Week 1: Getting Started with Pentesting and Linux

The course starts by exploring what a career as a penetration tester is like and demystifying the industry. Then it's straight into learning. We will get your lab set up and start work to get you comfortable with our testing machine - Kali Linux.

Why this matters: without a firm grasp of how your testing machine works, you won't be able to safely use the tools throughout the course. At the end of week 1, you will be ready to hit the ground running.

Week 2: Understanding how Networks Work

You may know how to use a computer, and how to connect to your WiFi and get to google, but do you honestly know how any of it works? During this week we focus on learning how computers actually communicate with each other.

Why this matters: networks are the backbone of everything we test. By understanding how they work, you'll be able to identify weaknesses.

Weeks 3 and 4: Infrastructure Testing

During these weeks we really dive into the attacker mindset, learning how to identify target machines and their weaknesses. Weeks 3 and 4 teach how to go from port scanning, to vulnerability analysis, to exploitation. This is where you will start to get your first taste of compromising systems.

Why this matters: networks are made up of countless devices, being able to successfully identify an avenue of attack is a key skill, and gaining access proves your skills.

Week 5: Privilege Escalation and Desktop Breakout

This is where it gets even more exciting! Initial access is only the beginning. This week focusses on how to break out of any desktop restrictions and escalate privileges to take full control of both Windows and Linux devices.

Why this matters: privilege escalation often makes the difference between just finding a vulnerability and truly understanding the risk it poses.

Week 6: Active Directory

Many organisations use Active Directory (AD) to manage users and permissions. Understanding how to attack AD is a crucial skill. We will jump into what AD is, learning how to identify critical information and how to launch powerful attacks, such as Kerberoasting and lateral movement.

Why it matters: AD is a prime target in real world breaches. Being able to identify risks in Active Directory can help organisations protect themselves from attacks

Weeks 7 and 8: Web Application Testing

Now it's onto website security. During these weeks, we will cover how websites actually work, and key vulnerabilities from OWASP Top 10. You will learn a range of manual and tool-based techniques to identify and exploit web application vulnerabilities, such as SQL injection, Cross-Site Scripting (XXS), Inadequate Access Control and more.

Why this matters: web applications can be accessed by anyone with an internet connection. They are therefore a common first step of an attack.

Week 9: Soft Skills and Consultancy

This week, we make sure you understand the difference between just hacking, and being a professional penetration tester. We'll discuss the soft skills needed to make a pentest a success. These will include understanding how to scope and report penetration tests, as well as how to work with clients.

Why this matters: technical skills are crucial, but your ability to effectively communicate findings and give appropriate recommendations is what sets great pentesters apart.

Weeks 10 and 11: Practical Penetration Test

In the final weeks, you will put everything you've learned into a simulated pentesting scenario. From scoping to testing, and delivering a report, you'll experience a complete pentest lifecycle, just as you would in the real world.

Why it matters: this demonstrates your ability to apply the skills you've learnt in a realistic scenario.

Week 12: Pentesting Career Guidance and Pentest Review

In the final week of the program, you will receive feedback on your pentest.

We will also focus on career advice and guidance, such as CV creation and interview prep, and discuss your goals to provide you the best possible support moving on from this course.

Why this matters: at the end of this program, we want to see you succeed - and this week is all about getting you ready to start your career as a tester.

WEEKLY **CONTENT**

Week 1: Getting Started with Pentesting and Linux

During this week, the goal is to introduce the topic of penetration testing to all attendees. We will then get the lab environment set up and run through any troubleshooting activities required.

As this course teaches the skills needed to launch cyber attacks against organisations, we will cover the UK laws around pentesting, followed by becoming familiar with Kali Linux.

Content:

- Introduction to the course
- Overview of penetration testing
- Pentesting roles/a day in the life of a pentester
- UK pentesting laws
- Lab set up

Practical Activities:

- Setting up your lab environment
- Getting familiar with Kali Linux

WEEKLY **CONTENT**

Week 2: Understanding how Networks Work

This week, we will build a strong foundation in networking, a crucial skill for any penetration tester. Understanding how networks function will help us identify vulnerabilities and exploit misconfigurations effectively.

We will begin with an overview of the OSI and TCP/IP models, breaking down how data moves through a network. Next, we will cover IP addressing, subnet masks, and essential network protocols such as ICMP and ARP. We will also explore the concept of ports and services, followed by a deep dive into DNS and its security implications.

Content:

- OSI and TCP/IP models
- IP addresses and network masks
- ICMP and ARP protocols
- Understanding what 'ports' are
- What is DNS
- Security concerns of DNS

Practical Activities:

- ARP and ICMP scanning
- network traffic analysis
- DNS lookups
- DNS zone transfers

WEEKLY **CONTENT**

Weeks 3 and 4: Infrastructure Testing

This week we scan the network, conduct vulnerability analysis and use exploitation tools to compromise vulnerable protocols and systems. We will cover a variety of different protocols, Operating Systems, and tools.

Content:

- What is infrastructure testing
- Host discovery
- Portscanning with Nmap
- Vulnerability analysis with Nessus
- Pentesting common protocols such as SSH, Telnet, NFS, FTP, MySQL, SMB
- Understand the concept of a 'shell'
- Exploit vulnerable machines to gain a 'shell'
- Common post-exploitation activities

Practical Activities:

- arp-scan and Nmap scan environments
- Nessus scanning
- Identify and attack protocol weaknesses
- Exploit vulnerable machines
- Password cracking

WEEKLY **CONTENT**

Week 5: Privilege Escalation and Desktop Breakout

With a level of initial access achieved, this week focusses on bypassing restrictions that stop pentesters from achieving a complete compromise.

