SYLLABUS

PENETRATION TESTING STUDENT
VERSION 4

The best course for beginners who want to become penetration testers

eLearnSecurity
Forging security professionals

eLearnSecurity has been chosen by students in over 140 countries in the world and by leading organizations such as:

hp Microsoft intel cisco AT&T verizon U.S. AIR FORCE pwc gemalto

COURSE GOALS

The Penetration Testing Student (PTS) course is a self-paced training course built for anyone with little to no background in IT Security that wants to enter the penetration testing field.

PTS builds a strong foundation by giving theoretical lessons, reinforced with practical exercises held in the most sophisticated virtual labs in the world.

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

PTSv4 has been created as the first step into penetration testing and prepares the student for the Penetration Testing Professional course, where more advanced topics and labs are covered.

Even if you are an inspiring security analyst, SOC analyst, Incident Handler or Incident Responder, you could still benefit from PTSv4 since it will provide you with both important fundamentals and knowledge of how attackers operate.

COURSE ORGANIZATION

This training course is self-paced with interactive slides and video material that students can access online without any limitation. Students have lifetime access to the training material.

Students can study from home, the office, or wherever an Internet connection is available.

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

PTSv4 is integrated with Hera Lab, the most sophisticated virtual lab in IT Security. A minimum amount of 30 hours is advised. For more intensive use, 60 hours may be necessary. Hera Lab provides on-demand vulnerable infrastructures, where a student can practice every topic seen in the course in a dedicated and isolated environment.

WILL I GET A CERTIFICATE?

The PTS course leads to the eJPT certification.

At the end of the course, students can test their skills on the eJPT exam. This practical exam will assess the student's skills on every topic covered in the course.

An eJPT certification proves that the student has all the prerequisites to enroll in our Penetration Testing Professional course.

ORGANIZATION OF CONTENTS

SECTION 1: PRELIMINARY SKILLS - PREREQUISITES

For a novice, entering the information security field can be overwhelming. They do not know what the career paths are, and professionals tend to use a lot of jargon. Moreover, being an information security professional means having a strong technical background and a deep understanding of the penetration testing process.

The *Preliminary skills - Prerequisites* section introduces students to information security, giving them all the foundational skills on computer networks, protocols, web applications, and the penetration testing process.

Through theoretical and hands-on sessions, students will be exposed to the technical aspects of systems, networks, and applications. They will also gain a deep understanding of the differences between hacking, vulnerability assessment, and penetration testing.

Several labs accompany this section, and each comes with an extensive PDF manual that will first guide the student through the lab, followed by the solutions portion which will explain and show how results were attained for the hands-on exercises.

This section is comprised of 4 modules:

- Module 1: Introduction
- Module 2: Networking
- Module 3: Web Applications
- Module 4: Penetration Testing

SECTION 2: PRELIMINARY SKILLS - PROGRAMMING

Performing a penetration test means attacking software and systems. Understanding and mastering basic programming techniques not only make Pentesters better professionals but also helps in automating tests and attacks. Being able to understand and write code is an extremely powerful weapon in every Pentesters arsenal.

- Module 1: Introduction
- Module 2: C++
- Module 3: Python
- Module 4: Command Line Scripting

SECTION 3: PENETRATION TESTING

This section covers the most important technical aspects of penetration testing with jargon-free language, following a proven learning path that ensures maximum results from the student's efforts.

Students will learn techniques, tools, and a professional penetration testing methodology. This section covers different phases from information gathering through footprinting, as well as scanning and vulnerability assessment, up to the exploitation phase.

Students will become familiar with typical infrastructural and web-based attacks, with real-world examples explained step-by-step.

Students will practice each theoretical topic covered in this section of the course by pentesting real applications and enterprise systems within the safe, isolated environments of Hera Lab; this will provide them with the confidence and experience required to perform a real penetration test.

Students will use modern tools and techniques such as Metasploit, Meterpreter, Burp Suite, Nmap, John the Ripper, and many more. Every tool presented is explained and analyzed during the course. Additionally, theory and techniques behind every tool are explained, making students not merely users of a tool, but professionals able to fully leverage their arsenal of tools.

Every chapter provides a "How does this support my pentester career" slide, explaining how studied topics can be used during a real-world pentesting engagement.

