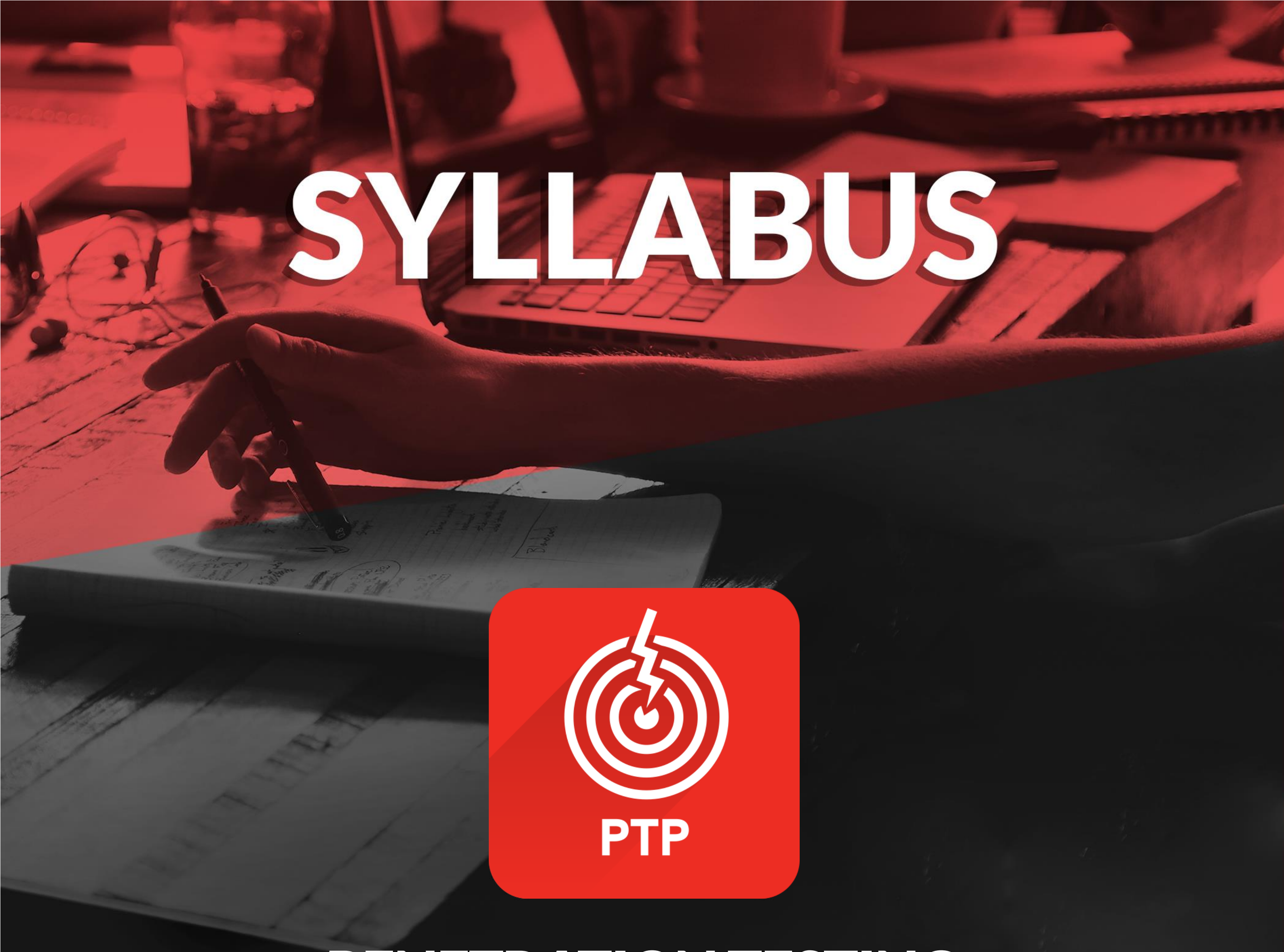


SYLLABUS

PTP

PENETRATION TESTING PROFESSIONAL
VERSION 5

The world's premier online penetration testing course

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 security to be free

COURSE GOALS

The Penetration Testing Professional (PTP) course is the most practical and comprehensive course on Penetration Testing. An online, self-paced training course built with the goal of creating knowledgeable IT security professionals.

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

At the end of the training course, the student will be challenged with a real-world exam environment, where he/she must produce a commercial-grade penetration testing report that correctly identifies the weaknesses in this "engagement."

COURSE ORGANIZATION

The training course is totally 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, office, or wherever an internet connection is available. It is always possible to resume studying from the last slide or video accessed.

The PTP course is integrated with Hera Lab: the most sophisticated virtual lab in IT Security. A minimum amount of 60 hours is advised. For more intensive use, 120 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.

All modules come in slides (HTML5), plus video format and PDFs. Modules can be accessed from within the eLearnSecurity Members Area.

Labs are also referenced within the slides in order to suggest the correct learning path to follow.

TARGET AUDIENCE AND PRE-REQUISITES

The PTP training course benefits those looking to move into a career as a professional penetration testers or IT Security personnel whose job is dependent on their ability to defend their organization.

This course allows organizations of all sizes to assess and mitigate the risk at which their infrastructure and web applications are exposed by building strong, practical in-house skills.

Penetration testing companies can train their teams with a comprehensive and practical training course without having to deploy internal labs that are often outdated and not backed by solid theoretical material.

The student willing to enroll in the course must possess a solid understanding of operating systems, web applications and web application security models.

No programming skills are required. However, a basic understanding of networks, internet protocols, IT security issues, and penetration testing concepts, as well as the ability to read and understand code will greatly reduce the learning curve of a student.

WILL I GET A CERTIFICATE?

The PTP course leads to the eCPPT v2 certification.

The certification can be obtained by successfully completing the requirements of the practical exam, which consists of a penetration test of a real-world network that is hosted in our eLearnSecurity Hera Labs.

An eCPPT voucher is included in all the plans of the PTP course.

ORGANIZATION OF CONTENTS

SYSTEM SECURITY

The System Security section will provide you with a thorough understanding of x86 Architecture and its weaknesses.

