Practical Network Penetration Tester (PNPT) Training Syllabus and Exam Overview

Date: January 6th, 2022
Version 1.0

Copyright © TCM Security (tcm-sec.com)

Exam Overview

The PNPT exam is a one-of-a-kind ethical hacking certification exam that assesses a student's ability to perform an external and internal network penetration test at a professional level. Students will have **five (5) full days** to complete the assessment and an **additional two (2) days** to write a professional report.

To receive the certification, a student must:

- Perform Open-Source Intelligence (OSINT) to gather intel on how to properly attack the network
- Leverage their Active Directory exploitation skillsets to perform A/V and egress bypassing, lateral and vertical network movements, and ultimately compromise the exam Domain Controller
- Provide a detailed, professionally written report
- Perform a live 15-minute report debrief in front of our assessors, comprised of all senior penetration testers

Training Overview

The PNPT Training consists of five (5) full-length video courses designed to take a student with little to no background in ethical hacking to being able to pass the exam and earn the certification. Upon purchase, the student will automatically be enrolled in the TCM Academy (https://academy.tcm-sec.com) and be provided access to the following courses (please click on any link below to read further information about the courses):

- Practical Ethical Hacking (25 hours)
- Open-Source Intelligence (OSINT) Fundamentals (9 hours)
- External Pentest Playbook (3.5 hours)
- Linux Privilege Escalation for Beginners (6.5 hours)
- Windows Privilege Escalation for Beginners (7 hours)

In total, the student will receive over 50+ hours of video training. We strongly recommend that the courses be taken in the order listed above.

In addition to the course videos, students will have access to the course Discord, which provides a place to ask course related questions, receive assistance/troubleshooting, and network with other students and cybersecurity professionals. At the time of this writing, the Discord has over 25,000 active members and the training courses have over 200,000 enrollments.

Starting on the next page, you can review the Table of Contents, which includes the topics and subtopics for each course provided with the PNPT training option.

Table of Contents

Table of Contents 3

Practical Ethical Hacking – 25 Hours 17

Before We Begin 17

Special Thanks & Credits 17

Course Repo 17

PNPT Certification Path Progression 17

Introduction 17

Course Introduction 17

Course Discord 17

FAQ - Important 17

A Day in the Life of an Ethical Hacker 17

Notekeeping 17

Part 1 – Effective Notekeeping 17

Part 2 – Important Tools 17

Networking Refresher 17

Introduction 17

IP Addresses 17

MAC Addresses 17

TCP, UDP, and the Three-Way Handshake 17

Common Ports and Protocols 17

The OSI Model 17

Subnetting Part 1 17

Subnetting Part 2 17

Setting Up Our Lab 17

Installing VMWare / VirtualBox 17

Installing Kali Linux 17

Configuring VirtualBox 17

Introduction to Linux 18

Exploring Kali Linux 18

Sudo Overview 18

Navigating the File System 18

Users and Privileges 18

Common Network Commands 18

Network Commands Update 18

Installing and Updating Tools 18

Installing gedit 18

Viewing, Creating, and Editing Files 18

Scripting with Bash 18

Copyright © TCM Security (tcm-sec.com)

Introduction to Python 18
Introduction 18
Strings 18
Math 18
Variables and Methods 18
Functions 18
Boolean Expressions 18
Rational and Boolean Operators 18
Conditional Statements 18
Lists 18
Tuples 18
Looping 18
Important Modules 18
Advanced Strings 18
Dictionaries 18
Sockets 18
Building a Port Scanner 18
The Ethical Hacker Methodology 18
The Five Stages of Ethical Hacking 18
Information Gathering (Reconnaissance) 19
Passive Reconnaissance Overview 19
Identifying Our Target 19
Discovering Email Addresses 19
Gathering Breached Credentials with Breach-Parse 19
Gathering Breached Credentials with DeHashed 19
Hunting Subdomains Part 1 19
Hunting Subdomains Part 2 19
Identifying Website Technologies 19
Information Gathering with Burp Suite 19
Google Fu 19
Utilizing Social Media 19
Additional Learning (OSINT Fundamentals) 19
Scanning & Enumeration 19
Installing Kioptrix 19
Scanning with Nmap 19
Enumerating HTTP and HTTPS Part 1 19
Enumerating HTTP and HTTPS Part 2 19
Enumerating SMB 19
Enumerating SSH 19
Researching Potential Vulnerabilities 19