This section contains 7 modules:

- Module 1: Information Gathering
- Module 2: Footprinting and Scanning
- Module 3: Vulnerability Assessment
- Module 4: Web Attacks
- Module 5: System Attacks
- Module 6: Network Attacks
- Module 7: Next Steps

MODULE 1: INTRODUCTION

In this module, the student will initially be introduced to the field of information security and then move on to studying how cryptography and virtual private networks work, with the module closing out with a chapter on binary arithmetic; this module provides students with the required background to connect to Hera Lab for the first time and perform their first hands-on lab.

1. Introduction
- **1.1. Welcome**
  - 1.1.1. Course Structure
  - 1.1.2. Slides
  - 1.1.3. Videos
  - 1.1.4. Virtual Labs
  - 1.1.5. Good Luck!
- **1.2. The Information Security Field**
  - 1.2.1. InfoSec Culture
  - 1.2.2. Career Opportunities
  - 1.2.3. Information Security Terms
    - 1.2.3.1. White Hat Hacker
    - 1.2.3.2. Black Hat Hacker
    - 1.2.3.3. Users and Malicious Users
    - 1.2.3.4. Root or Administrator
    - 1.2.3.5. Privileges
    - 1.2.3.6. Security through Obscurity
    - 1.2.3.7. Attack
    - 1.2.3.8. Privilege Escalation
    - 1.2.3.9. Denial of Service
    - 1.2.3.10. Remote Code Execution
    - 1.2.3.11. Shell Code
- **1.3. Cryptography and VPNs**
  - 1.3.1. Clear-text Protocols
  - 1.3.2. Cryptographic Protocols
  - 1.3.3. Virtual Private Networks
- **1.4. Wireshark Introduction**
  - 1.4.1. Video – HTTP and HTTPS Traffic Sniffing
  - 1.4.2. Hera Lab – HTTP and HTTPS Traffic Sniffing
- **1.5. Binary Arithmetic Basics**
  - 1.5.1. Decimal and Binary Bases
  - 1.5.2. Converting from and to Binary
    - 1.5.2.1. Converting from Binary Example

MODULE 2: NETWORKING

Computer networks are what make the Internet work, and they are a fundamental asset for nearly every business. Understanding networking protocols means being able to spot misconfigurations and vulnerabilities. Furthermore, a penetration tester with strong networking fundamentals can properly configure tools and scanners to obtain the best results.

In this module, students will study how networking devices and protocols work. Everything is explained jargon-free. Topics and concepts are introduced gradually, making sure that students have all the information they need before studying a new topic.

This module also covers devices and protocols at different OSI layers: TCP, IP, DNS, firewalls, intrusion detection/prevention systems. Students will also study how to capture network traffic and analyze it using Wireshark.

2. Networking
- **2.1. Protocols**
  - 2.1.1. Packets
    - 2.1.1.1. Example – The IP Header
  - 2.1.2. Protocol Layers
  - 2.1.3. ISO/OSI
  - 2.1.4. Encapsulation
- **2.2. IP**
  - 2.2.1. IPv4 Addresses
  - 2.2.2. Reserved IP Addresses
  - 2.2.3. IP/Mask
    - 2.2.3.1. IP/Mask CIDR Example
    - 2.2.3.2. IP/Mask Host Example
  - 2.2.4. Network and Broadcast Addresses
  - 2.2.5. IP Examples
  - 2.2.6. Subnet Calculators
  - 2.2.7. IPv6
    - 2.2.7.1. IPv6 Header
    - 2.2.7.2. IPv6 Forms
    - 2.2.7.3. IPv6 Reserved Addresses
    - 2.2.7.4. IPv6 Structure
    - 2.2.7.5. IPv6 Scope
    - 2.2.7.6. IPv6 Translation
    - 2.2.7.7. IPv6 Subnets

MODULE 3: WEB APPLICATIONS

Web Applications are more complex and pervasive than what many think; this module explains the protocols and technologies behind web applications and prepares students for web application penetration testing topics. Students will learn how to study a web application and use the information collected to mount attacks.