- Module 1: Architecture Fundamentals
- Module 2: Assembler Debuggers and Tool Arsenal
- Module 3: Buffer Overflow
- Module 4: Shellcoding
- Module 5: Cryptography and Password Cracking
- Module 6: Malware

NETWORK SECURITY

The Network Security section will cover security testing methodology, techniques, and tools for networked PC and devices.

- Module 1: Information Gathering
- Module 2: Scanning
- Module 3: Enumeration
- Module 4: Sniffing and MITM Attacks
- Module 5: Vulnerability Assessment & Exploitation
- Module 6: Post-Exploitation
- Module 7: Anonymity
- Module 8: Social Engineering

POWERSHELL FOR PENTESTERS SECTION

PowerShell is a powerful built-in shell and scripting environment we can utilize as penetration testers considering its wide-spread availability on all modern Windows-based systems. The use of PowerShell allows us to take advantage of the "living-off-the-land" concept, where using tools that are built-in to the Operating System work to our advantage once we've obtained access to a system.

While studying the PowerShell for Pentesters section, you will come across the following topics:

- Module 1: Introduction
- Module 2: Powershell Fundamentals
- Module 3: Offensive Powershell

LINUX EXPLOITATION SECTION

Linux and other variants of UNIX make up a very large segment of the overall internet infrastructure (including Critical Infrastructure), not to mention the exponentially expanding "Internet of Things" ecosystem of whose devices are mostly dependent on some form of *NIX or another. Those facts make Linux an increasingly popular target.

While studying the Linux Exploitation section, you will come across the following topics:

- Module 1: Introduction
- Module 2: Information Gathering
- Module 3: Exploitation Over the Network
- Module 4: Post Exploitation

WEB APPLICATION SECURITY

Today's penetration testers must master web application attack techniques; this lab-intensive section will teach the student how to conduct a thorough Penetration test against web applications.

- Module 1: Introduction
- Module 2: Information Gathering
- Module 3: Cross-Site Scripting
- Module 4: SQL Injection
- Module 5: Other Common Web Attacks

WI-FI SECURITY SECTION

The Wi-Fi Security section is an extremely in-depth section covering the most important attack techniques used against Wi-Fi networks. The student will learn the security mechanisms implemented in Wi-Fi architectures as well as their weaknesses and how to exploit them.

- Module 1: Prerequisites

- Module 2: Environment Setup
- Module 3: Wireless Standards and Networks
- Module 4: Discover Wi-Fi Networks
- Module 5: Traffic Analysis
- Module 6: Attacking Wi-Fi Networks
- Module 7: Wi-Fi as Attack Vector

RUBY FOR PENTESTERS AND METASPLOIT SECTION

The Ruby for Pentesters and Metasploit section covers Ruby programming from the very basics to advanced techniques, in addition to penetration testing topics. This section also covers topics such as exploiting vulnerable applications with Ruby, as well as creating and editing Metasploit modules.

- Module 1: Ruby Basic: Installation and Fundamentals
- Module 2: Ruby Basic: Control Structures
- Module 3: Ruby Basic: Methods, Variables, and Scope
- Module 4: Ruby Advanced: Classes, Modules, and Exceptions
- Module 5: Ruby Advanced: Pentester Prerequisites
- Module 6: Ruby for Pentesters: Input / Output
- Module 7: Ruby for Pentesters: Network and OS interaction
- Module 8: Ruby for Pentesters: The Web
- Module 9: Ruby for Pentesters: Exploitation with Ruby
- Module 10: Ruby for Pentesters: Metasploit

MODULE 1: ARCHITECTURE FUNDAMENTALS

In this module, you will learn fundamental concepts needed to help you improve your skills in topics such as fuzzing, exploit development, buffer overflows, debugging, reverse engineering and malware analysis.

Sample source codes of C++ and Assembly language are provided in order to get the student familiar with these languages.

Hera Labs are included in this module

MODULE 2: ASSEMBLERS, DEBUGGERS AND TOOLS ARSENAL

The previous module showed you that Assembly is a very low-level programming language consisting of a mnemonic code, also known as an opcode (operation code).

Although it is a low-level language, it still needs to be converted into machine code in order for the machine to execute.

In this module, you will see how this happens and what tools are required.

MODULE 3: BUFFER OVERFLOWS

Finding and exploiting buffer overflows in real-world applications is what you will learn during this incredibly hands-on module. A hard topic made easy through examples explained step by step starting from the very basics of stack manipulation.

Armed with assemblers, compilers, and debuggers, the students will learn how to hijack the execution of an application. At the end of the module, the student is exposed to the most modern techniques used to prevent Buffer overflows and the main methods to bypass them.

3. Buffer Overflows
- **3.1. Understanding Buffer Overflows**
  - Strcpy and Strncpy
  - Samples and code observation
  - Visual Studio
  - NULL bytes
- **3.2. Finding Buffer Overflows**
  - 3.2.1. Finding Buffer Overflows in Binary Programs
  - 3.2.2. Code Observation
  - 3.2.3. Overflow the Buffer
- **3.3. Exploiting Buffer Overflows**
  - 3.3.1. Finding the right offset
    - Pattern Create
    - Pattern Offset
    - Mona
  - 3.3.2. Overwriting the EIP
- **3.4. Exploiting a Real-World Buffer Overflow**
- **3.5. Security Implementations**
  - 3.5.1. Helpful Tools
  - 3.5.2. Address Space Layout Randomization
    - 3.5.2.1. Bypass Technique
    - 3.5.2.2. Protective Measures
  - 3.5.3. Data Execution Prevention
    - 3.5.3.1. Bypass Technique
    - 3.5.3.2. Protective Measures
  - 3.5.4. Stack Canary and SafeSEH
    - 3.5.4.1. Bypass Technique
    - 3.5.4.2. Protective Measures

MODULE 4: SHELLCODING

The art of Shellcoding is made available to anyone through easy to understand samples and complex real-world scenarios. A small theoretical overview will lead into practical examples, where you will create your own shellcode using compilers and assemblers. Different techniques are shown in order to let you create your own shellcode. Three source code examples are explained line by line.

