SYLLABUS

PENETRATION TESTING EXTREME
VERSION 2

The most advanced course on network penetration testing

eLearn Security
AN INE COMPANY

eLearnSecurity has been chosen by students in 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 eXtreme (PTX) course is the online, self-paced training course, that provides all the advanced skills required to carry out a thorough and professional penetration test against modern networks and infrastructure.

Specifically, PTX provides among others:

- The knowledge and skills to execute state-sponsored-like operations
- The ability to perform advanced adversary simulation
- Implementation details on numerous undocumented attacks

Thanks to the extensive use of Hera Lab and with coverage of the latest research in the network security field, the PTX course is not only the most practical training course on the subject, but also the most up to date.

COURSE ORGANIZATION

This 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 anywhere an internet connection is available. Some versions allow a student to download course material and study off-line.

While online studying, it is always possible to resume your studying from the last slide or video accessed.

The Penetration Testing Professional eXtreme 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 vulnerable infrastructures on demand where a student can practice each topic seen in the course in a dedicated and isolated environment.

TARGET AUDIENCE AND PRE-REQUISITES

The PTX training course benefits the career of penetration testers and IT Security personnel in charge of defending their organization's infrastructure and network.

This course allows organizations of all sizes, assess and mitigate the risk at which their network is 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their teams with a comprehensive and practical training course without having to deploy internal labs that are often outdated and not backed by solid theoretical material.

Students willing to enroll in the course must possess a solid understanding of networks and network related security models.

Students must be familiar with PowerShell scripting, as well as have Active Directory administration and Windows internals knowledge. Students are also required to have basic reverse engineering skills as well as possess good knowledge of network protocols.

WILL I GET A CERTIFICATE?

The PTX course leads to the eCPTXv2 certification.

The certification can be obtained by successfully completing the requirements of a 100% practical exam consisting in a penetration test of a real-world complex network hosted in our eLearnSecurity Hera Labs.

ORGANIZATION OF CONTENTS

SECTION 1: PREPARING THE ATTACK

- Module 1: Social Engineering Attack Vectors

SECTION 2: RED TEAMING ACTIVE DIRECTORY

- Module 1: Advanced AD Reconnaissance & Enumeration
- Module 2: Red Teaming Active Directory

SECTION 3: RED TEAMING CRITICAL DOMAIN INFRASTRUCTURE

- Module 1: Red Teaming MS SQL Server
- Module 2: Red Teaming Exchange
- Module 3: Red Teaming WSUS

SECTION 4: EVASION

- Module 1: Defense Evasion

SECTION 1: PREPARING THE ATTACK

In this section, you will be shown how to attack the human factor via advanced social engineering attacks, while remaining under the radar. Then, you will see advanced usages of the established toolkits as well as how to customize them and even develop your own custom attack vectors and payloads. Uncommon phishing techniques and anti-analysis practices are also included in this section.

MODULE 1: SOCIAL ENGINEERING ATTACK VECTORS

In this module, you will be shown how to execute advanced client-side attacks, while remaining under the radar. You will learn how to execute advanced social engineering attacks as well as how to develop your own custom attack vectors and payloads. Uncommon phishing techniques and anti-analysis practices are also included in this module.

1.1. Introduction
1.2. Email delivery & macro fundamentals
1.2.1 Email delivery fundamentals
- SPF, DKIM, DMARC, Accepted Domains & Spam Traps
- Circumventing Defenses

1.2.2 Macro fundamentals
- Macros: Documents Case
- Remote templates

1.3. Attack vector development
1.3.1 Custom macro development
- Macro leveraging file properties to hide its payload and StdIn to avoid logging
- Using ActiveX controls for macro execution
- The classic download and execute macro, with a twist
- Multi-platform macro malware
- RTF + Signed binary + DLL hijacking + Custom MSF loader = ❤️
- Embedding an executable in a macro (executable2vbs)
- Network-tracing macro
- Multi-stage macro malware using DNS for payload retrieval and exfiltration
- Macro malware performing direct shellcode injection
- Macros on PowerPoint (Custom Actions)
- Macro obfuscation

MODULE 1: SOCIAL ENGINEERING ATTACK VECTORS (cont.)