Our Notes So Far ... 19
Additional Scanning Tools ... 19
Scanning with Nessus Part 1 ... 19
Scanning with Nessus Part 2 ... 19
Exploitation Basics ... 19
Reverse Shells vs Bind Shells ... 19
Staged vs Non-Staged Payloads ... 19
Gaining Root with Metasploit ... 19
Manual Exploitation ... 19
Brute Force Attacks ... 19
Credential Stuffing and Password Spraying ... 19
Our Notes, Revisited ... 19
Mid-Course Capstone ... 20
Introduction ... 20
Set Up - Blue ... 20
Walkthrough - Blue ... 20
Set Up - Academy ... 20
Walkthrough - Academy ... 20
Walkthrough - Dev ... 20
Walkthrough - Butler ... 20
Walkthrough - Blackpearl ... 20
Introduction to Exploit Development (Buffer Overflows) ... 20
Required Installations ... 20
Buffer Overflows Explained ... 20
Spiking ... 20
Fuzzing ... 20
Finding the Offset ... 20
Overwriting the EIP ... 20
Finding Bad Characters ... 20
Finding the Right Module ... 20
Generating Shellcode and Gaining Root ... 20
Exploit Development Using Python3 and Mona ... 20
Active Directory Overview ... 20
Active Directory Overview ... 20
Physical Active Directory Components ... 20
Logical Active Directory Components ... 20
Active Directory Lab Build ... 20
Lab Overview and Requirements ... 20
Downloading Necessary ISOs ... 20
Setting Up the Domain Controllers ... 20

Setting Up the User Machines 20
Setting Up Users, Groups, and Policies 20
Joining Our Machines to the Domain 20
Lab Build – Cloud Alternative 20
Attacking Active Directory: Initial Attack Vectors 21
Introduction 21
LLMNR Poisoning Overview 21
Capturing NTLMv2 Hashes with Responder 21
Password Cracking with Hashcat 21
LLMNR Poisoning Defenses 21
SMB Relay Attacks Overview 21
Quick Lab Update 21
Discovering Hosts with SMB Signing Disabled 21
SMB Relay Attack Demonstration Part 1 21
SMB Relay Attack Demonstration Part 2 21
SMB Relay Attack Defenses 21
Gaining Shell Access 21
IPv6 Attacks Overview 21
Installing mitm6 21
Setting Up LDAPS 21
IPv6 DNS Takeover via mitm6 21
IPv6 Attack Defenses 21
Passback Attacks 21
Other Attack Vectors and Strategies 21
Attacking Active Directory: Post-Compromise Enumeration 21
Introduction 21
PowerView Overview 21
Domain Enumeration with PowerView 21
Bloodhound Overview and Setup 21
Grabbing Data with Invoke-Bloodhound 21
Enumerating Domain Data with Bloodhound 21
Attacking Active Directory: Post-Compromise Attacks 22
Introduction 22
Pass the Hash / Password Overview 22
Installing crackmapexec 22
Pass the Password Attacks 22
Dumping Hashes with secretsdump.py 22
Cracking NTLM Hashes with Hashcat 22
Pass the Hash Attacks 22
Pass Attack Mitigations 22
Token Impersonation Overview 22

Copyright © TCM Security (tcm-sec.com)

