Penetration Testing Training Tools and Techniques

Course: **00098**
Filter: **Beginner**
Duration: **4 days**
Category:: **Netwoking**
Price: **3000,00 €**

About Course

In this Penetration Testing training course, you learn how hackers compromise operating systems and evade antivirus software. You will learn to discover weaknesses in your own network by using the same mindset and methods as hackers. You then acquire the skills to test and exploit your defenses and implement countermeasures to reduce risk in your enterprise.

What you'll learn

- Deploy ethical hacking to expose weaknesses in your organization
- Gather intelligence by employing reconnaissance, published data, and scanning tools
- Test and improve your security by compromising your network using hacking tools

Pre-requisites

- Course Information Security Training,
- Course : CompTIA Security+® Training.
- Reinforce your pen-testing skills with CYBRScore Lab Bundles: Penetration Testing & Network Exploitation Labs.

Curriculum

Module 1: Introduction to Ethical Hacking

- Defining a penetration testing methodology
- Creating a security testing plan

Module 2: Footprinting and Intelligence Gathering

- Acquiring target information
- Scanning and enumerating resources

Module 3: Identifying Vulnerabilities

- Correlating weaknesses and exploits
- Leveraging opportunities for attack

Module 4: Attacking Servers and Devices to Build Better Defenses

- Bypassing router Access Control Lists (ACLs)
- Compromising operating systems
- Subverting web applications

Module 5: Manipulating Clients to Uncover Internal Threats

- Baiting and snaring inside users
- Manipulating internal clients
- Deploying the social engineering toolkit

Module 6: Exploiting Targets to Increase Security

- Initiating remote shells
- Pivoting and island–hopping
- Pilfering target information
- Uploading and executing payloads

Module 7: Testing Antivirus and IDS Security

- Masquerading network traffic

- Evading antivirus systems

Module 8: Mitigating Risks and Next Steps

- Reporting results and creating an action plan
- Managing patches and configuration
- Recommending cyber security countermeasures