The Best First for Beginners who want to become Penetration Testers

eLearnSecurity
Forging security professionals

PTSv2 in pills:

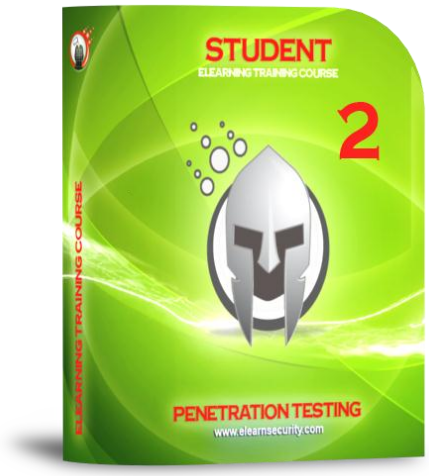
- Self-paced, online, flexible access
- 900+ interactive slides and 3 hours of video material
- Interactive and guided learning
- No Pre-requisites
- Jargon-free material
- Learn Networking
- Integrated with Hera Lab
- Learn C++
- Learn Python
- Network attacks
- Web Application attacks
- Prepares for the Professional course
- Self-assessment quizzes

This training course has been chosen by students in 103 countries in the world and by leading organization such as:

DELL U.S. AIR FORCE at&t verizon intel

Penetration Testing Course - Student Version 2.0

SYLLABUS



Course Goals

The Penetration Testing course Student v2 is the self-paced training course built for anyone with little to no background in IT Security wanting to enter the Penetration testing field.

It builds strong foundations by giving theoretical lessons enforced with practical exercises to be held in the most sophisticated virtual labs in the world.

At the end of the training, the student will possess the fundamental skills and practical pentesting knowledge to perform basic security audits.

The Student v2 course has been conceived as a first step into Penetration testing and prepares for the Penetration Testing course Professional where more advanced topics and labs are available.

Course Organization

The training course is totally self-paced with interactive slides and video material that the student can access online without any limitation, at any time in the future.

The student can study from home, office or everywhere an internet connection is available.

It is always possible to resume studying from the last slide or video accessed.

At the end of every chapter a self-assessment quiz is available to ensure the comprehension of the topics covered before moving with the next learning module.

The course Student v2 is integrated with Hera Lab. A minimum amount of 30 Hours is advised. For more intensive use, 60 Hours might be necessary.

Organization of Contents

The Penetration Testing course Student v2 is divided into two main sections. The first: Preliminary skills. The second: Penetration testing.

The student is provided with a suggested learning path to ensure the maximum success rate and the minimum effort.

Section 1: Preliminary skills

Too many Penetration Testers lack some basic fundamental skills. They are not programmers or they are not too much into networking. This section ensures that the beginner starts with building strong foundations before moving into Penetration testing topics.

The very first thing a beginner should have clear is the answer to these simple questions: Who is a Penetration tester? How does he perform its tasks? What methodology does he follow?

You will also learn the differences between Penetration Testing and Vulnerability Assessment, two often misunderstood terms.

In the Technical Background area you will start reinforcing your skills about Networking, Web Applications and Programming.

In the beginning you will study networking protocols with many practical examples and exercises to perform in our labs.

1. Preliminary skills

- 1.1. **Understanding the Penetration Testing Process**
  - 1.1.1. How Penetration testers work
- 1.2. **Vulnerability Assessment**
  - 1.2.1.1. Tools
    - 1.2.1.1.1. Nessus
    - 1.2.1.1.2. **Practical Lab in Hera**
- 1.3. **Technical Background**
  - 1.3.1. **Networking**
    - 1.3.1.1.1. Packets
    - 1.3.1.1.2. IP Addresses
    - 1.3.1.1.3. Routing
    - 1.3.1.1.4. **Practical Lab in Hera**
    - 1.3.1.1.5. Forwarding

1.3.1.1.6. ARP
1.3.1.1.7. TCP
1.3.1.1.8. UDP
1.3.1.1.9. Firewalls
1.3.1.1.10. Using Wireshark
1.3.1.1.10.1. Configuration
1.3.1.1.10.2. Exercises : Studying networking with Wireshark
1.3.1.1.11. **Practical Lab in Hera**

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 Policy
1.3.2.5. Study Web Apps and HTTP with Burp Suite
1.3.2.6. **Practical Lab in Hera**