- Token Impersonation with Incognito 22
- Token Impersonation Mitigation 22
- Kerberoasting Overview 22
- Kerberoasting Walkthrough 22
- Kerberoasting Mitigation 22
- GPP / cPassword Attacks Overview 22
- Abusing GPP: Part 1 22
- Abusing GPP: Part 2 22
- URL File Attacks 22
- PrintNightmare (CVE-2021-1675) Walkthrough 22
- Mimikatz Overview 22
- Credential Dumping with Mimikatz 22
- Golden Ticket Attacks 22
- Conclusion and Additional Resources 22

Additional Active Directory Attacks 22

- Abusing ZeroLogon 22

Post Exploitation 22

- Introduction 22
- File Transfers Review 22
- Maintaining Access Overview 22
- Pivoting Lab Setup 22
- Pivoting Walkthrough 22
- Cleaning Up 22

Web Application Enumeration, Revisited 22

- Introduction 22
- Installing Go 22
- Finding Subdomains with Assetfinder 22
- Finding Subdomains with Amass 22
- Finding Alive Domains with Httprobe 22
- Screenshotting Websites with GoWitness 22
- Automating the Enumeration Process 22
- Additional Resources 22

Testing the Top 10 Web Application Vulnerabilities 23

- Introduction 23
- The OWASP Top 10 and OWASP Testing Checklist 23
- Installing OWASP Juice Shop 23
- Installing Foxy Proxy 23
- Exploring Burp Suite 23
- Introducing the Score Board 23
- SQL Injection Attacks Overview 23

Copyright © TCM Security (tcm-sec.com)

SQL Injection Walkthrough 23
SQL Injection Defenses 23
Broken Authentication Overview and Defenses 23
Testing for Broken Authentication 23
Sensitive Data Exposure Overview and Defenses 23
Testing for Sensitive Data Exposure 23
XML External Entities (XXE) Overview 23
XXE Attack and Defense 23
Broken Access Control Overview 23
Broken Access Control Walkthrough 23
Security Misconfiguration Attacks and Defenses 23
Cross-Site Scripting (XSS) Overview 23
Reflected XSS Walkthrough 23
Stored XSS Walkthrough 23
Preventing XSS 23
Insecure Deserialization 23
Using Components with Known Vulnerabilities 23
Insufficient Logging and Monitoring 23
Wireless Penetration Testing 23
Wireless Penetration Testing Overview 23
WPA PSK Exploit Walkthrough 23
Legal Documents and Report Writing 23
Common Legal Documents 23
Pentest Report Writing 23
Reviewing a Real Pentest Report 23
Career Advice 23
Career Advice 23
Open-Source Intelligence (OSINT) Fundamentals – 9 Hours 24
Introduction 24
Course Introduction 24
Course Discord 24
Important Disclaimer 24
OSINT Overview 24
What is OSINT? 24
Note Keeping 24
Taking Effective Notes 24
Sock Puppets 24
Introduction to Sock Puppets 24
Creating Sock Puppets 24
Search Engine OSINT 24

Search Engine Operators ... 24
Image OSINT ... 24
Reverse Image Searching ... 24
Viewing EXIF Data ... 24
Physical Location OSINT ... 24
Identifying Geographical Locations ... 24
Where in the World…Part 1 ... 24
Where in the World…Part 2 ... 24
Email OSINT ... 24
Discovering Email Addresses ... 24
Password OSINT ... 24
Introduction to Password OSINT ... 24
Hunting Breached Password Part 1 ... 24
Hunting Breached Passwords Part 2 ... 24
Username OSINT ... 25
Hunting Usernames and Accounts ... 25
People OSINT ... 25
Searching for People ... 25
Voter Records ... 25
Hunting Phone Numbers ... 25
Discovering Birthdates ... 25
Searching for Resumes ... 25
Social Media OSINT ... 25
Twitter OSINT Part 1 ... 25
Twitter OSINT Part 2 ... 25
Twitter OSINT Part 3 ... 25
Facebook OSINT ... 25
Instagram OSINT ... 25
Snapchat OSINT ... 25
Reddit OSINT ... 25
LinkedIn OSINT ... 25
TikTok OSINT ... 25
Website OSINT ... 25
Website OSINT Part 1 ... 25
Website OSINT Part 2 ... 25
Website OSINT Part 3 ... 25
Business OSINT ... 25
Hunting Business Information ... 25
Wireless OSINT ... 25

