Penetration Testing & Network Exploitation Labs

Course: **00097**
Filter: **Beginner**
Duration: **2 days**
Category:: **Netwoking**
Price: **2500,00 €**

About Course

Learn the security techniques used by the Internet's most skilled professionals. This Pentesting & Network Exploitation lab bundle, which includes 4 distinct, hands-on labs, will provide you with an introduction to all manner of reconnaissance, scanning, enumeration, exploitation and pillaging for 802.3 networks. This lab bundle aligns with the learning objectives found in Course 537, Penetration Testing Training: Tools and Techniques.

What you'll learn

- Complete all manner of reconnaissance, scanning, enumeration, exploitation and pillaging for 802.3 networks
- Simulate an insider threat and escape restricted environments by abusing native services and functionalityHost target analysis on Linux and Windows systems

Pre-requisites

- None

Curriculum

Module 1: Linux Target Analysis Labs

- Using Linux

- More Linux
- IP Tables
- Custom Password Creation with Crunch

Module 2: Windows Target Analysis Labs

- Using DOS
- Using PowerShell
- Leveraging PowerShell

Module 3: LAN Exploitation Labs

- Scanning LAN Segment
- Verifying Scan Data through Banner Grabbing
- Target Host Enumeration
- Exploiting Linux Hosts
- Web Application Mapping, Discovery and Exploitation with BurpSuite & Nikto
- Windows Restricted Desktop Escape & Exploitation: Students will break into a Windows 7 desktop computer using standard windows tools.

Module 4: WAN/DMZ Exploitation & Pivoting Labs

- Scan Web Facing Target IP
- Web Application Scanning
- Web Application Spidering with BurpSuite
- SSH Exploitation
- Scan & Exploit Internal Segment
- Covering Tracks
- Final Challenges