4. Shellcoding

- **4.1. Execution of a Shellcode**
- **4.2. Types of Shellcode**
  - Local
  - Remote (Connect Back, Bind, Socket Reuse)
  - Staged / Egg-hunt / Omelet
- **4.3. Encoding of Shellcode**
  - 4.3.1. NULL-free Encoding
  - 4.3.2. Alphanumeric and Printable Encoding
- **4.4. Debugging a Shellcode**
- **4.5. Creating our first Shellcode**
  - 4.5.1. Finding Function Addresses
  - 4.5.2. Creating a small ASM code
- **4.6. A more advanced Shellcode**
  - 4.6.1. String Terminator
  - 4.6.2. NULL-Free Shellcode
  - 4.6.3. Manual Editing
  - 4.6.4. Encoder tools
- **4.7. Shellcode and Payload Generators**
  - 4.7.1. Msfvenom

MODULE 5: CRYPTOGRAPHY AND PASSWORD CRACKING

Almost all penetration test engagements require the understanding of cryptographic topics. This module will ensure that you are current with the most common cryptographic technologies, algorithms, and tools.

You will also learn how to perform advanced password cracking using the best tools available.

A thorough review of the most modern tools used to steal and crack Windows password hashes is provided.

5. Cryptography & Password Cracking

- **5.1. Introduction**
- **5.2. Classification**
- **5.3. Cryptographic Hash Function**
- **5.4. Public Key Infrastructure**
- **5.5. PGP**
- **5.6. Secure Shell (SSH)**
    - 5.6.1. SSH Tunneling
- **5.7. Cryptographic attacks**
- **5.8. Security pitfalls in implementing Cryptographic Systems**
- **5.9. Windows Passwords**
    - 5.9.1. LM and NT hashes
    - 5.9.2. SAM
    - 5.9.3. Stealing hashes – Remote
    - 5.9.4. Stealing hashes – Local
    - 5.9.5. Stealing hashes – Live host
    - 5.9.6. Stealing hashes – Offline
    - 5.9.7. Pass the hash
    - 5.9.8. Cracking the hash

MODULE 6: MALWARE

Here you are provided with a thorough and detailed introduction to the classifications of malware types, explaining the most advanced and obscure techniques used by modern malware. The module is complemented by three malware source codes being dissected and explained: a Keylogger, a Trojan, and a Virus.

6. Malware
- **6.1. Classification**
- **6.2. Techniques used by Malware**
  - 6.2.1. Streams
  - 6.2.2. Hooking SSDT
  - 6.2.3. Hooking IRP
  - 6.2.4. Hiding a process
  - 6.2.5. API Hooking
    - 6.2.5.1. IAT Hooking
    - 6.2.5.2. EAT Hooking
    - 6.2.5.3. Inline Hooking
  - 6.2.6. Anti-Debugging methods
  - 6.2.7. Anti-Virtual Machine methods
  - 6.2.8. Obfuscation
  - 6.2.9. Packers
  - 6.2.10. Polymorphism
  - 6.2.11. Metamorphism
    - 6.2.11.1. Garbage Insertion
    - 6.2.11.2. Registers Exchange
    - 6.2.11.3. Permutation
- **6.3. How malware spreads**
  - 6.3.1. Null free shellcode
  - 6.3.2. Alphanumeric shellcode
  - 6.3.3. Percentage encoding
- **6.4. Real-world Samples**
  - 6.4.1. Sample 1: Keylogger
  - 6.4.2. Sample 2: Trojan
  - 6.4.3. Sample 3: Virus

MODULE 1: INFORMATION GATHERING

The Information Gathering module is the most important phase of the overall engagement. A Penetration tester will use the information collected during this phase to map the attack surface and increase his chances to breach the organization in the same way criminals do. eLearnSecurity proposes an extremely thorough investigation methodology that takes into account the Business and the Infrastructure of the client. Students will learn how to get access to valuable, sensitive and sometimes secret documents by means of free services, databases, and specialized search engines. Infrastructure Information gathering will deal with the enumeration of DNS, Domains, netblocks and other web assets belonging to the organization.

Hera Labs are included in this module. The student is also required to conduct an investigation against a real company

1. Information Gathering
- **1.1. Introduction**
- **1.2. OSINT / Search Engines**
  - 1.2.1. Organization Web Presence
  - 1.2.2. Finding government contracts
  - 1.2.3. Partners and third parties
  - 1.2.4. Job postings
  - 1.2.5. Financial information
  - 1.2.6. Information Harvesting
    - 1.2.6.1. theHarvester
  - 1.2.7. Cached information
- **1.3. OSINT / Social Media**
  - 1.3.1. People search and investigation
  - 1.3.2. Real-world information gathering against eLSFoo
- **1.4. Infrastructure information gathering**
  - 1.4.1. Domains
    - 1.4.1.1. DNS Enumeration
    - 1.4.1.2. IPs
    - 1.4.1.3. Bing
    - 1.4.1.4. Netblocks & ASs
  - 1.4.2. Netblocks
    - 1.4.2.1. Live hosts
    - 1.4.2.2. Further DNS
  - 1.4.3. Maltego

- **1.5. Tools**
  - 1.5.1. DNSdumpster
  - 1.5.2. DNSEnum
  - 1.5.3. DNSMap
  - 1.5.4. Foca & Shodan

MODULE 2: SCANNING

As one of the most important steps in the penetration test of a network, this module will first teach you the theory behind port scanning and service reconnaissance.

If you are not a network expert, the first chapters of this module will introduce you to the basics of TCP and other network protocols.

We will then show you how to use the best tools to detect live hosts, open ports, and services running on them.

Through Nmap and Hping2, you will learn how to find zombies to mount stealth port scans against a target completely.

Passive and Active OS fingerprinting techniques will also be covered in depth.

Hera Labs are included in this module

2. Scanning

- **2.1. Introduction**
  - 2.1.1. Ports, Protocol, and Services
  - 2.1.2. The Three-Way Handshake
    - 2.1.2.1. Crafting Packets
- **2.2. Detect Live Hosts and Open Ports**
  - 2.2.1. Tools
    - 2.2.1.1. Nmap
      - 2.2.1.1.1. SYN Scan
      - 2.2.1.1.2. Connect Scan
      - 2.2.1.1.3. UDP Scan
      - 2.2.1.1.4. Idle Scan
      - 2.2.1.1.5. NULL / FIN / Xmas
      - 2.2.1.1.6. ACK Scan
      - 2.2.1.1.7. IP Scan
      - 2.2.1.1.8. Nmap NSE
    - 2.2.1.2. Hping

MODULE 3: ENUMERATION

The scope of this module is to provide you with the techniques professional penetration testers employ to enumerate resources on target.