3. Web Applications
- **3.1. Introduction**
- **3.2. HTTP Protocol Basics**
  - 3.2.1. HTTP Requests
  - 3.2.2. HTTP Responses
  - 3.2.3. HTTPS
  - 3.2.4. Video – HTTP and HTTPS Protocol Basics
  - 3.2.5. References
- **3.3. HTTP Cookies**
  - 3.3.1. Cookies Format
  - 3.3.2. Cookies Handling
  - 3.3.3. Cookie Domain
    - 3.3.3.1. Cookie Domain Examples
  - 3.3.4. Cookie Path
  - 3.3.5. Cookie Expires Attribute
  - 3.3.6. Cookie Http-only Attribute
  - 3.3.7. Cookie Secure Attribute
  - 3.3.8. Cookie Content
  - 3.3.9. Cookie Protocol
- **3.4. Sessions**
  - 3.4.1. Session Example
  - 3.4.2. Session Cookies
    - 3.4.2.1. Session Cookie Example
  - 3.4.3. GET Requests
  - 3.4.4. Video – HTTP Cookies and Sessions
- **3.5. Same Origin Policy**
  - 3.5.1. HTML Tags
- **3.6. Burp Suite**
  - 3.6.1. Intercepting Proxies
    - 3.6.1.1. Intercepting Proxy Example
    - 3.6.1.2. Proxy Server Example
  - 3.6.2. Burp Proxy
    - 3.6.2.1. Burp Proxy Configuration
  - 3.6.3. Burp Repeater

3.6.4. Video – Burp Suite
3.6.5. Hera Lab – Burp Suite Basics
3.6.6. Hera Lab – Burp Suite

MODULE 4: PENETRATION TESTING

In this module, we will answer fundamental questions like: Who are penetration testers? How do they perform their tasks? What methodology do they follow?

Skills and methodology are what differentiate a real professional from an amateur. This module also explains what methodology to use during an engagement, from the initial engaging phase to the final reporting and consultancy phase.

4. Penetration Testing
4.1. Introduction
4.2. Lifecycle of a Penetration Test
4.2.1. Engagement
4.2.1.1. Quotation
4.2.1.2. Proposal Submittal
4.2.1.3. Staying in Scope
4.2.1.4. Incident Handling
4.2.1.5. Legal Work
4.2.2. Information Gathering
4.2.2.1. General Information
4.2.2.2. Understanding the Business
4.2.2.3. Infrastructure Information Gathering
4.2.2.4. Web Applications
4.2.3. Footprinting and Scanning
4.2.3.1. Fingerprinting the OS
4.2.3.2. Port Scanning
4.2.3.3. Detecting Services
4.2.4. Vulnerability Assessment
4.2.5. Exploitation
4.2.6. Reporting
4.2.6.1. The Report
4.2.6.2. Consultancy
4.2.7. The Secret of an Effective Pentest

MODULE 1: INTRODUCTION TO PROGRAMMING

This module explains the basic concepts of programming and typical programming constructs. Every programming language is similar to each other in some ways. This module shows those universal similarities, as well as what programming is used for in general.

1. **Introduction to Programming**
   - **1.1. What is Programming**
   - **1.2. Low and High-Level Languages**
   - **1.3. Programming vs. Scripting**
   - **1.4. Basic Concepts**
     - 1.4.1. Variables
     - 1.4.2. Functions
     - 1.4.3. Conditional Statements
     - 1.4.4. Loops
     - 1.4.5. Understanding the Code
   - **1.5. Conclusion**

MODULE 2: C++

This module explains the basics of C++. C++ uses some features that are typical for this language, like pointers or predefined variables. At the end of the module, students can test their knowledge building a simple remote data stealing tool using C++.

2. **C++**
   - **2.1. C++ IDE**
   - **2.2. Structure of C++ Programs**
   - **2.3. Variables and Types**
   - **2.4. Input / Output**
   - **2.5. Operators**
   - **2.6. Iteration & Conditional Structures**
   - **2.7. Pointers**
   - **2.8. Arrays**
   - **2.9. Functions**
   - **2.10. 2.10 Lab – C++-assisted exploitation**

MODULE 3: PROGRAMMING IN PYTHON

This module explains the basics of Python, as well as shows how to properly set up the Python development environment. Moreover, students will learn how to write simple custom pentesting tools in Python

3. Programming in Python
- **3.1. What is Python?**
- **3.2. Variables and Types**
- **3.3. Input / Output**
- **3.4. Control Flow**
- **3.5. Lists**
- **3.6. Dictionaries**
- **3.7. Functions**
- **3.8. Modules**
- **3.9. Scripting for Pentesters**
  - 3.9.1. Network Sockets
  - 3.9.2. Port Scanner
  - 3.9.3. Backdoor
  - 3.9.4. HTTP
  - 3.9.5. Login Brute Force
  - 3.9.6. Lab – Python-assisted exploitation

MODULE 4: COMMAND LINE SCRIPTING

This module explains the basics of command line scripting, as well as the environment settings for it both from a Windows and a Linux perspective. Moreover, students will learn how to automate simple everyday tasks using bash scripting.

