Penetration Testing Course

for Students

Syllabus

The Penetration Testing Course for Student is divided into two main section:

- Preliminary Skills
- Penetration Testing

Every chapter in the above sections contains:

- Interactive slides (650)
- Video training (total 3 hours of video training)
- Self assessment quizzes
- Practical exercises (where possible)
- References and books for further studies

All examples, videos and exercises are based on Backtrack 4.

A Lab module will allow the student to set up a lab environment with Backtrack 4 and a vulnerable virtual machine.

1. Preliminary Skills

1.1. Understanding the Penetration Testing Process

1.1.1. How penetration testers work

1.2. Vulnerability Assessment

1.2.1. Tools:

1.2.1.1. Nessus

1.3. Technical Background

1.3.1. Networking

1.3.1.1. Packets

1.3.1.2. IP Address

1.3.1.3. Routing

1.3.1.4. Forwarding

1.3.1.5. ARP

1.3.1.6. TCP

1.3.1.7. UDP

1.3.1.8. Firewalls

1.3.1.9. Wireshark

1.3.1.9.1. Wireshark configuration

1.3.1.9.2. Exercises: Studying networking with Wireshark

1.3.2. Web Applications

1.3.2.1. HTTP Protocol basics

1.3.2.2. Cookies

1.3.2.3. Sessions

1.3.2.4. Same Origin

1.3.2.5. Study web applications and http with Burp Suite

2. Penetration Testing

2.1. Information Gathering

2.1.1. Open Source Information Gathering

2.2. Footprinting & Scanning

2.2.1. Mapping The Remote Network

2.2.2. OS Fingerprinting with nmap

2.2.3. Port Scanning

2.2.3.1. *Nmap*

2.3. Attacks & Exploitation

2.3.1. Malware

2.3.1.1. *Virus*

2.3.1.2. *Trojan Horses*

2.3.1.3. *Rootkit*

2.3.1.4. *Bootkit*

2.3.1.5. *Backdoors*

2.3.1.6. *Adware*

2.3.1.7. *Spyware*

2.3.1.8. *Greyware*

2.3.1.9. *Dialer*

2.3.1.10. *Key-logger*

2.3.1.11. *Botnet*

2.3.1.12. *Ransomware*

2.3.1.13. *Data-Stealing Malware*

2.3.1.14. *Worm*

2.3.2. XSS

2.3.2.1. *Finding vulnerable websites*

2.3.2.2. *Reflected XSS*

2.3.2.3. *Persistent and XSS*

2.3.2.4. *Exploitation*

2.3.3. Password Cracking

2.3.3.1. *Brute Force Attack*

2.3.3.2. ***Dictionary Attack***

2.3.3.3. ***Using Hydra and John the ripper to crack passwords***

2.3.4. Breaking into Windows machines with Null Sessions

2.3.4.1. Exploiting Null Sessions with Windows tools

2.3.4.1.1. Net, Nbtstat, Enum, Winfo

2.3.4.2. Exploiting Null Sessions with Linux tools

2.3.5. Web Servers

2.3.5.1. ***Fingerprinting***

2.3.5.1.1. Netcat

2.3.5.1.2. HttpRecon

2.3.5.2. ***Exploiting misconfigurations***

2.3.5.2.1. Finding hidden files

2.3.5.2.2. Uploading PHP shells

2.3.5.2.3. Using Google Hacking to discover hidden files

2.3.6. Buffer Overflows

2.3.6.1. ***Understanding Buffer overflow and the stack***

2.3.6.2. ***Exploitation***

2.3.7. Guide to Metasploit 3.6

2.3.8. SQL Injection

2.3.8.1. ***Understanding SQL injection***

2.3.8.2. ***Finding SQL injections in websites***

2.3.8.3. ***Retrieve data from remote databases through:***

2.3.8.3.1. Sqlninja

2.3.8.3.2. sqlmap

eLearnSecurity

Information Security Training Solutions

eLearnSecurity is a global Information Technology Security Training Solutions provider, catering to Government bodies, Educational Institutions and IT Security Professionals around the world.

Website: http://www.elearnsecurity.com

E-mail: contactus@elearnsecurity.com

Phone: +39 050 574113

Address: **Head Office**

Pisa, Italy