You will be able to explore, enumerate and map the remote network and its available services through a number of different Windows and Unix tools.

NetBIOS is the subject of the first part of this module: real-world examples will be explained to show most important techniques and tools to enumerate remote Windows shares and printers.

You will also learn how to test for NetBIOS Null Sessions that still affect old Windows versions.

SNMP basics will also be explained. The student will then be introduced to attacks against the protocols through a number of common tools.

3.2.4.3. Net Command

3.2.4.4. Smbclient and Mount

3.2.4.5. Null Session

3.2.4.5.1. Winfingerprint

3.2.4.5.2. Winfo

3.2.4.5.3. DumpSec

3.2.4.5.4. Enum4Linux

3.2.4.5.5. RPCClient

3.3. SNMP

3.3.1. What it is

3.3.2. How it works (Agents, MIB, OID)

3.3.3. SNMP Attacks

3.3.3.1. Enumeration

3.3.3.2. Obtaining Community Strings

3.3.3.3. SNMPWalk

3.3.3.4. SMBPSet

3.3.3.5. Nmap SNMP Scripts

MODULE 4: SNIFFING & MITM

Studying ARP, how it works and how it can be manipulated to mount sophisticated attacks is made extremely easy to understand. Sniffing is a technique that you will be able to fully grasp in its most practical aspects. We will make sure you have enough basics of network theory before we cover actual attack scenarios using the best tools available. LLMNR and NBT-NS spoofing/poisoning is also covered, including advanced scenarios leveraging the Responder toolkit. Man in the middle attacks are one of the most used penetration testing techniques today; you will be able to mount a man in the middle attacks within local networks and over the Internet.

4. Sniffing & MITM

4.1. What sniffing means

4.1.1. Why it is Possible

4.2. Sniffing in action

4.2.1. Passive Sniffing

4.2.2. Active Sniffing

4.2.2.1. MAC Flooding

4.2.2.2. ARP Poisoning

4.3. Basic of ARP

4.3.1. Gratuitous ARP

4.3.2. ARP Poisoning

MODULE 5: VULNERABILITY ASSESSMENT & EXPLOITATION

This module will teach the student how to master Nessus in order to perform thorough and targeted Vulnerability scans. Windows authentication protocols are dissected to demonstrate weaknesses and related attacks from Metasploit. The student is then immersed in common exploitation techniques used by today's Penetration testers, to exploit client-side and remote vulnerabilities in Workstations and Servers. The latest Windows remote code execution vulnerabilities are covered and combined with numerous other attacking techniques. Lastly, creating custom wordlists is another skill the student will acquire by studying this module.

It should be noted that this module is video and lab intensive.

Hera Labs are included in this module

5. Vulnerability Assessment & Exploitation

- **5.1. Vulnerability Assessment**
  - 5.1.1. Vulnerability Scanners
  - 5.1.2. Nessus
- **5.2. Low-Hanging Fruits**
  - 5.2.1. Weak Password
    - 5.2.1.1. Ncrack
    - 5.2.1.2. Medusa
    - 5.2.1.3. Patator
    - 5.2.1.4. EyeWitness
    - 5.2.1.5. Rsmangler
    - 5.2.1.6. CeWL
    - 5.2.1.7. Mentalist
- **5.3. Exploitation**
  - 5.3.1. Metasploit introduction
  - 5.3.2. Windows Authentication Weaknesses
    - 5.3.2.1. LM/NTLMv1
    - 5.3.2.2. NTLMv2
    - 5.3.2.3. SMB Relay on NTLMv1
    - 5.3.2.4. SMB Relay on NTLMv2
    - 5.3.2.5. Eternal Blue (MS17-010)
  - 5.3.3. Client-Side Exploitation
  - 5.3.4. Remote-Side Exploitation

MODULE 6: POST EXPLOITATION

eLearnSecurity's experienced instructors have come up with a proven methodology to conduct thorough exploitation of remote internal networks through advanced post-exploitation techniques. Once you are comfortable with most recent exploitation techniques, you will be exposed to the cyclic steps of a successful post-exploitation phase. This is the phase where criminals ensure stable high privileged access to the remote network in order to steal and ex-filtrate documents and credentials from the organization. Penetration testers must possess the same skill-set and tools in order to test not only the perimeter security but also any kind of internal weakness that affects the organization security. Privilege escalation through insecurely configured services, DLL hijacking, and DNS tunneling are only a small percentage of what students will learn in this module.

This is a video and hands-on intensive module.

Hera Labs are included in this module

6. Post Exploitation
- **6.1. Introduction**
  - 6.1.1. Maintaining Access and Clean-up
  - 6.1.2. Permanent Edits
- **6.2. Privilege Escalation and Maintaining Access**
  - 6.2.1. Privilege Escalation
    - 6.2.1.1. Stable
    - 6.2.1.2. Windows Privilege Escalation
      - 6.2.1.2.1. Unquoted Service Paths
    - 6.2.1.3. Linux Privilege Escalation
  - 6.2.2. Maintaining Access
    - 6.2.2.1. Password and Hashes
      - 6.2.2.1.1. Pass the Hash
      - 6.2.2.1.2. Cracking Hashes
      - 6.2.2.1.3. Mimikatz
      - 6.2.2.1.4. Windows Credentials Editor
    - 6.2.2.2. Enable RDP Service
    - 6.2.2.3. Backdoor
      - 6.2.2.3.1. Persistence
      - 6.2.2.3.2. Manual Installation
    - 6.2.2.4. New Users
    - 6.2.2.5. DLL Hijacking/Preloading
- **6.3. Pillaging**

MODULE 7. ANONYMITY

Penetration testers rarely need to cover their tracks.

However, there are times when testing the efficiency of the target organization incident response team is within the scope of a Penetration tester's engagement.

This module will teach techniques to perform your tests while covering your tracks.

MODULE 8: SOCIAL ENGINEERING

The social engineering module will guide you through the most modern social engineering attacking techniques.

