Penetration Testing

Master cybersecurity methods and tools in this intermediate Penetration Testing training. Learn techniques like white-box, black-box, and grey-box testing, and use Kali Linux for vulnerability analysis. This Penetration Testing course is ideal for IT professionals with network or systems experience, this course covers tools like BackTrack, WPA2 cracking, DNS spoofing, and exploiting systems, helping you become a skilled penetration tester.

CBT Nuggets course material →

STUDY PLAN

WEEK 1	Penetration Testing with Linux Tools (v1.0.2)	151 min.
	Supplemental File	1
	Welcome to the Tools of BackTrack and Kali Linux	7
	What is BackTrack?	4
	Install BT on a Virtual Machine	13
	Connecting to the Network	17
	Updating S/W and Using Integrated Help	7
	BT Wireless TX Power	10
	Uncovering Hidden SSIDs	12
	Bypassing MAC Address Filters	14
	Breaking WPA2 Wireless	10
	Rogue Wireless Access Points	24
	Wireless Mis-Association Attacks	16
	MITM Using Wireless Bridging	16

WEEK 2		171 min.
	Nmap: King of Scanners	36
	DHCP Starvation	12
	Vote for BT - as the new STP Root Bridge	19
	CDP Flooding	14
	Taking over HSRP	7
	DTP and 802.1q Attacks	22
	ARP Spoofing MITM	16
	Metasploit Framework	19
	PWNing a System with MSF	26

WEEK 3

152 min.

Creating a "Pivot Point"	18
Social-Engineer Toolkit (SET)	20
Ettercap and Xplico	18
DNS Spoofing	13
Hydra	22
Maltego	14
Kali Linux	15
Burp Suite	14
Raspberry Pi & Kali Linux	18

WEEK 4

163 min.

Scapy	23
Hping3	28
Parasite6	15
IPv6 THC Tools	28
Custom Password Lists	13
Hashes and Cracking Passwords	18
Rainbow Tables and Ophcrack	15
Wireshark	23

WEEK 5

69 min.

Virtual Test Environment	20
Detecting Rootkits	11

Penetration Testing Defined

Overview	1
What is Penetration Testing?	4
Modern Threat Landscape	6
Penetration Testing Methodologies	7
Penetration Testing Lab Fundamentals	10
Leveraging the Cloud for Labs	7
Where to Next?	1

Last updated 12.3.2024