Laboratorio COMPTIA SECURITY+ SY0-701

LABORATORIO COMPTIA SECURITY+ - SY0-701

1. Assisted Lab: Exploring the Lab Environment
2. Assisted Lab: Perform System Configuration Gap Analysis
3. Assisted Lab: Configuring Examples of Security Control Types
4. Assisted Lab: Finding Open Service Ports
5. Assisted Lab: Using SET to Perform Social Engineering
6. Applied Lab: Using Storage Encryption
7. Assisted Lab: Using Hashing and Salting
8. Assisted Lab: Managing Password Security
9. Assisted Lab: Managing Permissions
10. Assisted Lab: Setting up Remote Access
11. Assisted Lab: Using TLS Tunneling
12. Assisted Lab: Using Containers
13. Assisted Lab: Using Virtualization
14. Assisted Lab: Implement Backups
15. Assisted Lab: Performing Drive Sanitization
16. Assisted Lab: Exploiting and Detecting SQLi
17. Assisted Lab: Working with Threat Feeds
18. Assisted Lab: Performing Vulnerability Scans
19. Assisted Lab: Understanding Security Baselines
20. Applied Lab: Implementing a Firewall
21. Assisted Lab: Using Group Policy

22. Applied Lab: Hardening
23. Assisted Lab: Performing DNS Filtering
24. Assisted Lab: Configuring System Monitoring
25. Applied Lab: Incident Response: Detection
26. Applied Lab: Performing Digital Forensics
27. Assisted Lab: Performing Root Cause Analysis
28. Assisted Lab: Detecting and Responding to Malware
29. Assisted Lab: Understanding On-Path Attacks
30. Adaptive Lab: Using a Playbook
31. Assisted Lab: Implementing Allow Lists and Deny Lists
32. Assisted Lab: Performing Reconnaissance
33. Assisted Lab: Performing Penetration Testing
34. Assisted Lab: Training and Awareness through Simulation
35. Capstone Lab: Discovering Anomalous Behavior
36. Assisted Lab: Use Cases of Automation and Scripting
37. Applied Lab: Using Network Sniffers