Real world attacks will be illustrated by exploiting the potential of social networks such as Facebook, Spokeo or Twitter.

Almost one hour of video lessons will teach you everything you need to know to master the most important tool in the field: Social Engineering Toolkit.

8. Social Engineering

- **8.1. What is Social Engineering**
- **8.2. Types of Social Engineering**
  - 8.2.1. Pretexting
  - 8.2.2. Phishing
  - 8.2.3. Baiting
  - 8.2.4. Physical
- **8.3. Samples of Social Engineering Attacks**
  - 8.3.1. Canadian Lottery
  - 8.3.2. FBI Email
  - 8.3.3. Online Banking
- **8.4. Pretexting samples**
- **8.5. Tools**
  - 8.5.1. Social Engineering Toolkit

MODULE 1: INTRODUCTION

The PowerShell for Pentesters Introduction module offers an introduction into the Why and What of PowerShell. Introducing some of the benefits to using PowerShell for penetration testing engagements, and what PowerShell is at a high-level.

1. Introduction
  1.1. Why Powershell?
  1.2. What is Powershell?

MODULE 2: POWERSHELL FUNDAMENTALS

PowerShell Fundamentals takes the student through the very essentials of PowerShell. From utilizing the Command Line Interface to various useful commands and components as they relate to PowerShell and its use in Penetration Testing. The student will have a good understanding of Module usage, Cmdlets, Objects, Scripting, Loop-Statements and introduces some common PowerShell frameworks and other techniques for use with Penetration Testing.

2. Powershell Fundamentals
  2.1. The Powershell CLI
    2.1.1. Basic Usage
      2.1.1.1. Get-Help
      2.1.1.2. Get-Command
  2.2. Cmdlets
    2.2.1. Pipelining
    2.2.2. Useful Cmdlets & Usage
    2.2.3. Get-Process
    2.2.4. Get-ChildItem
    2.2.5. Get-WmiObject
    2.2.6. Export-Csv
    2.2.7. Exploring the Registry
    2.2.8. Select-String
    2.2.9. Get-Content
    2.2.10. Get-Service
  2.3. Modules
    2.3.1. Get-Module
    2.3.2. Import-Module
  2.4. Scripts

2.4.1. Loop Statements
2.4.2. ForEach-Object
2.4.3. Where-Object
2.4.4. Powershell TCP Port Scanner

2.5. Objects

2.5.1. Creating .Net Objects

MODULE 3: OFFENSIVE POWERSHELL

With the Offensive PowerShell module, students will dive deeper into specific PowerShell tools, techniques, and frameworks. From downloading and execution of payloads and scripts to Obfuscation, Information Gathering, and Post-Exploitation. This module will also provide the student with a greater understanding of the "Living Off the Land" concept as it relates to utilizing PowerShell for offensive purposes and introduces several powershell pentesting frameworks and tools including Nishang, PowerSploit, and Empire.

Hera Labs are included in this module

3. Introduction

3.1. Downloading & Execution

3.1.1. Net.WebClient DownloadString Method
3.1.2. Net.WebClient DownloadFile Method
3.1.3. Net.WebRequest
3.1.4. System.Xml.XmlDocument
3.1.5. COM Objects for Download & Execution
3.1.5.1. Msxml2.XMLHTTP COM Object
3.1.5.2. WinHttp.WinHttpRequest.5.1 COM Object
3.1.6. ExecutionPolicy Bypass and Hidden Window
3.1.7. Invoke-Cradle Crafter

3.2. Obfuscation

3.2.1. Invoke-Obfuscation
3.2.2. Encoded Commands

3.3. Information Gathering & Recon

3.3.1. Host Discovery & Port Scanning
3.3.2. PowerSploit – Invoke-PortScan
3.3.3. PowerSploit – Get-HttpStatus
3.3.4. Posh-SecMod – Invoke-ARPScan
3.3.5. Posh-SecMod – Invoke-ReverseDNSLookup
3.3.6. Posh-SecMod – Resolve-HostRecord

MODULE 1: INTRODUCTION

The Linux Exploitation introductory module introduces Linux as a platform-of-choice for many of today's Internet-connected devices covers some history and various common distributions.

1. Introduction
  1.1. Why Linux?
  1.2. Common Distributions

MODULE 2: INFORMATION GATHERING

This module takes the student through the methods and tools used during the Information Gathering process for Linux-based systems, from remote information gathering to gathering information locally on compromised systems. Including enumerating services such as SMTP, SMB, NFS and more, using both automated tools, and manual bash scripting-based methods.

2. Information Gathering
  2.1. Remote Enumeration
    2.1.1. OS Fingerprinting
    2.1.2. Enumerating NFS
    2.1.3. Enumerating Portmapper (rpcbind)
    2.1.4. SMB Enumeration (including shares)
    2.1.5. SMB Users (rpcclient scripting)
    2.1.6. SMTP User enumeration (including VRFY, RCPT TO and EXPN via telnet)
  2.2. Location Enumeration
  2.3. Cheatsheets

MODULE 3: REMOTE EXPLOITATION

The Exploitation Over the Network section is an in-depth dive into exploiting some of the most common and some not-so-common vulnerabilities found to affect Linux-based systems. The student will learn the concept of password spray attacks, to exploiting Java, Samba, Shellshock and a host of other vulnerabilities from a remote perspective. This module will enable the student to identify exploitable vulnerabilities and misconfigurations commonly found on Linux systems.

Hera Labs are included in this module

3. Remote Exploitation

3.1. Password Spray Attack

3.2. Exploiting Samba

3.2.1. Username Map Script – CVE-2007-2447

3.2.2. Samba Symlink Directory Traversal

3.2.3. Writeable Samba Share to Remote Command Execution via Perl Reverse Shell

3.3. Exploiting Shellshock

3.4. Exploiting Heartbleed

3.5. Exploiting Java RMI Registry

3.6. Exploiting Java Deserialization

3.7. Exploiting Apache Tomcat

3.7.1. Default Credentials / Weak Credentials

3.7.2. Malicious .war Deployment with Laudanum

MODULE 4: POST-EXPLOITATION

The post-exploitation module for Linux Exploitation will navigate the student through the various stages of post-exploitation from Privilege Escalation, to Lateral Movement, Data Exfiltration and Maintaining Access. The student will learn how to exploit misconfigurations, SUID executables, crack passwords, the basics of Kernel Exploits, and will also learn some lesser known techniques for obtaining root access, such as SSH hijacking and Shared Object Library loading, to several newer and lesser-known techniques that can be used to maintain persistence through custom services and utilities already built-in to the operating system.

