

Penetration Testing with Linux Tools

This penetration testing training prepares learners to use Kali Linux for penetration testing and vulnerability analysis. Discover essential tools like Backtrack, uncover hidden SSIDs, and execute spoofing attacks.

Designed for IT professionals with networking or programming experience, this Linux training prepares you to perform authorized penetration tests on wired and wireless networks, advancing your skills toward becoming a penetration tester.

[CBT Nuggets course material](#) →

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

32 min.

Virtual Test Environment	20
Detecting Rootkits	11