- 1.3.2 Abusing Office capabilities
  - OLE objects for payload execution
  - Exploiting MS16-032 via Excel DDE without macros
  - Office-handled links
- 1.3.3 Uncommon extensions
  - CHM Files + Custom JS Backdoor
  - HTML Application (HTA) files
  - Shortcut (LNK) files
  - Web Query (IQY) files
  - MSG files
  - Rich Text Format (RTF) files
- 1.3.4 Custom ClickOnce applications
  - Custom beaconing malware
  - Minimizing on-disk footprint (PowerShell without PowerShell)

1.4 Phishing techniques

- 1.4.1 Leveraging CSRF and Open Redirects
- 1.4.2 Creating trustworthy-looking redirect forms (Custom JavaScript)
- 1.4.3 URL spoofing techniques
  - Data URIs
  - Phishing page (multilayer) obfuscation
- 1.4.4 BeEF and custom scripting to gain administrative access
- 1.4.5 Mimicking DYRE banking trojan's spread method

1.5 Generic Anti-analysis

- 1.5.1 Apache mod_rewrite for anti-analysis
  - User Agent Redirection
  - Invalid URI Redirection
  - Operating System Based Redirection
  - IP Filtering
- 1.5.2 Macro-based anti-analysis
  - Red Team Infrastructure
  - Phishing with Reverse Proxies

1.6 Evasive C2 Frameworks

- 1.6.1 SilentTrinity
- 1.6.2 Covenant

MODULE 1: SOCIAL ENGINEERING ATTACK VECTORS (cont.)

1.7 Modern Social Engineering Attack Vectors

- 1.7.1 Excel 4.0 Macros
- 1.7.2 Spoofing Parent Processes and Command Line Arguments
- 1.7.3 Executable Database Files (ACCDE)
- 1.7.4 VBA Stomping
- 1.7.5 Abusing Excel Features
- 1.7.6 Evading Sandboxes and Application Whitelisting

SECTION 2: RED TEAMING ACTIVE DIRECTORY

In this section, you will learn how to find your way to a domain administrator inside an organization's network. First, you will perform stealthy reconnaissance and enumeration to identify hosts, servers, services and privileged users. Then, you will stealthily extract critical Active Directory and user information. Finally, you will be guided through red team oriented Active Directory attacks, exploiting common misconfigurations and abusing legitimate Windows/Active Directory functionality.

MODULE 1: ADVANCED AD RECONNAISSANCE & ENUMERATION

A red team member will usually identify misconfigurations or exploit trust relationships which will take him all the way to domain administrator. To achieve this, stealthy and extensive reconnaissance and enumeration are required, prior to any exploitation activities. In this module, you will be shown such advanced reconnaissance and enumeration techniques against Windows environments. You will actually learn how to retrieve the most important pieces of information out of Active Directory, while remaining undetected. Privileged user, group and computer hunting, SPN scanning, ACL attack path enumeration, situational awareness surveys, leveraging reflection, LDAP & WMI and advanced Powerview usage are only a subset of what you will learn in this module.

1.1 Introduction
1.2 The traditional approach
1.2.1 Using a sniffer or a network scanning tool
1.2.2 Recon & enumeration through a non-domain joined Linux machine
- Leveraging SNMP
- Recon through dig
- SMB (& NULL Sessions)
- Share enumeration

1.2.3 Defeating anonymous user restrictions (against legacy systems)
1.2.4 Recon & enumeration through a domain joined Windows machine
- net commands
- Enumeration through DNS
- Enumeration through NetBIOS
- dumpsec, shareenum, enum binaries

MODULE 1: ADVANCED AD RECONNAISSANCE & ENUMERATION (cont.)

1.3 Red team-oriented reconnaissance & enumeration

1.3.1 Fundamentals & User Hunting

- DNS using LDAP
- SPN Scanning / Service Discovery
- Group Policies
- Fundamentals of user hunting (API calls, LDAP, PSReflect, linkable patterns etc.)
    a. User Hunting
    b. Stealthy User Hunting
- Local Administrator Enumeration
- Derivative Local Admin
- Identifying Administrator Accounts: Group Enumeration
- Identifying Administrator Accounts: RODC Groups
- Identifying Administrator Accounts: AdminCount =1
- GPO Enumeration & Abuse
- Identifying Administrator Accounts: GPPs
- Identifying Active Directory Groups with Local Admin Rights
- Identifying regular users having admin rights
- Identifying Virtual Admins
- Identifying Computers Having Admin Rights
- Interesting Group Enumeration
- Follow the Delegation
- Custom Domain/OU Delegation
- MS LAPS Delegation

1.3.2 Important AD Component Enumeration

- AD Forest Information
- AD Domain Information
- The PDC emulator
- Domain Trusts
- BloodHound
- Identifying Partner Organizations using Contacts

1.3.3 Interesting Corners of Active Directory

- Active Directory ACLs
- Sensitive Data in User Attributes
- AD User & Computer Properties
- Deleted AD Objects
- Domain Password Policies

MODULE 1: ADVANCED AD RECONNAISSANCE & ENUMERATION (cont.)