Hera Labs are included in this module

4. Post-Exploitation

4.1. Privilege Escalation

4.1.1. Leveraging System and Network Information

4.1.2. Leveraging User Information

4.1.3. Privileged Access / Cleartext Credentials

4.1.4. Services
4.1.5. Jobs / Tasks
4.1.6. Leveraging Installed Software Version Information
4.1.7. SUID Binaries and Practical Exploitation Examples
4.1.8. Sudo Privileged Access (Including “less” shell escape, “man” arbitrary command execution and docker sudo privilege escalation)
4.1.9. Restricted Shells & Restricted Shell Escapes
4.1.9.1. Restricted shell escape with Vi / Vim
4.1.9.2. Restricted shell escape with “find”
4.1.9.3. Restricted shell escape with “python” or “perl”
4.1.9.4. Restricted shell escape from another system with SSH
4.1.10. Cracking the Shadow
4.1.10.1. Unshadow and John the Ripper
4.1.11. MimiPenguin (Retrieving clear-text passwords from memory)
4.1.12. Pilfering Credentials from Swap Memory
4.1.13. Code Execution via Shared Object Library Loading
4.1.14. Introduction to Kernal Exploits (Finding, compiling and executing the appropriate exploit)
4.1.15. Introduction to Unix Socket Exploitation

4.2. Lateral Movement

4.2.1. SSH Hijacking
4.2.2. Stealing SSH Credentials
4.2.3. Samba Secrets to Domain Admin
4.2.4. VPN pivoting
4.2.5. Dumping Stored FireFox Credentials

4.3. Data Exfiltration

4.3.1. Exfil over TCP Socket with EBCDIC and Base64
4.3.2. Exfil over SSH
4.3.3. Exfil via POST Request over HTTPS

4.4. Maintaining Access & Persistence

4.4.1. Reverse Shells
4.4.1.1. OpenSSL Reverse Shell
4.4.1.2. ICMP Reverse Shell
4.4.2. Custom Services
4.4.2.1. Xinetd UDP Portknock Backdoor
4.4.2.2. Systemd Netcat Bind Shell

MODULE 1: INTRODUCTION

This module will introduce you to the web application security field and its basic terminology.

If you are new to this field, you will gather all the skills you need to move to more advanced modules.

If you are already an advanced web application security tester, you will get introduced to the methodology and tools followed throughout the course.

Hera Labs are included in this module

- **1.4. Cookies**
  - 1.4.1. Cookies Domain
    - 1.4.1.1. Specified Cookie Domain
    - 1.4.1.2. Unspecified Cookie Domain
    - 1.4.1.3. IE Exception
    - 1.4.1.4. Inspecting the Cookie Protocol
    - 1.4.1.5. Cookie Installation
      - 1.4.1.5.1. Correct Cookie Installation
      - 1.4.1.5.2. Incorrect Cookie Installation
- **1.5. Sessions**
- **1.6. Web Application Proxies**
  - 1.6.1. Burp Suite
  - 1.6.2. OWASP ZAP

MODULE 2: INFORMATION GATHERING

Web application information gathering is a long and complex process.

It takes insight and perseverance.

You will learn the best methodologies to collect and store information about your target web assets. This information will be used at later steps in the exploitation process.

At the end of this module, you will have so much information on your target that exploiting it will be easy and fun.

Hera Labs are included in this module

- **2. Information Gathering**
  - **2.1. Gathering Information on Target**
    - 2.1.1. Finding Owner, IP Addresses, and Email Addresses
      - 2.1.1.1. WHOIS tools
      - 2.1.1.2. DNS
      - 2.1.1.3. Nslookup and Netcraft
  - **2.2. Infrastructure**
    - 2.2.1. Fingerprinting the Webserver
      - 2.2.1.1. Netcat
      - 2.2.1.2. WhatWeb
      - 2.2.1.3. Wappalyzer

MODULE 3: CROSS-SITE SCRIPTING

In this module, the most widespread web application vulnerability will be dissected and studied thoroughly.

At first, you will be provided with a theoretical explanation. This understanding will help you in the exploitation and remediation process.

Later, you will master all the techniques to find XSS vulnerabilities through black box testing and within PHP code.

Real-world exploitation examples will conclude the module; you will finally steal session cookies, modify website DOM and perform advanced phishing attacks.

This is a hands-on intensive module.

Hera Labs are included in this module

3. Cross-Site Scripting

- **3.1. Cross-Site Scripting**
  - 3.1.1. Basics
- **3.2. Anatomy of an XSS Exploitation**
- **3.3. The three types of XSS**
  - 3.3.1. Reflected XSS
  - 3.3.2. Persistent XSS
  - 3.3.3. DOM-based XSS
- **3.4. Finding XSS**
  - 3.4.1. Finding XSS
- **3.5. XSS Exploitation**
  - 3.5.1. XSS and Browsers
  - 3.5.2. XSS Attacks
    - 3.5.2.1. Cookie stealing through XSS
    - 3.5.2.2. Defacement
    - 3.5.2.3. XSS for advanced phishing attacks
    - 3.5.2.4. BeEF
- **3.6. Mitigations**
  - 3.6.1. Input Validation
  - 3.6.2. Context-Aware Output Encoding
  - 3.6.3. Never trust user input

MODULE 4: SQL INJECTION

This module contains the most advanced techniques to find and exploit SQL Injections, from the explanation of the most basic SQL injection to the most advanced.

Advanced methods will be taught with real-world examples, and the best tools will be demonstrated on real targets.

You will not be able to just dump remote databases but also get root on the remote machine through advanced SQL Injection techniques.

Tools will be covered in depth, and a taxonomy will help the student to pick the right tool according to the environment and scenario he will face in real engagements.

This is a video and hands-on intensive module.