1.3.3. **Programming**
1.3.3.1. **C++**
1.3.3.1.1. DevCPP
1.3.3.1.2. Structure of C++ Programs
1.3.3.1.3. Variables and types
1.3.3.1.4. I/O with C++
1.3.3.1.5. Operators
1.3.3.1.6. Conditional structures
1.3.3.1.7. Pointers
1.3.3.1.8. Arrays
1.3.3.1.9. Functions
1.3.3.2. **Python**
1.3.3.2.1. IDLE and Python shell
1.3.3.2.2. Variables and types
1.3.3.2.3. I/O with Python
1.3.3.2.4. Control Flow
1.3.3.2.5. Lists
1.3.3.2.6. Dictionaries
1.3.3.2.7. Functions
1.3.3.2.8. Modules
1.3.3.2.9. Scripting for Pentesters
1.3.3.2.9.1. Network Sockets
1.3.3.2.9.2. Creating a Client-Server application
1.3.3.2.9.3. Creating a Port Scanner with Python
1.3.3.2.9.4. Creating a Backdoor in Python
1.3.3.2.9.5. Working with HTTP from Python
1.3.3.2.9.6. Enumerating HTTP methods with Python

Hera Labs are included in this module
All source codes of exercises are given for download

Section 2: Penetration Testing

Penetration Testing methodologies and attack techniques explained jargon-free and with a proven learning path to ensure the student understands every technique in depth.

The student will be exposed to a proven Penetration testing methodology in different phases: from Information gathering through Footprinting & Scanning up to the Exploitation phase.

The student will become familiar with typical Infrastructural and Web based attacks with real world examples explained step by step and with practical exercises in our virtual labs.

Metasploit 4.5 will be used to perform remote exploitation against an FTP server.

2. Penetration Testing

- 2.1. **Information Gathering**
  - 2.1.1. Open Source Information Gathering
- 2.2. **Footprinting & Scanning**
  - 2.2.1.1. Mapping the remote network
  - 2.2.1.2. OS Fingerprinting with nmap
  - 2.2.1.3. Port scanning
    - 2.2.1.3.1. Nmap
    - 2.2.1.3.2. **Practical Lab in Hera**
- 2.3. **Attack & Exploitation**
  - 2.3.1. **Malware**
    - 2.3.1.1. Viruses
    - 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. Keylogger
    - 2.3.1.11. Botnet
    - 2.3.1.12. Ransomware
    - 2.3.1.13. Data-stealing Malware
    - 2.3.1.14. Worms
  - 2.3.2. **XSS**
    - 2.3.2.1. Finding vulnerable websites
    - 2.3.2.2. Reflected XSS
    - 2.3.2.3. Persistent XSS

2.3.2.4. Exploiting XSS
2.3.2.5. **Practical Lab in Hera**
2.3.3. **Password Cracking**
2.3.3.1. Brute Force Attacks
2.3.3.2. Dictionary Attacks
2.3.3.3. Using Hydra and John the ripper to crack passwords
2.3.3.4. **Practical Lab in Hera**
2.3.4. **Breaking into Windows machines with Null Sessions**
2.3.4.1. Exploiting Nulls Sessions with Windows tools
2.3.4.1.1. Net, Nbtstat, Enum, Winfo
2.3.4.2. Exploiting Null Sessions with Linux tools
2.3.4.3. **Practical Lab in Hera**
2.3.5. **Web Servers Vulnerabilities**
2.3.5.1. Fingerprinting web servers
2.3.5.1.1. NetCat
2.3.5.1.2. HTTP Recon
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 Overflow**
2.3.6.1. Understanding Buffer Overflow and the stack
2.3.6.2. Exploiting Buffer overflows
2.3.7. **Metasploit 4.5**
2.3.7.1. **Practical Lab in Hera**
2.3.8. **SQL Injection**
2.3.8.1. Understanding SQL injection attacks
2.3.8.2. Finding SQL injections in websites
2.3.8.3. Retrieve data from remote databases
2.3.8.3.1. Sqlninja
2.3.8.3.2. Sqlmap
2.3.8.3.3. **Practical Lab in Hera**

Hera Labs are included in this section

About eLearnSecurity

Based in Pisa, Italy eLearnSecurity is a leading provider of IT security and penetration testing courses for IT professionals. eLearnSecurity advances the careers of IT security professionals by providing affordable top-level instruction. We use engaging eLearning and the most effective mix of theory, practice and methodology in IT security — all with real-world lessons that students can immediately apply to build relevant skills and keep their companies' data and systems safe. For more information, visit http://www.elearnsecurity.com.

Via Matteucci 36-38
56124 Pisa, Italy

For more information, please visit http://www.elearnsecurity.com.