

# Cybersecurity White Hat Hacking v10

This White Hat Hacking v10 training covers how to lawfully identify weaknesses and vulnerabilities of a system, and improve your network's security posture. With this security training, you'll learn how to scan networks for vulnerabilities, use Kali Linux to (legally) hack into systems, and write reports on how you did it. Use this course for penetration and vulnerability exam prep, skills development for security professionals, or to create training plans for your team.

[CBT Nuggets course material](#) →

## WEEK 1

### Build and Configure your White Hat Hacking Lab 151 min.

Getting the Most From Your Time	2
Building a LAB: Concepts	6
Building a LAB: Networking	9
Deploy a Kali Linux VM	14
Adding Metasploitable to Your Lab	10
Adding Windows to Your Lab	14
Configure a Static IP on Kali	4

### Prerequisite Hacking Knowledge

Overview	1
Ethics and Hacking	7
Hacking Vocabulary	5
InfoSec Concepts	5
Attack Categories, Types, and Vectors	4
Five Phases of Hacking	6

### Footprinting and Reconnaissance Tools

Overview	1
Footprinting and Reconnaissance Concepts	10
Search Engine Tools	7
Hacking Using Google	12
Website Recon Tools	9
Metagoofil Metadata Tool	3
Email Headers for Footprinting	5
Using WHOIS for Recon	4
DNS Tools	10

## WEEK 2

### Network Scanning

153 min.

Overview	1
Network Scanning Overview	4
Network Scanning Methodology	8
Port Discovery	10
Stealth Idle Scanning	10
OS and Application Fingerprinting	10

### Find Vulnerabilities

Overview	1
Vulnerability Scanning	8
Network Mapping Tools	4
NMAP	37
Scapy	23
Hping3	28
Proxy Servers	8

## WEEK 3

151 min.

Using Public Proxy Services	5
Shellshock	5

### Gain More Information with Enumeration Tools

Overview	1
Enumeration Concepts	6
NetBIOS Enumeration	7
SNMP Enumeration Concepts	9
SNMP Enumeration Tools	8

LDAP Enumeration Concepts	4
LDAP Enumeration Example	6
NTP Enumeration	7
SMTP Enumeration	8

### Hack Passwords and Systems

Overview	1
System Hacking Overview	9
Password Cracking Concepts	11
Password Attack Example: MITM and Sniffing	12
Rainbow Crack Lab Setup	9
Rainbow Crack Demonstration	8
Password Reset Hacking	7
DHCP Starvation	11
Remote Access	15

## WEEK 4

154 min.

NTFS Alternate Data Streams Exploit	8
Steganography with OpenPuff	8
Steganography with SNOW	6
Covering Tracks	7

### Understand Common Malware Types

Overview	1
Malware Overview	10
Spyware	8
Buffer Overflow	13
Trojan Overview	11

Creating a Trojan	12
Virus Overview	12
Virus Creation	8
Detecting Malware	17
Malware Analysis	9
File Verification via Hash	9

### Network Sniffing Tools

Overview	1
Sniffing Overview	12

## WEEK 5

157 min.

CAM Table Attack and Port Security	10
DHCP Snooping	11
Dynamic ARP Inspection (DAI)	8

### Understand Social Engineering

Overview	1
Social Engineering Concepts	6
Social Engineering Phases	4
Social Engineering Prevention	3

### Common Types of Cyber Attacks

Overview	1
DoS and DDoS Overview	9
DoS and DDoS Prevention	7
Session Hijacking Overview	11
Reducing the Risk of Session Hijacking	5

Firewall Evasion	13
Firewall ACL Example	15
NAT and PAT Fundamentals	12
IDS/IPS Evasion	17
Honeypots	12
Hacking Web Servers	10

## WEEK 6

165 min.

OWASP Broken Web Application Project	11
Web App Vulnerabilities: WordPress	9
SQL Introduction	9
SQL Injection	16

### Understand Wireless Technologies for Hacking Purposes

Overview	1
Wireless Hacking Overview	12
Wireless Topologies and Vocabulary	20
Standards and Regulations	15
RF Fundamentals	21
Antenna Fundamentals	13
WLAN Frame Types	22
WLAN Frame Flow	15

## WEEK 7

151 min.

### Hack Wireless Technologies

Overview	1
Uncovering Hidden SSIDs	12

Bypassing MAC Address Filters	15
Breaking WPA2 Wireless	10
Rogue Wireless Access Points	24
Wireless Mis-Association Attacks	16
MITM Using Wireless Bridging	16
Protecting Wireless	6

### Hack Mobile and Cloud Technologies

Overview	1
Using an Android VM	3
Malware for Mobile	11
Mobile Device Risks	6
Improving Mobile Security	6
Cloud Computing Overview	9
Cloud Computing Security Concerns	6
Cloud Computing Security Benefits	7

## WEEK 8

**141 min.**

IoT Security Overview	5
IoT Web, Cloud, and Mobile Interfaces	6

### Understand Encryption

Overview	1
Symmetrical Encryption Concepts	9
Hashing Concepts for Data Integrity	4
Asymmetrical Encryption Concepts	4

### Secure your Information and Systems

Overview	1
Control Types	4
Multifactor Authentication	4
CIA: Confidentiality, Integrity, and Availability	2
Quantifying Risk	6
Separation of Duties	6
Centralized Identity Management	6
Kerberos and Single Sign On (SSO)	7
Backups and Media Management	4
Operations Security Controls	5
Physical Security Controls	5
Incident Response	3
VPNs	4
Disaster Recovery Planning	5

### Tips and Tools when Pen Testing

Overview	1
Pen Testing Tips	10
Useful Tools	11
Case Study for Security	20
Additional Resources	4