Wireless OSINT 25
Building an OSINT Lab 25
Building an OSINT Lab Part 1 25
Building an OSINT Lab Part 2 25
Building an OSINT Lab Part 3 25
Working with OSINT Tools 26
Introduction 26
Image and Location OSINT 26
Hunting Emails and Breached Data 26
Username and Account OSINT 26
Phone Number OSINT 26
Social Media OSINT 26
Website OSINT 26
Exploring OSINT Frameworks 26
Other Tools 26
OSINT Automation Foundations 26
Automating Website OSINT 26
Course Challenge 26
Course Challenge Overview 26
Course Challenge 26
Course Challenge Walkthrough 26
OSINT Report Writing 26
Writing an OSINT Report 26
Conclusion & Additional Resources 26
Conclusion & Additional Resources 26
External Pentest Playbook – 3.5 Hours 27
Introduction 27
Course Introduction 27
Course Discord 27
Before We Start 27
Objectives of an External Pentest 27
Checklists, FTW 27
Rules of Engagement 27
Verifying Scope 27
Client Communications 27
Kicking Off 27
Attack Strategy 27
Vulnerability Scanning 27
Reviewing & Extracting Information 27

Information Gathering / OSINT 27
Overview 27
Hunting Breached Credentials 27
Identifying Employees & Emails 27
Enumerating Valid Accounts (Pre-Attack) 27
Other Useful Information 27
Attacking Login Portals 27
Overview & Strategy 27
Attacking O365 27
Attacking OWA 27
Attacking Other Portals 27
Bypassing MFA 27
Escalating Access 27
Strategy & Walkthrough 27
Report Writing 27
Report Writing 27
Common Pentest Findings 28
Overview 28
Insufficient Authentication Controls 28
Weak Password Policy 28
Insufficient Patching 28
Default Credentials 28
Insufficient Encryption 28
Information Disclosure 28
Username Enumeration 28
Default Web Pages 28
Open Mail Relays 28
IKE Aggressive Mode 28
Unexpected Perimeter Services 28
Insufficient Traffic Blocking 28
Undetected Malicious Activity 28
Historical Account Compromises 28
Wrapping Up 28
Client Debriefs 28
Attestation Letters 28
Client Retests 28
Conclusion 28
Course Conclusion 28
Linux Privilege Escalation for Beginners – 6.5 Hours 29
Introduction 29

Course Introduction 29
Course Discord 29
Course Tips & Resources 29
Lab Overview & Initial Access 29
Lab Overview & Initial Access 29
Initial Enumeration 29
System Enumeration 29
User Enumeration 29
Network Enumeration 29
Password Hunting 29
Exploring Automated Tools 29
Introduction 29
Exploring Automated Tools 29
Escalation Path: Kernel Exploits 29
Kernel Exploits Overview 29
Escalation via Kernel Exploit 29
Escalation Path: Passwords & File Permissions 29
Overview 29
Escalation via Stored Passwords 29
Escalation via Weak File Permissions 29
Escalation via SSH Keys 29
Escalation Path: Sudo 29
Sudo Overview 29
Escalation via Sudo Shell Escaping 29
Escalation via Intended Functionality 29
Escalation via LD_PRELOAD 29
Challenge Overview 29
Challenge Walkthrough 29
CVE-2019-14287 Overview 30
Escalation via CVE-2019-14287 30
Overview and Escalation via CVE-2019-18634 30
Escalation Path: SUID 30
SUID Overview 30
Gaining a Foothold 30
Escalation via SUID 30
Escalation Path: Other SUID Escalation 30
Escalation via Shared Object Injection 30
Escalation via Binary Symlinks 30
Escalation via Environmental Variables 30

Copyright © TCM Security (tcm-sec.com)