MODULE 1: INFORMATION GATHERING

Information gathering is the most important phase of the overall pentesting engagement. A penetration tester will use the information collected during this phase to map the attack surface and increase their chances to breach the organization in the same way criminals do. Students will see how to use different sources to perform the information gathering phase.

1. Information Gathering
- **1.1. Introduction**
- **1.2. Open-source Intelligence**
  - 1.2.1. Social Networks Information Gathering
    - 1.2.1.1. LinkedIn Example
    - 1.2.1.2. Linked Social Network Profiles
  - 1.2.2. Public Sites Information Gathering
    - 1.2.2.1. CrunchBase
    - 1.2.2.2. Government Sites
  - 1.2.3. Whois
    - 1.2.3.1. Whois Example
  - 1.2.4. Browsing Client's Sites
  - 1.2.5. Discovering Email Pattern
- **1.3. Subdomain Enumeration**
  - 1.3.1 Video – Subdomain enumeration
- **1.4. The Importance of Information Gathering**

MODULE 2: FOOTPRINTING AND SCANNING

This module covers infrastructural information gathering. Remotely identifying operating systems, server applications, and clients is of paramount importance to widen the attack surface and prepare the penetration tester for the vulnerability assessment activity and the following exploitation phase.

2. Footprinting and Scanning
- **2.1. Disclaimer**
- **2.2. Mapping a Network**
  - 2.2.1. Why Map a (Remote) Network
  - 2.2.2. Ping Sweeping
    - 2.2.2.1. FPing
    - 2.2.2.2. Nmap Ping Scan
  - 2.2.3. OS Fingerprinting
    - 2.2.3.1. OS Fingerprinting with Nmap
  - 2.2.4. Video – OS Fingerprinting with Nmap
- **2.3. Port Scanning**
  - 2.3.1. Under the Hood of a Port Scanner
    - 2.3.1.1. TCP Three-Way Handshake
    - 2.3.1.2. TCP Connect Scan
    - 2.3.1.3. TCP SYN Scan
  - 2.3.2. Scanning with Nmap
    - 2.3.2.1. Nmap Scan Types
    - 2.3.2.2. TCP Connect Scan with Nmap
    - 2.3.2.3. TCP SYN Scan with Nmap
    - 2.3.2.4. Version Detection with Nmap
  - 2.3.3. Specifying the Targets
    - 2.3.3.1. By DNS Name
    - 2.3.3.2. With an IP Addresses List
    - 2.3.3.3. By Using CIDR Notation
    - 2.3.3.4. By Using Wildcards
    - 2.3.3.5. Specifying Ranges
    - 2.3.3.6. Octets Lists
    - 2.3.3.7. Combining the Previous Methods
  - 2.3.4. Choosing the Ports to Scan
  - 2.3.5. Nmap Examples
  - 2.3.6. Video – Port Scanning
  - 2.3.7. Discovering Network with Port Scanning
  - 2.3.8. Spotting a Firewall
  - 2.3.9. Masscan

2.3.9.1. Video - Masscan
2.3.10. Hera Lab – Scanning and OS Fingerprinting

MODULE 3: VULNERABILITY ASSESSMENT

Vulnerability Assessment is the process through which a penetration tester uncovers all the vulnerabilities in a computer system or application. This module explains how vulnerability assessment can be carried out using automatic tools or manual investigation.