Hera Labs are included in this module

4. SQL Injection

- **4.1. Introduction to SQL Injections**
  - 4.1.1. SQL Statements
    - 4.1.1.1. SELECT
    - 4.1.1.2. UNION
  - 4.1.2. SQL Queries in Web Apps
  - 4.1.3. Vulnerable Dynamic Queries
  - 4.1.4. How Dangerous is an SQLi
  - 4.1.5. SQLi Attack Classification
    - 4.1.5.1. In-Band SQLi
    - 4.1.5.2. Error-Based SQLi
    - 4.1.5.3. Blind SQLi
- **4.2. Finding SQL Injections**
  - 4.2.1. Simple SQL Injection
  - 4.2.2. SQL Errors in Web Apps
  - 4.2.3. Boolean-Based Detection
- **4.3. Exploiting In-Band SQL Injections**
  - 4.3.1. Scenario
  - 4.3.2. In-band Attack Challenges
  - 4.3.3. Enumerating the Number of Fields
    - 4.3.3.1. Different DBMS UNION Mismatch Errors

MODULE 5: OTHER COMMON WEB ATTACKS

Sophisticated attacks against web applications are the subject of this module.

Session Fixation and CSRF are often underestimated and overlooked vulnerabilities, which will be covered in depth. They will be covered in depth.

A working exploit will be created step by step to demonstrate a CSRF vulnerability found in a famous CMS.

Hera Labs are included in this module

MODULE 1: PREREQUISITES

In the first module of the Wi-Fi section, we will see which are the hardware/software prerequisites of the course.

1. Prerequisites

  1.1. Software

  1.2. Hardware

    1.2.1. Antennas

    1.2.2. A Note on Signal Strength

    1.2.3. Conclusions

MODULE 2: ENVIRONMENT SETUP

In this module, the student will learn how to properly configure the test environment in order to obtain the best outcome from the successive modules.

2. Environment setup

  2.1. Introduction

    2.1.1. Considerations on Linux drivers

  2.2. Adapter configuration

    2.2.1. Testing your Setup

MODULE 3: WIRELESS STANDARDS AND NETWORKS

In this module, the student will learn the basic concepts at the base of the Wi-Fi infrastructures.

We will see which types of Wi-Fi configurations exist, how they work, and which are the security features and mechanisms implemented.

We will also present an overview of the most important flaws that affect different types of Wireless infrastructures and protocols.

Downloadable scripts are included in this module

3. Wireless Standards and Networks

  3.1. IEEE 802.11 Standards

  3.2. Types of Wireless Network

MODULE 4: DISCOVER WI-FI NETWORKS

The first step when running penetration tests against Wi-Fi networks is to discover and identify our target. In this module, we will see how to do this through a series of tools available for different platforms.

Downloadable exercises are included in this module

4. Discover Wi-Fi Networks
- **4.1. Tools**
  - 4.1.1. inSSIDer
  - 4.1.2. Kismet
  - 4.1.3. Airodump-ng
- **4.2. Hidden SSID**
  - 4.2.1. Network de-cloaking

MODULE 5: TRAFFIC ANALYSIS

After the target network has been identified, this module takes us to the next step, which is to configure our tools in order to sniff and intercept the traffic.

This is a very important step for all the attacks that come hereafter.

Downloadable exercises are included in this module

5. Traffic Analysis
- **5.1. Capturing traffic**
- **5.2. Monitor mode**
- **5.3. Channel Hopping**
- **5.4. Wireshark filters**
- **5.5. Traffic decryption**

MODULE 6: ATTACKING WI-FI NETWORKS

This module focuses on the attacks that can be executed on Wi-Fi networks.
The student will learn how to attack and access remote Wi-Fi networks, obtain keys, password and much more, according to their configuration and security mechanism.

We will first start exploring the attacks against WEP and then focus our tests on more secure networks: WPA, WPA2, and WPS.

Downloadable exercises are included in this module

MODULE 7: WI-FI AS AN ATTACK VECTOR

In this final module of the Wi-Fi section, the student will learn how to use Wi-Fi as an attack vector.

This means that we will not attack Wi-Fi networks. Instead, we will use Wi-Fi in order to create fake networks, obtain credentials, run MitM attacks and much more. The effective evil-twin attack will be demonstrated in detail, in addition to describing how WPA2-Enterprise can be attacked.

7. Wi-Fi as an attack vector
- **7.1. Rogue AP**
  - 7.1.1. A Typical Rogue AP Scenario
  - 7.1.2. Recover PRGA with a Rogue AP
  - 7.1.3. Initiate a WPA/WPA2 Handshake
  - 7.1.4. Man-in-the-Middle Attack
  - 7.1.5. Rouge AP: An Alternative Definition
  - 7.1.6. Rogue AP: “Evil Twin Attack”
  - 7.1.7. Attacks Against WPA2-Enterprise
    - 7.1.7.1. Eaphammer
- **7.2. Wardriving**

MODULE 1: INSTALLATION AND FUNDAMENTALS

In the first module of the Ruby section, you will see how to install and configure the Ruby environment.

Once the environment is configured, you will learn the basic concepts of Ruby, such as running and writing scripts, using the interpreter, installing gems and much more. You will also learn the basic concepts of Ruby such as data types, variables declarations and more.

Downloadable scripts are included in this module

MODULE 2: CONTROL STRUCTURES

One of the most important program structures that a programmer has to master is the ‘flow control structure.’

In this module, the student will learn how to write and define different types of Ruby control structures. This will allow the student to create scripts and programs that are not limited to a linear sequence of statements.

Downloadable scripts are included in this module

MODULE 3: METHODS, VARIABLES, AND SCOPE

Every program must be clean and have reusable structures.

In this module, the student will learn how to define and use Ruby methods, blocks, aliases and more. This is useful for creating very powerful tools and scripts.

With the introduction of methods and blocks, a very important topic needs to be covered: the scope.

Downloadable scripts are included in this module

MODULE 4: CLASSES, MODULES AND EXCEPTIONS

Ruby is an Object-Oriented Programming language. With that said, an OO program involves classes and objects.

In this module, we will start covering more advanced topics, and we will see how to define and use classes, functions, modules, mixin, namespaces and much more.

Along with these topics, we will also see how to handle exceptions; exceptions are a very useful topic that needs to be mastered in order to take control of the program behavior.

