TRAINING

MWR CYBERSEC

Proactive Network Defence

A three-day training course in network security, teaching you to defend against attacks of all levels of sophistication, up to and including APTs

PND is an exercise-driven training course that will guide you through attacking a real network step by step, so that you can gain a thorough understanding of a modern attacker's mindset and capabilities. We then teach you techniques that will help you to defend your network against attacks of all levels of sophistication, up to and including Advanced Persistent Threats.

Who should attend?

This is a technical course aimed mainly at those who are responsible for deploying and managing network infrastructure, but if you're interested in understanding hacking and security, this is also for you. You won't need any prior security knowledge, as we cover the basics on the way to advanced topics. You will need to know Unix and Windows basics (setting an IP address, installing software, copying, moving, deleting and reading files) and network fundamentals such as the difference between TCP and UDP, the format of an IP address, subnetting / CIDR notation, and to be familiar with the more common protocols such as ICMP, HTTP, DNS and SNMP.

Course highlights

- You'll gain an in-depth understanding of how modern attackers can bypass current perimeter security controls and **break into an internal network**
- You'll see how it's possible to gain full control over a fully patched **Windows 2012 domain**
- You'll learn about security weaknesses in the common flavours of Unix (Solaris, RedHat, Debian, etc.)
- Most importantly, you'll learn how to **build a secure network** that can withstand a targeted attack

Benefits to your organization

- Helps to ensure that your network is resilient to an attack, against even the most **advanced threats**
- **Reduces** the number and severity of the **vulnerabilities** that are introduced into the network
- **Increases your organization's overall understanding** of security, reducing the time and cost of remediating vulnerabilities
- **Stimulates a positive attitude** and an understanding of the importance of security within the infrastructure team

How is this course different?

The course is delivered by experienced security professionals, who perform penetration tests and APT attack simulations on a daily basis.

We focus on teaching offensive security techniques, so that you can fully understand the capabilities of modern attackers and therefore how to defend against them.

This is a practical, exercise driven course. We've simulated a real network for you to attack, which allows us to teach you the core principles that you could usually gain only through real world experience.

We teach you how to implement robust security that really works, not just security 101 like configuring firewalls and setting strong passwords

The philosophy

By teaching you how to understand the attacker mindset, you'll be better equipped to make informed decisions about the security of your own network.

Our previous generation of courses guided delegates through isolated lab exercises to demonstrate tools and techniques that could be used to exploit security weaknesses. However, hacking is not just about learning to drive the tools; it's about identifying and collecting information and vulnerabilities across the target organization and leveraging them in the context of that organization.

That's why we've revamped our courses and remodelled our labs with a complete corporate infrastructure to get you as close as possible to the experience of attacking and defending a real organization.

MWR CYBERSEC

Topics / Syllabus

Foundation

- Hackers - Culture and Motives
- A History of Hacking
- The Rise of Cyber Warfare
- Advanced Persistent Threats (APTs)
- CNE and CNA
- War Stories
- The CIA Triad

Perimeter Security

- The Traditional Attack Methodology
- Reconnaissance – Information Gathering, Google Hacking
- Target Identification – Network Mapping, Port Scanning, Banner Grabbing
- Vulnerability Discovery (Manual & Automated)
- Vulnerability Scanner Limitations
- Common Vulnerabilities
  - Configuration, Patching and Passwords
- Hacking JBoss
- Hacking SMTP Servers
- Hacking Web Apps
  - SQL Injection, Code Execution
- Network Perimeter Hardening

Windows Security

- The Modern Attack Methodology
- APT Mind-Set and Capabilities
- Spear-Phishing, Drive -By Download and Watering-Hole Attacks
- Botnets
- Exploiting Java, Adobe Flash and Other Browser Plugins
- Exploiting Microsoft Word and Adobe Reader
- Bypassing Antivirus
- Maintaining Persistence and Rootkits
- Windows Privilege Escalation
- Key Logging and Screen Capture
- Hacking Windows Domains (Server 2012)
- Cracking Windows Password Hashes
- Abusing Windows Access Tokens
- Buffer Overflows
- Data Exfiltration (CNE)
- Windows Network Hardening

Network Security

- DNS Cache Poisoning, Spoofing and DoS
- Sniffing / Intercepting Network Traffic
- Man-in-the-Middle (MitM) Attacks and ARP Cache Poisoning
- Transport Encryption Flaws
  - SSL/TLS, etc.
- Hacking Vulnerable Cisco Kit
- VLAN Hopping
- Bypassing Router Access Controls
- Network Device Hardening

Unix Security

- Unix File Permissions
- Hacking Traditional Unix Services
  - XServer and R* Services, etc.
- Hacking Common Unix Services
  - SSH, NFC, etc.
- Hacking Popular Unix Platforms
  - RedHat, Solaris, etc.
- Unix Privilege Escalation
- Cracking Unix Password Hashes
- Denial of Service
- Network Sabotage (CNA)

Integrating Security

- The Death of the Perimeter
- Defending Against Client-Side Attacks
- Workstation Hardening
- Compliance Auditing
- Preventing Lateral Movement
- Windows Domain Hardening
- Server Hardening
- Secure Network Design Techniques
- Jumping Air Gaps
- An Introduction to Intrusion Detection
- Signature vs Anomaly Based Detection

For more information visit www.mwrcybersec.com or email us on info@mwrcybersec.com