SY0701 - CompTIA Security+

Durata: 35 ore

Descrizione: in questo corso imparerai come:

- Rilevare e neutralizzare minacce avanzate in ambito informatico.
- Comprendere tecniche avanzate di crittografia e sicurezza dei dati.
- Gestire in modo sicuro le identità digitali e l'accesso a sistemi e reti.
- Valutare e gestire i rischi IT, assicurando la conformità alle normative vigenti.
- Applicare protocolli di sicurezza in contesti IT diversificati.

Pubblico: amministratori IT

Prerequisiti: competenze di base per l'amministrazione del sistema Windows, Linux. Conoscenze di base di rete, security dei sistemi e del cloud

Labs: macchine virtuali con accesso tramite interfaccia web

Versione software: 701

Certificazione collegata: SY0701-CompTIA-Security+

Struttura del corso:

- Introduction to Security Concepts
  - The cybersecurity landscape
  - Roles and responsibilities in cybersecurity
  - Security frameworks and best practices
- Threats, Attacks, and Vulnerabilities
  - Types of threats and threat actors
  - Common attack techniques and vectors
  - Vulnerability assessment and management
- Technologies and Tools
  - Network security devices and technologies
  - Endpoint and mobile device security
  - Security information and event management (SIEM) tools
- Risk Management
  - Risk assessment and management
  - Business continuity and disaster recovery planning
  - Incident response planning and procedures
- Architecture and Design
  - Secure network and system design principles
  - Cloud and virtualization security
  - Security for Internet of Things (IoT) devices
- Identity and Access Management
  - Authentication, authorization, and accounting (AAA) models
  - Identity and access management solutions
  - Access control models and policies
- Cryptography and Public Key Infrastructure (PKI)
  - Cryptographic algorithms and encryption techniques
  - Key management and distribution
  - Public Key Infrastructure (PKI) components and concepts
- Wireless and Mobile Security
  - Wireless network security protocols and technologies

  - Mobile device security considerations
  - Bring Your Own Device (BYOD) policies
- Social Engineering and Human Factors
  - Social engineering techniques and prevention
  - Security awareness training and education
  - Insider threats and user behavior analytics
- Compliance and Operational Security
  - Legal, regulatory, and compliance considerations
  - Security policies, standards, and procedures
  - Physical security and environmental controls

Struttura del laboratorio:

- Exploring the Lab Environment
- Scanning and Identifying Network Nodes
- Intercepting and Interpreting Network Traffic with Packet Sniffing Tools
- Analyzing the Results of a Credentialed Vulnerability Scan
- Installing, Using, and Blocking a Malware-based Backdoor
- Performing Network Reconnaissance and Vulnerability Scanning
- Managing the Lifecycle of a Certificate
- Managing Certificates with OpenSSL
- Auditing Passwords with a Password Cracking Utility
- Managing Centralized Authentication
- Managing Access Controls in Windows Server
- Configuring a System for Auditing Policies
- Managing Access Controls in Linux
- Configuring Identity and Access Management Controls
- Implementing a Secure Network Design
- Configuring a Firewall
- Configuring an Intrusion Detection System
- Implementing Secure Network Addressing Services
- Implementing a Virtual Private Network
- Implementing a Secure SSH Server
- Implementing Endpoint Protection
- Securing the Network Infrastructure
- Identifying Application Attack Indicators
- Identifying a Browser Attack
- Implementing PowerShell Security
- Identifying Malicious Code
- Identifying Application Attacks
- Managing Data Sources for Incident Response
- Configuring Mitigation Controls
- Acquiring Digital Forensics Evidence
- Backing Up and Restoring Data in Windows and Linux
- Managing Incident Response, Mitigation and Recovery

