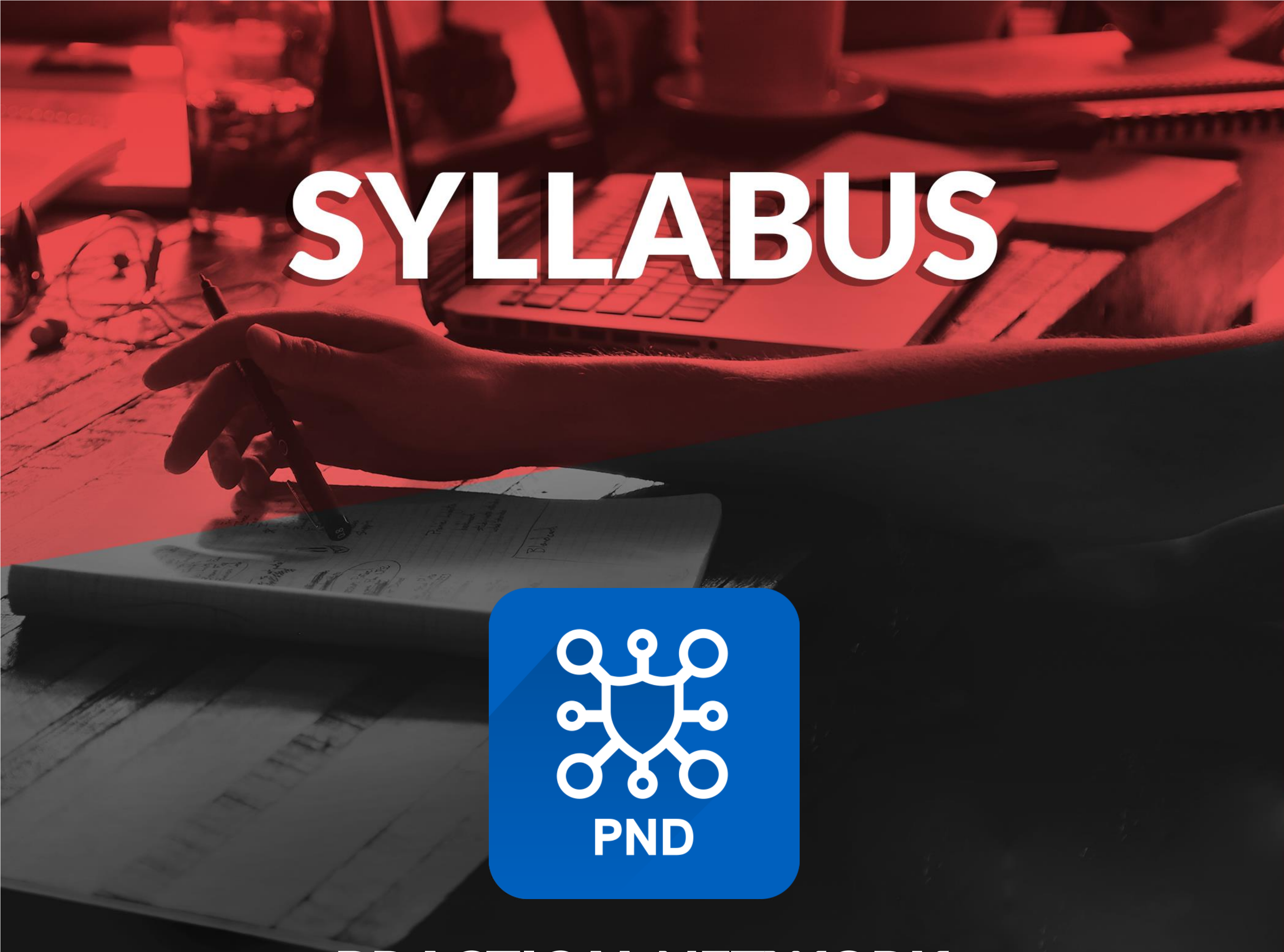

SYLLABUS

PND

PRACTICAL NETWORK DEFENSE

VERSION 1

The world's premiere online practical network defense 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

COURSE GOALS

Practical Network Defense is a practical self-study course which covers network and system security topics. The lessons include full practical setup guides, as well as virtual labs in Hera for the student to practice their new skills before deploying these technologies and strategies in a production network.

