Laboratorio COMPTIA SECURITY+

LABORATORIO COMPTIA SECURITY+

01: Exploring the Lab Environment
02: Scanning and Identifying Network Nodes
03: Intercepting and Interpreting Network Traffic with Packet Sniffing Tools
04: Analyzing the Results of a Credentialed Vulnerability Scan
05: Installing, Using, and Blocking a Malware-based Backdoor
06: Performing Network Reconnaissance and Vulnerability Scanning
07: Managing the Life Cycle of a Certificate
08: Managing Certificates with OpenSSL
09: Auditing Passwords with a Password Cracking Utility
10: Managing Centralized Authentication
11: Managing Access Controls in Windows Server
12: Configuring a System for Auditing Policies
13: Managing Access Controls in Linux
14: Configuring Identity and Access Management Controls
15: Implementing a Secure Network Design
16: Configuring a Firewall
17: Configuring an Intrusion Detection System
18: Implementing Secure Network Addressing Services
19: Implementing a Virtual Private Network
20: Implementing a Secure SSH Server
21: Implementing Endpoint Protection
22: Securing the Network Infrastructure
23: Identifying Application Attack Indicators
24: Identifying a Browser Attack
25: Implementing PowerShell Security
26: Identifying Malicious Code
27: Identifying Application Attacks
28: Managing Data Sources for Incident Response
29: Configuring Mitigation Controls
30: Acquiring Digital Forensics Evidence
31: Backing Up and Restoring Data in Windows and Linux
32: Managing Incident Response, Mitigation and Recovery