Downloadable scripts are included in this module

MODULE 5: PENTESTERS PREREQUISITES

Ruby is a very powerful programming language and thanks to its many features, it can be used for many different purposes.

From this module on, we will focus on how to use Ruby for penetration testing purposes. One of the first topics we will cover is *'Regular Expression.'*

Regex is widely used in the security field; it is used to find and locate important information stored in files, web pages, network communication and so on.

Good working knowledge of how to use and define regex is a ‘must’ for a penetration tester!

During this module, the student will also learn how to use date and time classes as well as manage and interact with files and directories: read, delete, create and so on.

Downloadable scripts are included in this module

        - 5.3.1.2. Change Directory
        - 5.3.1.3. Creation / Deletion
        - 5.3.1.4. Directory Listings
        - 5.3.1.5. Testing Directories
        - 5.3.1.6. Dir Objects
        - 5.3.1.7. Example: Windows Application Directory Listing
    - 5.3.2. Files
        - 5.3.2.1. Testing Files
        - 5.3.2.2. Working with Names
        - 5.3.2.3. Create/Delete/Rename
        - 5.3.2.4. Change Permission
- **5.4. Conclusion**

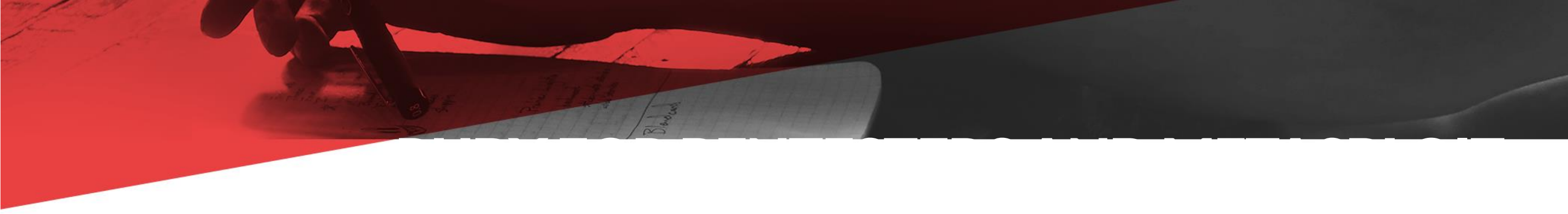
MODULE 6: INPUT / OUTPUT

In this module, the student will learn how to use different input and output mechanisms and techniques in order to find (read) or store (write) information to and from files.

We will see several examples and scripts that can be used in conjunction with other tools (i.e., Nmap) in order to gather, filter and store important information.

Downloadable scripts are included in this module

6. Input / Output
- **6.1. File Stream**
    - 6.1.1. Reading from A File
    - 6.1.2. Writing to A File
- **6.2. Working with NMAP Files**
    - 6.2.1. IP Extraction
        - 6.2.1.1. Normal Format
        - 6.2.1.2. Grepable Format
        - 6.2.1.3. XML Format
        - 6.2.1.4. All Together
    - 6.2.2. Open Port Extraction
        - 6.2.2.1. Normal Format
        - 6.2.2.2. Grepable Format
        - 6.2.2.3. XML Format
        - 6.2.2.4. All Together
- **6.3. Conclusion**



MODULE 7: NETWORK AND OS INTERACTION

Another very important topic that a penetration tester should master is ‘network communication.’

In this module, the student will learn how to use the power of Ruby in order to create, forge, intercept network communications.

Thanks to many useful examples and scripts, the student will learn how to create raw sockets, forge packets, create TCP/UDP scanners and much more.

We will also see how to interact with local and remote operating systems.

This, in conjunction with the network communication skills, may be useful to create powerful tools (i.e., backdoors that are able to retrieve information from remote systems, as well as send and run specific commands).

Downloadable scripts are included in this module

Hera Labs are included in this module

MODULE 8: THE WEB

In the previous module, the student will study network communications and local interactions with the OS. Now it is time to focus on Web Applications.

We will see how to create and intercept HTTP and HTTPS requests and responses, as well as how to send/read GET and POST parameters and much more. Along with these topics, the student will also be presented with some useful scripts and use cases useful to run attacks against web application or identify vulnerabilities such as XSS.

Downloadable scripts are included in this module

Hera Labs are included in this module

8. The Web

8.1. Starting point

8.1.1. HTTP Protocol
8.1.2. Ruby's alternatives
8.1.2.1. Using simple socket
8.1.2.2. Net::HTTP library
8.1.2.3. Open-URI library
8.1.2.4. URI object

8.2. Request & Response

8.2.1. Net::HTTP class and instances
8.2.2. GET
8.2.2.1. Net::HTTP get
8.2.2.2. Net::HTTP get_response
8.2.2.3. HTTPResponse object
8.2.2.3.1. Status
8.2.2.3.2. Headers
8.2.2.3.3. Body
8.2.2.3.4. Response object types
8.2.2.4. Parameters
8.2.2.4.1. URL encapsulation
8.2.2.4.2. Dynamic parameters
8.2.2.5. Net::HTTP Instances
8.2.2.5.1. Using get Instance method
8.2.2.5.2. Using HTTP::Get request object
8.2.2.5.3. URI and parameters
8.2.2.6. Request Headers

MODULE 9: EXPLOITATION WITH RUBY

During the study of previous modules, the student should have acquired many Ruby programming skills.

It is time to take advantage of these skills and use Ruby in order to write and exploit vulnerable services and software.

In this module, we will present a vulnerable application that the student can use to learn how to write a full working exploit.

Downloadable scripts are included in this module

Hera Labs are included in this module

MODULE 10: METASPLOIT

Now that the student has mastered Ruby and its features, it is time to start working with one of the most powerful Ruby tools: Metasploit.

In this module, the student will study the Metasploit architecture and the framework and will learn how to create, add and edit custom Metasploit modules.

Thanks to our virtual labs, the student will also have the opportunity to practice against real vulnerable machines.

Downloadable scripts are included in this module

Hera Labs are included in this module

ABOUT US

We are eLearnSecurity.

Based in Santa Clara, California, 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

Via Gian Battista Queirolo
Pisa, Italy

2040 Martin Ave.
Santa Clara, CA, USA

Apricot Tower, Dubai Silicon Oasis
Dubai, UAE