The course starts with an introductory section which covers security basics, the terms you need to know and a brief primer on TCP/IP. The primary sections of the course are divided up into network security and endpoint security. Network security will teach you secure network design concepts, configuration of network appliances such as switches, and a look into the secure configuration of firewalls, web filtering and advanced malware protection. The endpoint security section focuses mainly on Windows security, as most corporate networks have a majority of Windows systems. You will also learn Active Directory, Group Policy, patch management, endpoint hardening and the vulnerability management cycle.

These topics are taught in a practical manner with step-by-step guides on deploying the actual technology in use. You will leave this class knowing exactly how to accomplish these tasks.

The course also prepares you for the eLearnSecurity Network Defense Professional certification exam.

PRE-REQUISITES

This course explains many of the fundamental topics of information security: however, knowledge and experience of information technology skills prior to the class will be very beneficial for your learning. You should have a(n):

- Basic understanding of networking: TCP/IP, Routing
- Basic understanding of IT Security subjects
- Intermediate understanding of the Windows operating system

WHO SHOULD TAKE THIS COURSE

The PND training course is primarily geared towards Network/System administrators who manage an internal network and would like to protect their network from attacks or malware. Penetration testers and security assessors will also greatly benefit from this course as they will learn how to practically remediate many of the issues they discover and can provide a new value-added service. Additionally, penetration testers will also learn more about how different networks are defended and gain a better understanding of how to penetrate them.

- Penetration testers
- System Administrators
- IT Security Professionals
- Network Administrators
- IT Personnel

HOW AM I GOING TO LEARN THIS?

eLearnSecurity courses are very interactive, addictive, and presents content in such a way that it appeals to all learning styles. During this training course, you will have several guided labs. That will provide you with relevant and hands-on practical application experience. Do not expect the outdated way of learning, merely reading pages of theoretical methodologies.

IS THERE A FINAL EXAMINATION?

Yes. The final examination consists of two parts. The first part is a multiple-choice test. Once you have passed this, you will proceed to the hands-on examination. During the second part of your exam, you will have to remediate security issues and harden a virtual network against attacks.

WILL I GET A CERTIFICATE?

The PND course leads to the eNDP certification.

Once you have passed both parts of the final examination, you will be an “eLearnSecurity Network Defense Professional” and will granted the eNDP certification. You can print your shiny new certificate or have it shipped to you internationally.

ORGANIZATION OF CONTENTS

INTRODUCTION

The introductory section will provide you with the background knowledge you need to succeed in information security. These topics will add to and reinforce what you already know, and help to ensure that you have a more secure understanding of the topics in other modules.

- Module 1: Introduction
- Module 2: TCP
- Module 3: Attacks

NETWORK SECURITY

The network security section covers many aspects of securing the network through network design, several network appliances and properly hardening those appliances.

- Module 1: Perimeter Appliances
- Module 2: Secure Network Design – Part I
- Module 3: Firewall Configuration – Part I
- Module 4: Firewall Configuration – Part II
- Module 5: Secure Network Design – Part II
- Module 6: VPN
- Module 7: Switch Configuration

ENDPOINT SECURITY

In addition to network security, securing the endpoints is equally as important. This section will cover everything you need to get started in hardening your Windows environment. When it comes to securing your network, the approach is no longer planning for “if” an attacker gets into your network but “when.” Endpoint security is just as important as network security when it comes to reducing the attack surface and preventing lateral movement.

- Module 1: System Security
- Module 2: Active Directory
- Module 3: WSUS

- Module 4: Microsoft EMET
- Module 5: Group Policy Revisited
- Module 6: Endpoint Security
- Module 7: Printers
- Module 8: Vulnerabilities
- Module 9: Controlling Vendor Access

MODULE 1: INTRODUCTION

In this module, you will learn the basics of information security, including the ‘why,’ as well as the associated vocabulary. The terms will not only be referenced a lot in the course but will be used quite a bit throughout your information security career.

1. Introduction
    1.1. Opening Statements
    1.2. Security Background
    1.3. Terms

MODULE 2: TCP

How TCP works is a very important concept to understand. This module covers the OSI/TCP models, the connections themselves and how you can explore live connections yourself with Wireshark. Being able to understand and recognize different TCP connections helps you to identify potentially malicious traffic and understand network-related logs.