1.3.4 Post-Exploitation Recon & Enumeration
- Defensive measure related information

1.3.5 Recon & Enumeration Tips & Tricks
- Recon & Enumeration without PowerShell
- Mapping the application server attack surface of an organization
    a. Stealthy web application mapping
    b. Gathering browser data to identify internal websites and applications

1.4 Situational Awareness

1.4.1 Evade Parent-Child Process Anomaly Detection
1.4.2 Abusing PowerShell
1.4.3 Information Gathering Through WMI
1.4.4 Seatbelt

MODULE 2: RED TEAMING ACTIVE DIRECTORY

In this module, you will be shown how to attack Active Directory environments. Specifically, you will be shown how to attack Windows authentication leveraging inefficiencies in its core (regardless of the basis being NTLM or Kerberos), how to bypass the latest in Windows security enhancements (Script block logging, AMSI, Constrained Language Mode, Applocker etc.) and how to identify and abuse common Active Directory misconfigurations. Then, you will be taught how to stealthily move laterally into a network leveraging native Windows functionality, how to abuse domain trusts and finally, how to stealthily own the whole infrastructure and persist on it. The whole range of Active Directory attacks and attacker TTPs are covered. From targeted kerberoasting to the infamous "printer bug" and from resource-based constrained delegation to abusing PAM trusts, attacking LAPS and abusing DPAPI as well as JEA. Three (3) fully featured and enterprise-like Active Directory environments will be provided to you where you will apply all the above and more while using the latest in C# and .NET tradecraft.

2.1 Introduction
2.2 AD Fundamentals
- LDAP
- Authentication (incl. weaknesses & known attacks)
- Authorization
- AD & DNS
- AD Components (DCs, RODCs, Global Catalogs, Data Store, Replication, Domains, Forests, Trusts etc.)

2.3 Traditional AD Attacks
2.3.1 LDAP Relay
2.3.2 Exploiting Group Policies
2.3.3 RDP MiTM
2.3.4 Sniffing Authentication Traffic
2.3.5 Downgrading NTLM
2.3.6 Non-MS Systems Leaking Credentials
2.3.7 LLMNR and NBT-NS poisoning (incl. enhancing Responder)

MODULE 2: RED TEAMING ACTIVE DIRECTORY (cont.)

- **2.4 Red team-oriented AD attacks (Part 1)**
  - 2.4.1 PowerShell Defenses in AD
  - 2.4.2 Bypassing PowerShell's Security Enhancements
  - 2.4.3 Paths to AD Compromise
    - 2.4.3.1 MS14-068
    - 2.4.3.2 Unconstrained Delegation (incl. pass-the-ticket)
    - 2.4.3.3 OverPass-the-Hash (Making the most of NTLM password hashes)
    - 2.4.3.4 Pivoting with Local Admin & Passwords in SYSVOL
    - 2.4.3.5 Dangerous Built-in Groups Usage
    - 2.4.3.6 Dumping AD Domain Credentials
    - 2.4.3.7 Golden Tickets
    - 2.4.3.8 Kerberoast
    - 2.4.3.9 Silver Tickets
    - 2.4.3.10 Trust Tickets
- **2.5 Leveraging Kerberos Authentication**
  - 2.5.1 Kerberos tickets when NTLM is disabled
  - 2.5.2 Password spraying using Kerberos
- **2.6 Red team-oriented AD attacks (Part 2)**
  - 2.6.1 Targeted Kerberoasting
  - 2.6.2 ASREPRoast
  - 2.6.3 Over-pass The Hash / Pass The Key (PTK)
  - 2.6.4 Pass The Ticket (PTT)
  - 2.6.5 The "Printer Bug" and Kerberos Unconstrained Delegation
  - 2.6.6 Kerberos Constrained Delegation
  - 2.6.7 Kerberos Resource-Based Constrained Delegation
    - 2.6.7.1 Kerberos Resource-Based Constrained Delegation Computer Object Take Over
    - 2.6.7.2 Kerberos Resource-Based Constrained Delegation Via Image Change
  - 2.6.8 Kerberos Attacks Using Proxies
  - 2.6.9 Abusing Forest Trusts
  - 2.6.10 LAPS
    - 2.6.10.1 LAPS Exploitation
  - 2.6.11 ACLs on AD Objects
  - 2.6.12 Backup Operators

