

PEN101

Network Ethical Hacking and Penetration Testing

Description

This course prepares you to be a professional ethical hacker and penetration tester who is able to conduct comprehensive and complete penetration testing either for your own organizations or for your clients. The course covers in depth techniques and methodologies, along with state-of-the-art tools, for a high-quality ethical hacking engagement. The course starts with pre-engagement preparatory works, then, it dives into reconnaissance, where you will learn how to build an information profile of your target. After that, you will learn advanced network scanning and vulnerability assessment methods. Then, you will be taught how you can effectively exploit vulnerable systems and maintain access. Furthermore, you will learn all the technical details of password cracking. Finally, and in addition to all the previous skills, you will learn how to break wireless networks.

The uniqueness of this course is that it combines theoretical knowledge with practical hand-on labs. Students will learn about the theories of vulnerabilities and exploitations, in addition, they will practice all the techniques of a standard penetration testing in labs simulating real-world scenarios. In addition, each student will get an e-book as a course material covering all topics. At the end of the course, the students become confident at utilizing the best cyber security and hacking tools in the industry.



Outline

- **MODULE 01** INTRODUCTION TO PENETRATION TESTING
- **MODULE 02** PRE-ENGAGEMENT PREPARATION
- **MODULE 03** INTELLIGENCE GATHERING
- **MODULE 04** NETWORK TRAFFIC MANIPULATION
- **MODULE 05** NETWORK MAPPING AND SCANNING
- **MODULE 06** VULNERABILITY ANALYSIS
- **MODULE 07** EXPLOITATION
- **MODULE 08** POST-EXPLOITATION
- **MODULE 09** PASSWORD CRACKING
- **MODULE 10** HACKING WIRELESS NETWORK

Hands-On Labs

- Traffic Analysis with Wireshark & Tcpdump
- Man-in-the-Middle using Arpspoof, Ettercap, and SSLStrip
- Network Mapping using Nmap
- VA using OpenVAS and Nessus
- Exploitation using Metasploit and Meterpreter
- Password Cracking using John, Cain, and Hydra
- Wireless Assessment using Aircrack-ng

Duration

- 30 Hours total
- Delivered in 5 or 10 days.

Who Should Attend

- IT Engineers/Managers
- Network Administrator
- Network Security Engineers
- Security Professionals

Requirement

- Laptop

Courseware

- Student Manual
- Virtual Machines (VMs) + Tools