2. TCP
    2.1. OSI Model
    2.2. TCP Model
    2.3. TCP Flags
    2.4. TCP Connections
    2.5. Wireshark

MODULE 3: ATTACKS

As Sun Tzu said, “know your enemy.” This module explains some of the attack vectors you will be dealing with when it comes to defending your network. This module concludes with a full scenario of a company’s network being compromised.

3. Attacks
    3.1. Brute Force
    3.2. Exploits
    3.3. Denial of Service
    3.4. Web Attacks
    3.5. Client-Side Attacks
    3.6. Full Attack Example

MODULE 1: PERIMETER APPLIANCES

In this module, you will learn the majority of the network security appliances in use today. Although new appliances do not necessarily mean better security, knowing what is available and their purpose can aid in a secure network design.

1. Perimeter Appliances
- **1.1. Web filters**
- **1.2. Intrusion Prevention Systems**
- **1.3. Advanced Malware Protection**
- **1.4. Firewalls**
- **1.5. Virtual Private Networks**

MODULE 2: SECURE NETWORK DESIGN – PART I

One of the most important fundamental topics when it comes to securing a network is the design and topology of the network. This module will teach you the considerations and strategies used when planning for a secure network. Here we introduce more of the "theory" side before diving into the next practical modules to ensure you have a solid understanding of what we are trying to accomplish.

2. Secure Network Design – Part I
- **2.1. Topology**
- **2.2. DMZ**
- **2.3. Network Address Translation**
- **2.4. Access Control List**

MODULE 3: FIREWALL CONFIGURATION – PART I

When it comes to the perimeter or network segmentation, the firewall is an integral piece of technology. In this module, you will look at configuring a firewall appliance from start to finish, with focus on the ACL. This module also covers some of the Next Generation Firewall features such as application identification, IPS and web filtering. Although we focus on the configuration of two specific firewalls, our goal is to teach you the methodologies to configuring them as a whole so you can apply them to ANY firewall you come across.

Hera Labs are included in this module

3. Firewall configuration – Part I

- **3.1. Device Configuration**
- **3.2. Objects**
- **3.3. Network Setup**
- **3.4. NAT**
- **3.5. ACL**
- **3.6. FTP Example**

MODULE 4: FIREWALL CONFIGURATION – PART II

Some of today's firewalls and other network security appliances include advanced features, which allow you to secure your network even more. This module will show you some of these features to help you control, identify and prevent threats.

4. Firewall configuration – Part II

- **4.1. Advanced Malware Protection**
- **4.2. User Identification**
- **4.3. SSL Inspection and Decryption**

MODULE 5: SECURE NETWORK DESIGN – PART II

The first module introduced secure network design, which we will expand upon in this module. You will learn more about network segmentation at both the layer 3 and layer 2 levels. We will also brief you on some of the planning topics you will encounter when planning secure design.

5. Secure network design – Part II

- **5.1. Network Zones**
- **5.2. Secure Network Planning**
- **5.3. Segmentation**
- **5.4. Secure Switching**
- **5.5. Securing the Device**

MODULE 6: VPN

Providing secure remote access is becoming a very common requirement these days, whether it is a site to site tunnel or remote access for your mobile workforce. This module will teach you what you need to know about both, as well as walk you through practical examples of deploying them. It also covers both IPSEC site to site VPN, as well as remote client-access VPN using desktop VPN software.

Hera Labs are included in this module

6. VPN

- **6.1. The connection**
- **6.2. Site to site tunnels**
- **6.3. Remote Access VPN**
- **6.4. OpenVPN – Remote Access VPN**

MODULE 7: SWITCH CONFIGURATION

Switches are often overlooked in the security plan but can provide additional security at layer two. This module will look at setting up a switch, hardening the device itself and setting up many layer 2 security layers. As with the firewall module, we will focus on the configuration of one switch, but aim to teach you to apply the same methodologies to any switch you encounter.

7. Switch configuration

- **7.1. Initial Configuration**
- **7.2. DHCP-Snooping**
- **7.3. Port Security**
- **7.4. Dynamic ARP Inspection**
- **7.5. Segmentation**
- **7.6. Access Control Lists**

MODULE 1: SYSTEM SECURITY

This module introduces some of the core topics on system security. It covers the basics of the technologies and strategies involved in every endpoint protection plan.