3. Vulnerability Assessment
3.1. Vulnerability Assessment
3.1.1. Vulnerability Scanners
3.1.2. Manual Testing
3.2. Nessus
3.2.1. Architecture
3.2.2. Under the Hood of a Vulnerability Scanner
3.2.2.1. Port Scanning
3.2.2.2. Service Detection
3.2.2.3. Vulnerabilities Database Lookup
3.2.2.4. Probing
3.2.3. Video – Nessus
3.2.4. Hera Lab – Nessus

MODULE 4: WEB ATTACKS

This module dissects and explains the most widespread web application vulnerabilities. Students will study the most common web application attacks, starting from the information gathering phase to the exploitation phase. Additionally, students will learn how to perform attacks manually and then learn how to automate them by utilizing the most commonly used tools.

4. Web Attacks
- **4.1. Introduction**
  - 4.1.1. Disclaimer
- **4.2. Web Server Fingerprinting**
  - 4.2.1. Fingerprinting with Netcat
    - 4.2.1.1. Fingerprinting with Netcat Examples
    - 4.2.1.2. Common Mistakes
  - 4.2.2. Fingerprinting with OpenSSL
  - 4.2.3. Limits of Manual Fingerprinting
  - 4.2.4. Fingerprinting with Httprint
- **4.3. HTTP Verbs**
  - 4.3.1. GET
  - 4.3.2. POST
  - 4.3.3. HEAD
  - 4.3.4. PUT
  - 4.3.5. DELETE
  - 4.3.6. OPTIONS
    - 4.3.6.1. REST APIs
  - 4.3.7. Using HTTP 1.0 Syntax
  - 4.3.8. Exploiting Misconfigured HTTP Verbs
    - 4.3.8.1. Enumeration with OPTIONS
    - 4.3.8.2. Exploiting DELETE
    - 4.3.8.3. Exploiting PUT
    - 4.3.8.4. Uploading a PHP Shell with PUT
  - 4.3.9. Conclusions
  - 4.3.10. Video - Netcat
- **4.4. Directories and File Enumeration**
  - 4.4.1. Brute-force Enumeration
  - 4.4.2. Dictionary-based Enumeration
  - 4.4.3. Enumerating Web Resources with Dirbuster
    - 4.4.3.1. Video – Dirbuster
  - 4.4.4. Enumerating Web Resources with Dirb
    - 4.4.4.1. Video – Dirb

MODULE 5: SYSTEM ATTACKS

From malware, through password cracking attacks, up to buffer overflows, students will learn the most common attack vectors used against computer systems nowadays, as well as which malware they can use during an engagement.

In the Password Attacks chapter, we explain how to recover passwords from a compromised machine.

Then, we conclude this module with an entire chapter dedicated to buffer overflows, one of the most used attack vectors against applications and operating systems.

5. System Attacks
- **5.1. Malware**
  - 5.1.1. Viruses
  - 5.1.2. Trojan Horses
  - 5.1.3. Backdoors
    - 5.1.3.1. Firewalls vs. Backdoors
    - 5.1.3.2. Firewalls vs. Connect-back Backdoors
  - 5.1.4. Rootkits
  - 5.1.5. Bootkit
  - 5.1.6. Adware
  - 5.1.7. Spyware
  - 5.1.8. Greyware
  - 5.1.9. Dialer
  - 5.1.10. Keylogger
    - 5.1.10.1. Hardware Keyloggers
    - 5.1.10.2. Rootkit Keyloggers
  - 5.1.11. Bots
  - 5.1.12. Ransomware
  - 5.1.13. Data-Stealing Malware
  - 5.1.14. Worms
  - 5.1.15. Video – Backdoors
  - 5.1.16. References
- **5.2. Password Attacks**
  - 5.2.1. Brute Force Attacks
    - 5.2.1.1. Brute Force Algorithm
    - 5.2.1.2. Brute Forcing Weaknesses
    - 5.2.1.3. John the Ripper
      - 5.2.1.3.1. Unshadow
      - 5.2.1.3.2. Brute Force with John the Ripper

MODULE 6: NETWORK ATTACKS

This module provides a comprehensive explanation of the most common and historical remote attacks. Students will learn attacking techniques against authentication services, Windows file sharing, and network devices. Every attacking technique can be tested in a hands-on lab.

The last two chapters explain in theory and practice, how to use Metasploit and Meterpreter to automate attacks and penetration testing techniques.

