Network Penetration Testing Essentials (PEN-100)

PEN-100: Network Penetration Testing Essentials is a foundational OffSec training for aspiring ethical hackers. Learn Linux and Windows command line, network protocols, scripting with Bash and Python, and essential security tools like Nmap and Metasploit. Build a strong ethical hacking mindset with hands-on practice in reconnaissance, exploitation, and post-exploitation techniques. Perfect for beginners looking to start a cybersecurity career.

CBT Nuggets course material →

STUDY PLAN

WEEK 1

Introduction to PEN-100 — 154 min.

What will Pen-100 cover?	13
Understanding Virtualization	9
We need permission!	11
Challenge	1

Installing and Configuring Kali

What is Kali?	7
Picking our Kali	10
Downloading and installing Kali	23
Live Kali	3
Challenge	6

Linux Basics

POSIX-Based Systems	3
Formatting	9
Directory Structure	7
Missing File Types?	6
File Permissions	9
Usernames and Passwords	7
Services and Logs	9
Challenge	2

Installing and Configuring Windows

Getting to know Windows	8
Formatting	11

WEEK 2 — 156 min.

Directory Structuring	8
File Types	5
Username and Passwords	6
Challenge	3

Windows Basics

Getting into the Windows Operating System	4
Local Security Policy	15
Registry	11
Temporary and Hidden Folders	9
Services and Logs	9
Challenge	1

Linux Networking

Linux Networking	3
ifconfig	13
DNS Configuration	5
Routing Configuration	7
iptables	11
Challenge	4

Network Access Link Layer 2

Windows Networking	22
IP Link Layer 3	1
Network Access Link Layer 2	1
Identifying Layer 3	1
Identifying Layer 2	1
Layer 3 Communication	1
Layer 2 Communication	1
Setting up IPs on the interface	12

IP Layer 3

Windows Networking	22
IP Link Layer 3	1
Network Access Link Layer 2	1
Identifying Layer 3	1
Identifying Layer 2	1
Layer 3 Communication	1
Layer 2 Communication	1
Setting up IPs on the interface	12

Windows Networking

Windows Networking	22
IP Link Layer 3	1
Network Access Link Layer 2	1
Identifying Layer 3	1
Identifying Layer 2	1
Layer 3 Communication	1
Layer 2 Communication	1
Setting up IPs on the interface	12

WEEK 3

152 min.

Windows Firewall	5
Where is Layer 3 in our Packet?	1
Where is Layer 2 in our Packet?	1
Wireshark	4
Packet Examples	1

Packet Examples	1
Challenge	2
Windows Firewall	5
Where is Layer 3 in our Packet?	1
Where is Layer 2 in our Packet?	1
Wireshark	4
Packet Examples	1
Packet Examples	1
Challenge	2
Windows Firewall	5
Where is Layer 3 in our Packet?	1
Where is Layer 2 in our Packet?	1
Wireshark	4
Packet Examples	1
Packet Examples	1
Challenge	2

Networking Basics

Understanding how the network talks	5
Scoping things out	13
Capturing some traffic	18
Active and passive listening	5
Challenge	12

Wireless Networking Basics

Wireless Networks	5
Heat mapping	8
Wireless Channels and Rogue Access Points	10
Wireless Promiscuous	5
Kismet	12
Challenge	4

PowerShell Scripting

Baby steps before running	12
Where do we script at?	9
Checking system online status	12
Scripting for more details	3

WEEK 4

152 min.

Challenge	9

Python Scripting

Let's learn another loop	8
Why Python?	12
Scanning with Python	12
What's the difference between the two?	4
Challenge	8

Bash Scripting

Bash is a bit stronger than its Windows command prompt counterpart. It's the default on most POSIX-based systems and is what we've been referring to as a terminal. Before we begin...	7
Scripting in Bash	12
Making sure we stay in Bash	7

Creating a program to run in Bash	16
Challenge	13
Script Resource	1

Monitoring with Kali

Kali being used for good	16
Monitoring and discovering networks	21
Monitoring for hidden networks	6

WEEK 5

154 min.

Challenge	12

Metasploit Framework

Knowing our targets	3
Intro to the Metasploit Framework	4
Web Application Backbone	29
Metasploit Startup and Workspaces	12

Cryptography

Overview	1
Supplemental File	1
Cryptography Overview	6
Synchronous Crypto	8
Synchronous Crypto Examples	11
Asynchronous Crypto	7
Asynchronous Crypto Example	10
Cryptography Review	1
Overview	1

Web Application Understanding

Knowing our targets	3
Intro to the Metasploit Framework	4
Web Application Backbone	29
Metasploit Startup and Workspaces	12

WEEK 6

116 min.

Discovering Web Application use on a target	5
Challenge	9
Managing Metasploit Sessions	8
Using Meterpreter	15
Metasploit Framework Review	2

Discovering Web Application use on a target	5
Challenge	9
Managing Metasploit Sessions	8
Using Meterpreter	15
Metasploit Framework Review	2

Introduction to Active Directory

What is Active Directory?	4
Installing Active Directory	9
Post Install	11
User and Group information	8
Policy Enforcement	6
Challenge	8