https://www.it4all.tech/

IT4all Security Pro

Course Content

Expiration date: December 31, 2021

This course prepares you to pass the CompTIA Security+ certifications. The course prepares you to implement processes to protect an organization's assets against danger, damage, loss, and criminal activity.

Certification is so important because it gives potential employers information they need when making hiring decisions. Basically, having certifications gives you a critical boost during the application and interview process.

Course outline

1.0: Introduction
- 1.1: Security Overview
- 1.2: Using the Simulator

2.0: Security Basics
- 2.1: Understanding Attacks
- 2.2: Defense Planning
- 2.3: Access Control
- 2.4: Cryptography Basics
- 2.5: Network Monitoring
- 2.6: Incident Response

3.0: Policies, Procedures, and Awareness
- 3.1: Security Policies
- 3.2: Risk Management
- 3.3: Business Continuity
- 3.4: Manageable Network Plan
- 3.5: Social Engineering
- 3.6: App Development and Deployment
- 3.7: Employee Management
- 3.8: Mobile Devices
- 3.9: Third-Party Integration

4.0: Physical
- 4.1: Physical Threats
- 4.2: Device Protection
- 4.3: Network Infrastructure Protection
- 4.4: Environmental Controls

5.0: Perimeter
- 5.1: Recon and Denial
- 5.2: Spoofing and Poisoning
- 5.3: Security Appliances
- 5.4: Demilitarized Zones (DMZ)
- 5.5: Firewalls
- 5.6: Network Address Translation (NAT)
- 5.7: Virtual Private Networks (VPN)
- 5.8: Web Threat Protection
- 5.9: Network Access Protection
- 5.10: Wireless Overview
- 5.11: Wireless Attacks
- 5.12: Wireless Defenses

6.0: Network
- 6.1: Network Threats
- 6.2: Network Device Vulnerabilities
- 6.3: Network Applications
- 6.4: Switch Attacks
- 6.5: Switch Security
- 6.6: Using VLANs
- 6.7: Router Security
- 6.8: Intrusion Detection and Prevention
- 6.9: Vulnerability Assessment
- 6.10: Protocol Analyzers
- 6.11: Remote Access
- 6.12: Network Authentication
- 6.13: Penetration Testing
- 6.14: Virtual Networking
- 6.15: Software-Defined Networking (SDN)
- 6.16: Cloud Services

7.0: Host
- 7.1: Malware
- 7.2: Password Attacks
- 7.3: Windows System Hardening
- 7.4: Hardening Enforcement
- 7.5: File Server Security
- 7.6: Linux Host Security
- 7.7: Embedded Systems

- 7.8: Log Management
- 7.9: Audits
- 7.10: Email
- 7.11: BYOD Security
- 7.12: Mobile Device Management
- 7.13: Host Virtualization

8.0: Application
- 8.1: Access Control Models
- 8.2: Authentication
- 8.3: Authorization
- 8.4: Web Application Attacks
- 8.5: Internet Browsers
- 8.6: Application Development
- 8.7: Active Directory Overview
- 8.8: Windows Domain Users and Groups
- 8.9: Linux Users
- 8.10: Linux Groups
- 8.11: Linux User Security
- 8.12: Group Policy Overview
- 8.13: Hardening Authentication 1
- 8.14: Hardening Authentication 2

9.0: Data
- 9.1: Data Management
- 9.2: Advanced Cryptography
- 9.3: Cryptography Implementations
- 9.4: Cryptographic Attacks
- 9.5: Symmetric Encryption
- 9.6: Asymmetric Encryption
- 9.7: File Encryption
- 9.8: Public Key Infrastructure (PKI)
- 9.9: Hashing
- 9.10: Data Transmission Security
- 9.11: Data Loss Prevention (DLP)
- 9.12: Redundancy
- 9.13: Backup and Restore
- 9.14: Cloud Storage

Practice Exams

A.0: Security Pro Certification Practice Exam

B.0: CompTIA Security+ Certification Practice Exam