6. Network Attacks
- **6.1. Authentication Cracking**
  - 6.1.1. Brute Force vs. Dictionary Attacks
  - 6.1.2. Weak and Default Credentials
    - 6.1.2.1. Installing Dictionaries
  - 6.1.3. Authentication Cracking Tools
  - 6.1.4. Hydra
    - 6.1.4.1. Telnet Attack Example
    - 6.1.4.2. HTTP Basic Auth Attack Example
  - 6.1.5. Video – Hydra Cracking Session
  - 6.1.6. Hera Lab – Brute Force and Password Cracking
- **6.2. Windows Shares**
  - 6.2.1. NetBIOS
  - 6.2.2. Shares
  - 6.2.3. UNC Paths
  - 6.2.4. Administrative Shares
  - 6.2.5. Badly Configured Shares
- **6.3. Null Sessions**
  - 6.3.1. Enumerating Windows Shares
    - 6.3.1.1. Nbtstat
    - 6.3.1.2. NET VIEW
    - 6.3.1.3. Nmblookup
    - 6.3.1.4. Smbclient
  - 6.3.2. Checking for Null Sessions
    - 6.3.2.1. Checking for Null Sessions with Windows
    - 6.3.2.2. Checking for Null Sessions with Linux
  - 6.3.3. Exploiting Null Sessions
    - 6.3.3.1. Exploiting Null Sessions with Enum
    - 6.3.3.2. Exploiting Null Sessions with Winfo
    - 6.3.3.3. Exploiting Null Sessions with Enum4linux
  - 6.3.4. Video – Null Sessions

- 6.3.5. About Null Sessions
- 6.3.6. Hera Lab – Null Sessions

6.4. ARP Poisoning

- 6.4.1. ARP Poisoning Actors
- 6.4.2. Gratuitous ARP Replies
- 6.4.3. Forwarding and Mangling Packets
- 6.4.4. Local to Remote Man-in-the-Middle
- 6.4.5. Dsniff Arpspoof
  - 6.4.5.1. Example – Using Arpspoof
- 6.4.6. Video – ARP Poisoning
- 6.4.7. Hera Lab – ARP Poisoning

6.5. Metasploit

- 6.5.1. MSFConsole
- 6.5.2. Identifying a Vulnerable Service
- 6.5.3. Searching
- 6.5.4. Configuring an Exploit
- 6.5.5. Configuring a Payload
- 6.5.6. Running an Exploit
- 6.5.7. Video – Metasploit
- 6.5.8. Lab - Metasploit

6.6. Meterpreter

- 6.6.1. Bind and Reverse
- 6.6.2. Launching Meterpreter
- 6.6.3. Sessions
- 6.6.4. Information Gathering with Meterpreter
  - 6.6.4.1. System Information
  - 6.6.4.2. Network Configuration
  - 6.6.4.3. Routing Information
  - 6.6.4.4. Current User
- 6.6.5. Privilege Escalation
  - 6.6.5.1. Bypassing UAC
- 6.6.6. Dumping the Password Database
- 6.6.7. Exploring the Victim System
- 6.6.8. Uploading and Downloading files
- 6.6.9. Running an OS Shell
- 6.6.10. The Help
- 6.6.11. Video – Meterpreter
- 6.6.12. Video – Beyond Remote Code Execution (RCE)
- 6.6.13. Video – Shells

MODULE 7: NEXT STEPS

This module is a summary of the course. It contains useful advice and information about how to continue learning in the field of IT Security in the most efficient way. Also, students can test their skills against special lab challenges, which are very similar to real-life penetration testing scenarios.