Windows desktop breakout techniques will be used to be able to bypass user restrictions, while privilege escalation will focus on both Windows and Linux, to teach horizontal and vertical privilege escalation.

Content:

- What is privilege escalation
- How does horizontal escalation differ from vertical escalation
- Windows privilege escalation techniques and tools
- Linux privilege escalation techniques and tools
- Windows desktop breakout

Practical Activities:

- Bypass windows desktop protections to gain access to restricted functionality
- Manual and automated techniques to achieve Windows privilege escalation
- Manual and automated techniques to achieve Linux privilege escalation

WEEKLY **CONTENT**

Week 6: Active Directory

Active Directory is the most common tool used by large corporate environments to manage their users and resources. This week focusses on explaining the concept of Active Directory, what a domain is, how user permissions and privileges are applied in these environments, and common real-world hacking techniques.

Content:

- What is Active Directory
- What are Domain Controllers
- Why do we care about Active Directory
- Enumeration of Windows devices and accounts
- Attack techniques used against Active Directory

Practical Activities:

- LLMNR poisoning
- Kerberoasting
- AS-REP roasting
- LDAP enumeration
- Extracting data with Mimikatz

WEEKLY **CONTENT**

Weeks 7 and 8: Web Application Testing

During this part of the course, we move away from individual protocols and explore how modern web applications work.

This will cover the fundamentals of how the internet works, how web applications function, and how to identify and exploit weaknesses in application logic.

Content:

- Fundamentals of web applications
- OWASP Top 10 Vulnerabilities
- Client-side weaknesses
- Server-side weaknesses

Practical Activities:

- SQL injection
- Cross-Site Scripting
- Session hi-jacking
- Bypassing access control
- Attacking user authentication and authorisation

WEEKLY **CONTENT**

Week 9: Soft Skills and Consultancy

The technical skills used by pentesters are only half the story. This week focusses on the less visible, soft skills that make a successful tester. We will cover the lifecycle of a penetration test, which includes pre and post testing activities such as scoping, reporting and client communication.

Content:

- Different types of security tests
- How to interact with clients
- What is 'scoping'
- How to produce an effective penetration test report

Practical Activities:

- Scoping activity
- Reporting activity

WEEKLY **CONTENT**

Weeks 10 and 11: Practical Penetration Test

Students will be provided with a simulated penetration test to complete. It will include a scoping engagement, a full penetration test of an environment, and the production of a penetration testing report.

This will be an activity that is as close to reality as possible, and will give students the chance to see what pentesting is like in the real world.

Practical Activities:

- Penetration test scoping activity
- Infrastructure and Application penetration test
- Formal reporting

WEEKLY **CONTENT**

Weeks 12: Pentesting Career Guidance and Pentest Review

Students will be provided with detailed feedback on their penetration test and report with guidance on how to improve.

Career guidance will include the creation of CVs and interview techniques and prep, as well as discussions about different types of job roles in the industry.

Content:

- Penetration test report feedback
- CV guidance
- Interview prep

Practical Activities:

- CV creation

PRE-COURSE **RESOURCES**

You may be thinking "What should I know before we start?".

This is a good question - and while this course will build from an assumption of no knowledge, the more you can prepare, the more effective you will be.

Virtual Machines:

- Setting up Virtual Machines e-book: https://shorturl.at/FNwQS
- What is a Virtual Machine video: https://shorturl.at/JQaxI

Understanding Linux:

- Introduction to Linux video: https://www.youtube.com/watch?v=xp0ebiK0LC4

Understanding Networking and Key Protocols:

- Understand TCP/IP: https://www.youtube.com/watch?v=CRdL1PcherM
- Understanding IP Addresses: https://shorturl.at/3e8Td

Understanding tools and security issues:

- Network Scanning: https://nmap.org
- Exploitation: https://docs.rapid7.com/metasploit/
- Web Vulnerabilities: https://owasp.org/www-project-top-ten/
- General Testing: https://book.hacktricks.wiki

Turning individuals into experts

North Green Security is a leader in penetration testing and cyber security training. Offering a comprehensive range of courses to suit you. We are here to provide guidance and skills that will make you more successful.

Our trainers have over 12 years experience creating and delivering training courses that get results

MORE **ABOUT US**

Academy
www.ngsacademy.co.uk

Email
training@northgreensecurity.com

Website
www.northgreensecurity.com

Discord
https://discord.gg/w7K8yVaFbD

www.northgreensecurity.com

NORTH GREEN SECURITY

Increasing security through education, training and testing

North Green Security is a leader in penetration testing and cyber security training. Offering a comprehensive range of courses to suit you. We are here to provide guidance and skills that will make you more successful.

Our trainers have over 12 years experience creating and delivering training courses that get results

CYBER SECURITY TRAINING TO PROGRESS YOUR CAREER

Training courses

Explore our catalogue of training courses ranging from half-day targeted workshops, to week long courses all designed and delivered by experts that can teach you the skills needed to take your next steps

https://northgreensecurity.com/upcoming-events/

North Green Academy

For those who prefer self-study and want to learn around their schedule, the north green academy provides an ever growing library of videos to teach you the skills needed to drive your career forward

https://www.ngsacademy.co.uk/

Have the best career possible

Our trainers are cyber security professionals who know the skills you need to be successful. Reach out for a chat, or book onto a training course