Linux Professional Institute Security Essentials (020-100)

This Linux Professional Institute Security Essentials (020-100) training covers how to implement best practices in network security maintenance, identify vulnerabilities, and respond effectively to incidents in Linux-based IT infrastructures. You'll learn cybersecurity skills that apply in any environment, as well as techniques and tools that are particular to Linux environments. The LPI Security Essentials certification is an excellent start for a cybersecurity career, and this 020-100 exam prep will prepare you to earn it.

CBT Nuggets course material →

STUDY PLAN

WEEK 1

Goals, Roles, and Actors — 155 min.

IT Goal: Making Resources Available	6
IT Goal: Making Resources Secure	11
Four Pillars of Security	8
Common Hacker Goals	6
Types of Hackers	6
Validation	4

Risk Assessment and Management

Zero-Day and Bug Bounty	8
Privilege Escalation	10
Privilege Escalation Demo	10
Penetration Testing	5
ISMS, IRPs, and CERT	10
Untargeted Attacks and Advanced Persistent Threats (APT)	12
Bonus: Drive-By Malware in Action	4
Validation	4

Ethical Behavior

Intro: IT Access and Responsibility	9
Case Study: Edward Snowden	7
Personal and Private Data	10
Web Data Visibility	8
Regulatory Compliance	8
Example of Data Breach Disclosure	4
Your Data on Social Media	5

WEEK 2

162 min.

Handling Potentially Illegal Information	5
Validation	5

Implement Encryption

Describe Encryption and its Use	7
Encrypt Data at Rest	18
Encrypt Data in Transit	13
Data in Use	13
Validation	9

Encryption Types and Protocols

The Symmetric Encryption Concept	6
The Case for Symmetric Encryption	9
Symmetric Encryption Details	10
Symmetric Encryption Algorithms	5
Asymmetric Encryption	6
Perfect Forward Secrecy	2
RSA and ECC Encryption Algorithms	4
Validation	5

Public Key Infrastructure (PKI)

Understanding PKI Operation	11
Identifying and Extracting a Web Cert	7
Handling Untrusted Certificates	10
Certificate Signing Requests	17

WEEK 3

154 min.

Validation	5

X.509, Web Certificates, and Hashing

X.509 Concepts and Fields	2
Obtaining and Using Web Certificates	10
How SSL/TLS Operate	9
Hash Data	15
Compare Hashing and Encryption	3
Validation	1

Email Encryption and Signatures

PGP and GPG Overview	5
Configure Thunderbird for OpenPGP	16
Encrypt and Sign Email with PGP	11
Encrypt and Sign Email with S/MIME	9
Encryption and Gmail	3
Validation	2

Intro to PC Hardware

Motherboard Overview	10
Motherboard Diagram	3
Motherboard Form Factors and BIOS	8
Processors	13
Memory (RAM)	8
Hard Disk Drive Physical Characteristics	4
Solid State Drive Characteristics	7
Peripherals and Other Miscellaneous Devices	6
Validation	4

WEEK 4

Application and OS Sources — 167 min.

Firmware and its Risks	11
Mobile Software	7
Jailbreaking, Rooting, and the Risks	10
Securing Applications and Operating Systems	9
Protection via Isolation	10
Validation	10

Updates, Common Vulnerabilities, and Firewalls

Update Mobile Devices	6
Update Linux Devices	9
Update Windows	6
Buffer Overflow	5
SQL Injection	5
Implement Firewall Protection	17
Validation	12

Malware

Common Types of Malware Part 1	9
Common Types of Malware Part 2	10
Camera, Microphone Hijacking	4
Symptoms of Malware	8
Understanding Virus and Malware Scanners	19

WEEK 5

153 min.

Validation	6

Data Availability

Understand the Importance of Backups	9
Recovery Point Objective and Recovery Time Objective	6
Backup Location Strategy	6
Backup Type: Full	3
Backup Type: Differential	6
Backup Type: Incremental	5
Backup Media and Drives	8
Backup Security	5
Backup Solutions	11
Understanding of data storage, access, and sharing in cloud services	9
Validation	11

Networks and the Internet

Network Equipment	12
IP Basics	9
Binary Subnet Masks	9
Classful Subnet Masks and Private IP Addresses	4
Routing Network Traffic	4
Switch Traffic	5
Validation	3

Protocols and Vulnerabilities

TCP and UDP Vulnerabilities	22

WEEK 6

152 min.

TCP and UDP Ports	6
Other Common Protocol Vulnerabilities	12

Validation	5

DHCP, DNS, IPv6, and Cloud Computing

Introduction	1
Understanding DHCP	12
Understanding DNS	8
Forward and Reverse DNS	8
IPv6 Addresses	6
Understanding the Cloud	9
A Quick Tour of Azure	9
The Cloud - It's Not Just in the Sky!	1
IaaS, PaaS, and SaaS	8
Validation	3

Wireless Networking

Wired Equivalency Protocol (WEP)	8
WiFi Protected Access (WPA) + WPA2 and WPA3	8
WiFi Passwords	3
Configure WiFi Security	17
Understand Implications of Link-Layer Access	3
Validation	3

Network Encryption and Anonymity

Virtual Private Network (VPN) Overview	4
VPN Common Uses	10
Common VPN Features	8

WEEK 7

151 min.

VPN Disadvantages	5
Proxy Servers	6
The Onion Router (TOR)	13
Validation	3

Principles of Digital Identity

Authentication	16
Using a Security Key	7
Windows Hello Facial and Fingerprint Recognition	4
Security Questions and Account Recovery Tools	9
Authorization and Accounting	1
Validation	1

Passwords

Password Practices to Avoid	10
Password Best Practices	9
How Passwords are Stored	12
Common Attacks Against Passwords	9
Password Leaks	2
Using a Password Manager	8
Validation	2

Confidentiality and Secure Communication

The Email & Marketing Landscape	8
Spam and its Impact	7
Spam Filters	10
Handling Attachments and Links	9

WEEK 8

103 min.

Advantages of Messaging Apps 4

Social Media Messaging 4

E2EE Messaging Apps 5

Validation 2

Social Engineering and Handling Information

Introduction to Social Engineering 6

Social Engineering Psychology 12

Social Engineering Attacks 14

Social Engineering Improvements, and Protection 7

Data Classification and NDAs 4

Validation 1

Privacy Protection

Where is Personal Data Exposed? 6

Cyberbullying 4

Cyberstalking 4

Cybermobbing, Doxxing, and Fraudulent Accounts 6

Cookie Handling 9

Browser Privacy Settings 8

Browser Security Settings 5

Validation 2

Last updated 12.3.2024