CompTIA Security+ SY0-601 Practical Guide

CompTIA Security+ SY0-601. Network defense, risk management, and hands-on labs for exam prep.

IT Certifications Instructor: Brian Taylor • 5 sections • 46 lessons • 16.50h total

View this course online Browse all courses

About this course

This course is for IT professionals and career changers who want to pass the CompTIA Security+ SY0-601 exam and build practical security skills. We cut through the noise and focus on what you need to know, using clear explanations and real examples from corporate IT environments.

You will learn how to apply security concepts, from network defense to risk management, through video lessons, practical labs, and downloadable study guides. We cover all exam objectives with a focus on using these skills on the job.

Course curriculum

Foundations and Exam Overview

- Understanding the SY0-601 Exam Structure (12m)
  Learn the exam domains, question types, and scoring to create an effective study plan from day one.
- Setting Up Your Virtual Lab Environment (18m)
  Step-by-step guide to building a safe, practical lab using free tools for hands-on practice.
- Core Security Concepts You Must Know (25m)
  Define key terms like confidentiality, integrity, and availability with real-world examples.
- How to Read and Interpret Security Policies (15m)
  Learn to analyze and apply organizational security policies in practical scenarios.
- Basic Threat Modeling for Beginners (22m)
  A simple framework for identifying and categorizing threats in your environment.
- Introduction to Security Frameworks (14m)
  Overview of NIST, ISO 27001, and how they guide real security decisions.
- Downloadable Study Plan Template (8m)
  Get a customizable template to organize your SY0-601 study schedule effectively.

Core Security Domains: Threats and Attacks

- Common Network Attacks and How They Work (30m)
  Explore DDoS, man-in-the-middle, and other attacks with simulation examples.
- Malware Types and Detection Techniques (28m)
  Identify viruses, ransomware, and trojans, and learn detection strategies.
- Social Engineering: Phishing and Beyond (19m)
  Analyze real phishing emails and learn how to train users to spot them.
- Wireless Network Vulnerabilities (24m)
  Step-by-step guide to securing Wi-Fi and spotting rogue access points.
- Application Security Flaws (26m)
  Understand OWASP Top 10 vulnerabilities with code examples.
- Insider Threats: Real Case Study (17m)
  Analyze a real incident and discuss prevention strategies.
- Vulnerability Scanning Tools (21m)
  Hands-on demo of using tools like Nessus for practical assessment.
- Threat Intelligence Sources (13m)
  Learn where to find reliable threat data for your organization.
- Problem-Solving Session: Attack Analysis (32m)
  Work through a complex attack scenario and apply your knowledge.

Security Architecture and Design

- Secure Network Design Principles (27m)
  Learn how to segment networks and apply defense in depth.

- Firewall Configuration and Rules (31m)
  Step-by-step guide to setting up and testing firewall policies.
- VPN Technologies and Implementation (23m)
  Compare IPsec vs. SSL VPNs with configuration examples.
- Cloud Security Basics (20m)
  Understand shared responsibility models for AWS, Azure, and GCP.
- Secure System Design Patterns (29m)
  Apply principles like least privilege and separation of duties.
- Hardware Security Modules (HSMs) (11m)
  When and why to use HSMs for key management.
- Secure Baseline Configuration (16m)
  Create a hardening checklist for Windows and Linux systems.
- Real Case: Designing a Secure DMZ (25m)
  Walk through a practical design for a demilitarized zone.

Advanced Access Control and Cryptography

- Implementing Multi-Factor Authentication (22m)
  Step-by-step setup of MFA using authenticator apps and hardware tokens.
- Role-Based vs. Attribute-Based Access Control (18m)
  Compare RBAC and ABAC with real policy examples.
- Identity and Access Management (IAM) Solutions (26m)
  Overview of tools like Active Directory and Okta.
- Cryptography Fundamentals for Security+ (35m)
  Learn hashing, symmetric, and asymmetric encryption with examples.
- Digital Signatures and Certificates (21m)
  How to use PKI for secure communication and verification.
- Key Management Best Practices (15m)
  Generate, store, and rotate keys securely.
- Secure File Transfer Methods (14m)
  Compare SFTP, FTPS, and other protocols.
- Hands-On Lab: Encrypting Data at Rest (28m)
  Use BitLocker and LUKS to encrypt disks step-by-step.
- Real Case: Breaking Weak Encryption (24m)
  Analyze a case where poor crypto led to a breach.
- Troubleshooting Access Issues (19m)
  Common problems and solutions for authentication failures.

Operations and Incident Response

- Creating an Incident Response Plan (23m)
  Template and step-by-step guide for your first IR plan.
- Incident Identification and Triage (20m)
  How to spot and prioritize security incidents.

- Forensic Analysis Basics (27m)
  Tools and techniques for collecting evidence.
- Disaster Recovery Planning (25m)
  Build a DR plan with RTO and RPO targets.
- Business Continuity Strategies (18m)
  Ensure operations continue during and after an incident.
- Security Monitoring and SIEM (30m)
  Set up alerts and analyze logs with a SIEM tool.
- Patch Management Process (22m)
  Step-by-step workflow for testing and deploying patches.
- Vulnerability Management Lifecycle (19m)
  From scanning to remediation in a real environment.
- Real Case: Responding to a Ransomware Attack (32m)
  Walk through a full incident response from detection to recovery.
- Post-Incident Review and Lessons Learned (16m)
  How to conduct a blameless review to improve security.
- Downloadable IR Checklist (10m)
  A practical checklist to guide your next incident response.
- Automation for Security Operations (21m)
  Use scripts and tools to automate routine tasks.