1. System Security

- **1.1. Antivirus**
- **1.2. Endpoint Encryption**
- **1.3. Buffer Overflows**
- **1.4. Mitigations**
- **1.5. Virtualization**
- **1.6. Log Review**

MODULE 2: ACTIVE DIRECTORY

The foundation for any Windows network is Active Directory. It takes care of your access control, manages users and groups, and sets policies to control and harden your Windows domain-joined computers/servers via Group Policy. Finally, we will cover Active Directory Certificate Services and how to set it up correctly so you can implement a PKI.

Hera Labs are included in this module

2. Active Directory

- **2.1. Active Directory Basics**
- **2.2. Active Directory Integrated DNS**
- **2.3. Group Policy**
- **2.4. Group Policy Permissions**
- **2.5. Active Directory Certificate Services**

MODULE 3: WSUS

As you will learn in this course and may already know, patch management is essential to keeping your systems safe. This module will teach you how to setup and manage Windows Server Update Services so you can control and monitor the Windows patch levels in your environment. We will also introduce Windows Package Publisher, which is a free third-party tool which allows you to deploy third party updates via WSUS.

Hera Labs are included in this module

3. WSUS
    3.1. Install WSUS
    3.2. Setting up WSUS
    3.3. WSUS Group Policy
    3.4. WSUS Upkeep
    3.5. Extending WSUS

MODULE 4: MICROSOFT EMET

Vulnerabilities and exploits are growing exponentially. Signature-based IDS/IPS is the most efficient method to prevent attacks: in this module, you will learn about Microsoft EMET which makes a successful exploit much more “expensive” for the attacker. This program also helps to keep your network safer in the zero-day window when no patch is available for a given program or operating system.

Hera Labs are included in this module

4. Microsoft EMET
    4.1. Install WSUS
    4.2. Setting up WSUS
    4.3. WSUS Group Policy
    4.4. WSUS Upkeep
    4.5. Extending WSUS

MODULE 5: GROUP POLICY REVISITED

The first Active Directory module provided an introduction to Group Policy. In this module, we will take a look at several more Group Policy examples to show you different ways you can secure your Windows endpoints.

Hera Labs are included in this module

5. Group Policy Revisited
    5.1. Password Policies
    5.2. User Control
    5.3. Restricting Null Sessions
    5.4. Remote Desktop
    5.5. Controlling Removable Media

MODULE 6: ENDPOINT SECURITY

The first module introduced many of the endpoint security topics. This module will take a deeper dive into endpoint security and some of the specific things you should consider in your strategy. You will also see a couple of attacks and the practical mitigation steps to prevent them.

Hera Labs are included in this module

6. Endpoint Security
- **6.1. Common Pitfalls**
- **6.2. Third Party Programs**
- **6.3. User Access Control**
- **6.4. Mitigate Pass the Hash**
- **6.5. Advanced Security Products**
- **6.6. Practical Malware Defense**

MODULE 7: PRINTERS

Printers are usually overlooked yet sensitive information is usually sent to the printer via print or fax capabilities. In addition, many of today's printers run on a Linux kernel and are sometimes used as pivot points in attacks. This module will teach you the settings you need to configure to harden every printer on your network.

7. Printers
- **7.1. Hardening HP Printers**
- **7.2. Hardening Xerox Printers**

MODULE 8: VULNERABILITIES

An important part of any security program is vulnerability management. This module will teach you the steps of a vulnerability management program including port scans, vulnerability scans, reporting and remediation.

Hera Labs are included in this module

8. Vulnerabilities
- **8.1. Introduction**
- **8.2. Port scanning**

- **8.3. Nessus**
  - 8.3.1. Setting up Nessus
  - 8.3.2. Running First Scan
  - 8.3.3. Reviewing the Report
- **8.4. Qualys**
  - 8.4.1. Setting up Qualys
  - 8.4.2. Network Map
  - 8.4.3. Vulnerability Scan

MODULE 9: CONTROLLING VENDOR ACCESS

Understanding the need to give your vendors secure access to your network while protecting your network from their connection is crucial; many of the attacks over the past few years have stemmed from vendors being compromised and the attackers using the vendor's remote access to pivot deeper into their target's network. This module will look at some important factors to consider regarding vendor management and how to secure you against unwanted activity.

9. Controlling Vendor Access
- **9.1. Active Directory**
- **9.2. Network**
- **9.3. Group Policy Example**

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

2040 Martin Ave.
Santa Clara, CA, USA

Via Matteucci 36/38
Pisa, Italy

Apricot Tower, Dubai Silicon Oasis
Dubai, UAE