MODULE 2: RED TEAMING ACTIVE DIRECTORY (cont.)

- **2.6 Red team-oriented AD attacks (Part 2)**
  - 2.6.13 ACLs in Active Directory
    - 2.6.13.1 Escalating Privileges using Exchange
    - 2.6.13.2 Invoke-ACLPwn
    - 2.6.13.3 NTLMRelayx
  - 2.6.14 Abusing Privileged Access Management (PAM)
  - 2.6.15 Just Enough Administration (JEA)
    - 2.6.15.1 Abusing Just Enough Administration (JEA)
  - 2.6.16 DNSAdmins
    - 2.6.16.1 Privilege Escalation using DNSAdmins
  - 2.6.17 DPAPI Abuse
  - 2.6.18 Token Abuses
- **2.7 Persisting in Active Directory**
  - 2.7.1 PsExec
  - 2.7.2 SC
  - 2.7.3 Schtasks.exe
  - 2.7.4 AT
  - 2.7.5 WMI
  - 2.7.6 PoisonHandler
  - 2.7.7 Remote Desktop Services
  - 2.7.8 Browser Pivoting
  - 2.7.9 ChangeServiceConfigA
  - 2.7.10 WinRM
  - 2.7.11 DCOM
  - 2.7.12 Named Pipes
  - 2.7.13 PowerShell Web Access
  - 2.7.14 Net-NTLM Relaying
  - 2.7.15 Computer Accounts
- **2.8 Pivoting in Active Directory**
  - 2.8.1 Remote Desktop Tunneling Using Virtual Channels
    - 2.8.1.1 SocksOverRDP
    - 2.8.1.2 Proxychains for Windows
  - 2.8.2 SMB Pipes
  - 2.8.3 Windows Firewall
  - 2.8.4 SharpSocks
  - 2.8.5 SSHuttle
  - 2.8.6 RPivot
  - 2.8.7 reGeorg

MODULE 2: RED TEAMING ACTIVE DIRECTORY (cont.)

2. 8 Pivoting in Active Directory
- 2.8.8 Mssqlproxy

2. 9 Persisting in Active Directory
- 2.9.1 Start-Up
- 2.9.2 Registry
- 2.9.3 LNKs
- 2.9.4 Scheduled Tasks
- 2.9.5 WMI Permanent Event Subscriptions
- 2.9.6 Intro to COM Hijacking
  - 2.9.6.1 Phantom COM Objects
  - 2.9.6.2 Scheduled Tasks COM Object Hijacking
  - 2.9.6.3 COM “TreatAs” Hijack
- 2.9.7 MS Office Trusted Locations
  - 2.9.7.1 VBA “Add-Ins” For Excel

SECTION 3: RED TEAMING CRITICAL DOMAIN INFRASTRUCTURE

In this section, you will learn about leveraging MS SQL Server, Exchange and Windows Update to gain an initial foothold, stealthily move laterally or spread the compromise into an organization's network. You will be shown their inefficiencies and common misconfigurations as well as their powerful features and how they can be abused for exploitation or escalation.

MODULE 1: RED TEAMING MS SQL SERVER

The majority of organizations base their database infrastructure on SQL Server. In this module, attention will be given on weak and default SQL Server configurations that can be leveraged by a penetration tester / red team member. The whole SQL Server attack surface will also be mapped in this module. You will eventually learn how to locate and access SQL servers from various attack perspectives, how to identify insufficiently secure configurations, how to escalate privileges within SQL server from various attack perspectives and how to perform post-exploitation activities against SQL servers.