7. Next Steps

7.1 Preparing for the exam

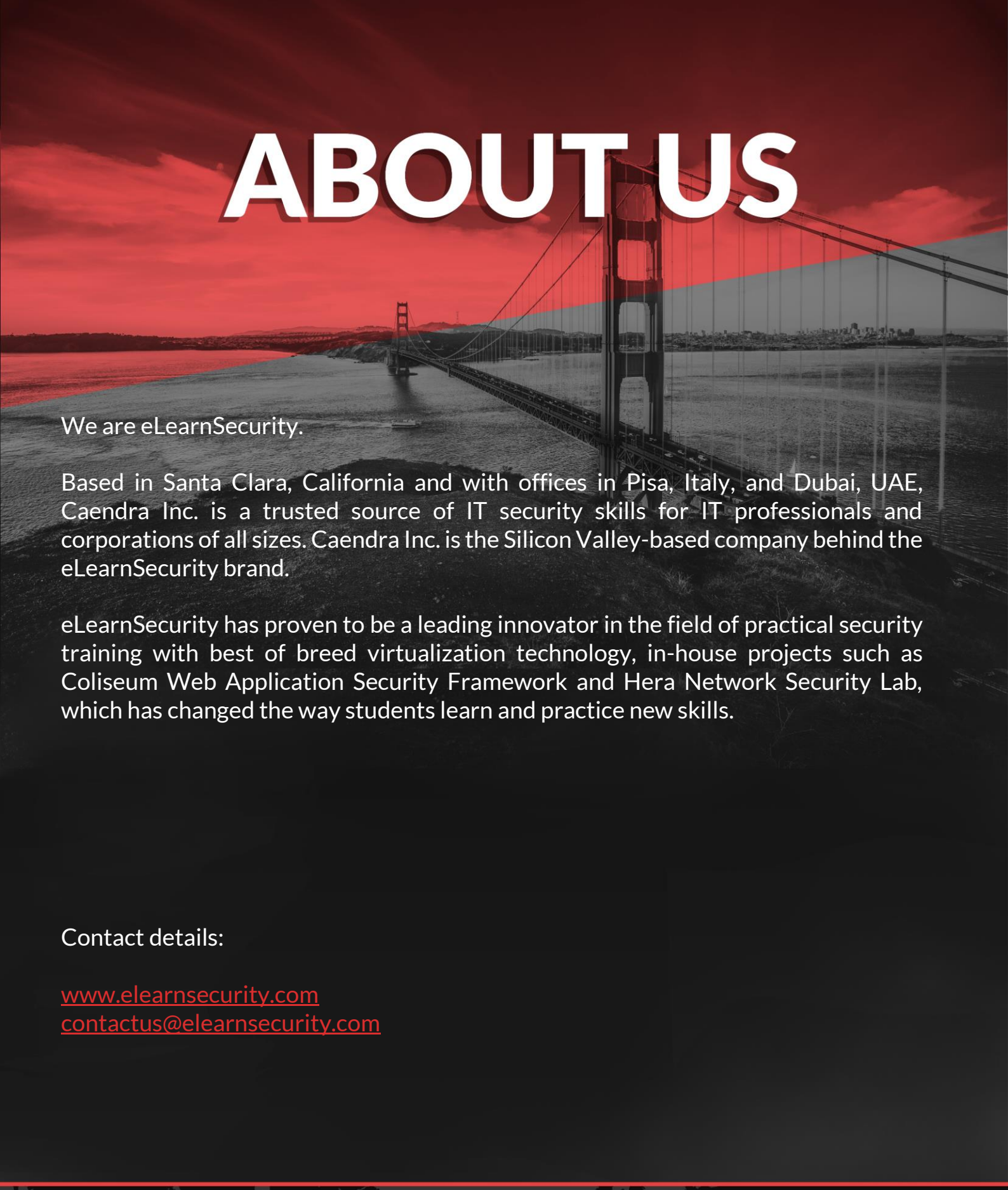
7.1.1.1 Preparing for the exam
7.1.1.2. Lab – Black-box Penetration Test #1
7.1.1.3. Lab – Black-box Penetration Test #2
7.1.1.4. Lab – Black-box Penetration Test #3
7.1.2. Taking the eJPT
7.1.3. Staying Connected

7.2. Penetration Testing Approach

7.3. Career Paths

7.4. Beyond PTS

ABOUT US



We are eLearnSecurity.

Based in Santa Clara, California and with offices in Pisa, Italy, and Dubai, UAE, Caendra Inc. is a trusted source of IT security skills for IT professionals and corporations of all sizes. Caendra Inc. is the Silicon Valley-based company behind the eLearnSecurity brand.

eLearnSecurity has proven to be a leading innovator in the field of practical security training with best of breed virtualization technology, in-house projects such as Coliseum Web Application Security Framework and Hera Network Security Lab, which has changed the way students learn and practice new skills.

Contact details:

www.elearnsecurity.com
contactus@elearnsecurity.com

2040 Martin Ave.
Santa Clara, CA, USA

Via Gian Battista Queirolo
Pisa, Italy

Apricot Tower, Dubai Silicon Oasis
Dubai, UAE