Escalation Path: Capabilities ... 30
Capabilities Overview ... 30
Escalation via Capabilities ... 30
Escalation Path: Scheduled Tasks ... 30
Cron & Timers Overview ... 30
Escalation via Cron Paths ... 30
Escalation via Cron Wildcards ... 30
Escalation via Cron File Overwrites ... 30
Challenge Overview ... 30
Challenge Walkthrough ... 30
Escalation Path: NFS Root Squashing ... 30
Overview & Escalation via NFS Root Squashing ... 30
Escalation Path: Docker ... 30
Overview ... 30
Gaining a Foothold ... 30
Escalation via Docker ... 30
Capstone Challenge ... 31
Capstone Overview ... 31
Capstone Walkthrough #1 ... 31
Capstone Walkthrough #2 ... 31
Capstone Walkthrough #3 ... 31
Capstone Walkthrough #4 ... 31
Capstone Walkthrough #5 ... 31
Wrapping Up ... 31
Conclusion ... 31
Windows Privilege Escalation for Beginners – 7 Hours ... 32
Introduction ... 32
Course Introduction ... 32
Course Discord ... 32
Resources & Tips for Succes ... 32
Gaining a Foothold ... 32
Introduction ... 32
Gaining a Foothold (Box 1) ... 32
Initial Enumeration ... 32
System Enumeration ... 32
User Enumeration ... 32
Network Enumeration ... 32
Password Hunting ... 32
AV Enumeration ... 32

Exploring Automated Tools 32
Automated Tools Overview 32
Exploring Automated Tools 32
Escalation Path: Kernel Exploits 32
Kernel Exploits Overview 32
Escalation with Metasploit 32
Manual Kernel Exploitation 32
Escalation Path: Passwords and Port Forwarding 32
Overview 32
Gaining a Foothold (Box 2) 32
Escalation via Stored Passwords 32
Escalation Path: Windows Subsystem for Linux 32
Overview 32
Gaining a Foothold (Box 3) 32
Escalation via WSL 32
Impersonation and Potato Attacks 33
Token Impersonation Overview 33
Impersonation Privileges Overview 33
Potato Attacks Overview 33
Gaining a Foothold (Box 4) 33
Escalation via Potato Attack 33
Alternate Data Streams 33
Escalation Path: getsystem 33
getsystem Overview 33
Escalation Path: RunAs 33
Overview of RunAs 33
Gaining a Foothold (Box 5) 33
Escalation via RunAs 33
Additional Labs 33
Overview of TryHackMe Labs 33
Escalation Path: Registry 33
Overview of Autoruns 33
Escalation via Autorun 33
AlwaysInstallElevated Overview and Escalation 33
Overview of regsvc ACL 33
regsvc Escalation 33
Escalation Path: Executable Files 33
Executable Files Overview 33
Escalation via Executable Files 33

Copyright © TCM Security (tcm-sec.com)

Escalation Path: Startup Applications 33
Startup Applications Overview 33
Escalation via Startup Applications 33
Escalation Path: DLL Hijacking 33
Overview and Escalation via DLL Hijacking 33
Escalation Path: Service Permissions (Paths) 34
Escalation via Binary Paths 34
Escalation via Unquoted Service Paths 34
Challenge Overview 34
Gaining a Foothold 34
Escalation via Unquoted Service Path – Metasploit 34
Manual Challenge Walkthrough 34
Escalation Path: CVE-2019-1388 34
Overview of CVE-2019-1388 34
Gaining a Foothold 34
Escalation via CVE-2019-1388 34
Capstone Challenge 34
Capstone Overview 34
Capstone Walkthrough 1 34
Capstone Walkthrough 2 34
Capstone Walkthrough 3 34
Capstone Walkthrough 4 34
Capstone Walkthrough 5 34
Conclusion 34
Conclusion 34

Copyright © TCM Security (tcm-sec.com)

Last Page

Copyright © TCM Security (tcm-sec.com)