1.1 Introduction
1.2 MS SQL Server Fundamentals
1.3 Locating & Accessing SQL Servers
- The unauthenticated perspective
- The local user perspective
- The domain user perspective

1.4 Escalating privileges within SQL Server
- Unauthenticated User / Local User / Domain User -> SQL login
    - Gaining Initial Foothold on SQL Server
- SQL login -> sysadmin
    - Weak Passwords & Blind SQL Server Login Enumeration
    - Impersonation
        i. Impersonation Privilege
        ii. Stored Procedure and Trigger Creation / Injection Issues
        iii. Automatic Execution of Stored Procedures

MODULE 1: RED TEAMING MS SQL SERVER (cont.)

- sysadmin -> Service Account
    - OS Command Execution through SQL Server
    - Shared Service Accounts
    - Crawling Database Links
    - UNC Path Injection

1.5 Common Post-Exploitation Activities

- Persistence
    - Setting up a debugger for utilman.exe
    - Establishing persistence with xp_regwrite
    - Exporting and backdooring custom CLR assemblies
- Identifying Sensitive Data
    - Parsing and searching for sensitive data
    - Targeting DBs featuring transparent encryption
- Extracting SQL Server Login password hashes

1.6 Poisoning the SQL Server Resolution Protocol

MODULE 2: RED TEAMING EXCHANGE

The majority of organizations base their email infrastructure on MS Exchange Server and Outlook. In this module, you will see that those two components offer capabilities that can greatly assist us in a Red Team engagement. You will learn how you can compromise an organization externally by attacking its Exchange infrastructure. Specifically, you will be shown how to gain initial foothold, move laterally and even bypass network segregation by abusing Exchange functionality. Stealthily spreading the compromise and escalating your privileges are two additional things that you will be taught to do again by abusing Exchange functionality. The same actions, as you will see, can also be performed during an internal red teaming engagement.

2.1 Introduction
2.2 Exchange fundamentals
2.2.1 Protocols
2.2.2 Functions / Components
- Autodiscover
- Global Address List
- Outlook Rules
- Outlook Forms

2.3 Attacking externally (Remote Compromise)
2.3.1 Recon & OWA Discovery
2.3.2 Domain Name Discovery (Timing attack)
2.3.3 Naming Schema Fuzzing
2.3.4 Username Enumeration (Timing attack)
2.3.5 Password Discovery (Password Spraying)
2.3.6 GAL Extraction
2.3.7 More password discovery
2.3.8 Bypassing 2 Factor Authentication
2.3.9 Remote Compromise
- Spreading the compromise
    - Pillaging mailboxes for credentials/sensitive data
    - Internal Phishing
    - Malicious Outlook Rules (including bypassing network segmentation)
    - Malicious Outlook Forms (including bypassing network segmentation)

2.4 Attacking from the inside
- Misusing Exchange ActiveSync (EAS) to access internal file shares

2.5 Privilege Escalation By Busing Exchange

MODULE 3: RED TEAMING WSUS

Windows updates are an important aspect of security in every organization. Due to the trust relationship that exists between users and Windows updates, WSUS has some great potential for serious compromise. In this module, you will learn how to manipulate WSUS components, using a variety of techniques, to gain initial foothold, move laterally and even spread the compromise into an organization's network.

3.1 Introduction

3.2 Windows Update Fundamentals

- Windows Update from a security perspective
- Windows Update Overview (Windows Update Communications, Update types and storage)
- WSUS
    - WSUS Security
    - Identifying WSUS

3.3 Attacking WSUS

- Unencrypted Communications & Malicious Update injection
    - Via straight ARP spoofing
    - Via tampering with the target's proxy settings (WPAD Injection)
- Leveraging WSUS Interconnectivity

3.4 Leveraging Windows Update for Persistence

SECTION 4: EVASION

MODULE 1: DEFENSE EVASION

The majority of organizations base their defenses in multiple security solutions.

During an engagement, a red team member may come across multiple defense layers, from IDS/IPS and firewalls all the way to network segmentation, A/V, EDR, Sysmon, ETW and HIDS solutions.

In this module you will be shown how to move around such defenses as well as the common pitfalls in a red team member's tradecraft.

Removing hooks placed by A/Vs or EDRs, bypassing ETW, evading Sysmon, advanced AMSI patching and executing assemblies in memory are only a subset of what you will be taught during this module.

- **1.1 Evasion**
- **1.2 AMSI**
- **1.3 Bring Your Own Interpreter (BYOI)**
- **1.4 Event Tracking for Windows (ETW)**
- **1.5 SYSMON**
- **1.6 Endpoint Detection and Response (EDR)**
- **1.7 Discovery**
- **1.8 Lateral Movement**
- **1.9 Credential Access**
- **1.10 Sensitive Groups**
- **1.11 Custom Payload Development**
- **1.12 Removing User-Mode Hooks**
- **1.13 Stealth Macro Development**

The PTX course is a practice-based curriculum. Being integrated with Hera Lab, the most sophisticated virtual lab in IT Security, it offers an unmatched practical learning experience. Hera is the only virtual lab that provides fully isolated per-student access to each of the real-world scenarios available on the platform. Students can access Hera Lab from anywhere through VPN.

Modules will be accompanied by 7 hands-on labs that include 100+ red teaming challenges, spread across 11+ extensive Active Directory attack scenarios.

Lab 1: Custom Undetectable Macro Development
Your goal is to develop a custom macro-based attack (and the accompanying payloads), to compromise a target without being detected.

Lab 2: Establishing A Shell Through the Victim's Browser
During the lab you will develop a payload from scratch that will establish a shell through the victim's browser.

Lab 3: Serving a Malicious Update Through WSUS
You are engaged in an internal network penetration test. Your goal is to compromise a Windows 7 machine (10.100.11.101) through a Windows 10 machine (10.100.11.100), leveraging weak network configurations and abusing WSUS.

Lab 4: SQL injection to Domain Administrator Hash
You are engaged in an external network penetration test. Your goal is to stealthily capture the Domain Administrator's password hash through the internet facing Web App 1, leveraging weak SQL Server and database configurations as well as legitimate SQL Server capabilities.

Lab 5: Red-teaming Active Directory Lab #1 (Covenant C2 VS ELS.LOCAL)
In this fully-featured Active Directory lab you will heavily use Covenant C2 and modern C#/.NET tradecraft to achieve a great number of red-teaming objectives. You will have the opportunity to practice: attack path enumeration using Bloodhound, pivoting, lateral movement, (targeted) kerberoasting, golden/silver ticket creation, SIDHistory attacks, abusing constrained/unconstrained delegation, DCSync, SMB-based C2, bypassing Constrained Language Mode/AMSI/Applocker, attacking SQL Server, HTTP NetNTLM Relaying, privilege escalation, ACL-based attacks and much more...

Lab 6: Red-teaming Active Directory Lab #2 (ELS.BANK)
In this fully-featured and hardened Active Directory lab you will have to opportunity to practice: abusing a PAM trust, privilege escalation, ACL-based attacks, DCSync, abusing constrained delegation, decrypting a powershell secure string, malicious Kerberos ticket creation, abusing AD description attributes, abusing resource-based delegation, the "printer bug", abusing the machine key of IIS and much more...

Lab 7: Red-teaming Active Directory Lab #3 (ELS.CORP)
In this fully-featured Active Directory lab you will have to opportunity to practice: Phishing, stealthy enumeration, pivoting and lateral movement, SQL Server attacks, abusing forest trusts, Linux and Windows privilege escalation, malicious Kerberos ticket creation, the "printer bug", exploiting web app vulnerabilities to gain initial foothold, exploiting domain-joined Linux machines and Jumphosts and much more...

ABOUT US

We are eLearnSecurity.

eLearnSecurity was founded with the simple mission of revolutionizing the way IT professionals develop their information security skills. Now based in Cary, North Carolina with offices and employees around the United States and Europe, eLearnSecurity is a worldwide leader in cyber security training.

Through a blend of in-depth content and real-world simulations, our detailed courses, training paths, and certifications equip businesses and individuals with the skills needed to take on the cyber security challenges of today and tomorrow.

Whether you are interested in brushing up on specific ethical hacking techniques or following a comprehensive training path, eLearnSecurity provides a unique opportunity for security professionals to enhance their knowledge of the industry. We train red, blue, and purple teams in the latest cyber security techniques with classes ranging from beginner to expert levels.

eLearnSecurity's Hera Labs is an industry-leading virtual lab that offers our clients practical penetration testing and ethical hacking experience, changing the way students and businesses take on the future of cyber security.

Contact details:

www.elearnsecurity.com
contactus@elearnsecurity.com

Via Gian Battista Quierlo 15
Pisa, Italy

575 New Waverly Place #201
Cary, NC, USA