**How to Study for (and Pass) the CompTIA Security+ Certification Exam**

Published on 24 February 2025 at 18:36

Author: Kimberly Wiethoff

The **CompTIA Security+ (SY0-701)** certification is one of the most recognized entry-level cybersecurity certifications, validating foundational security skills essential for IT professionals. Whether you’re breaking into cybersecurity or strengthening your IT security knowledge, passing the Security+ exam requires strategic preparation and hands-on understanding of security principles.

In this post, I’ll walk you through **what to expect on the exam, how to prepare effectively, and tips to ensure success**.



**1. Understanding the Security+ Exam**

Security+ is a vendor-neutral certification covering essential cybersecurity concepts. The exam tests your ability to **identify, assess, and mitigate security threats**, making it an excellent starting point for IT and security professionals.

**🔹 Exam Overview**

* **Exam Code**: SY0-701 (latest version)
* **Number of Questions**: 90 (multiple-choice + performance-based)
* **Time Limit**: 90 minutes
* **Passing Score**: 750 (on a scale of 100-900)
* **Cost**: ~$392 USD (discounts available for students & military)

**🔹 Security+ Domains (SY0-701)**

The exam is broken down into **five key areas**:

* **General Security Concepts (12%)** – Core security principles, least privilege, threat actors, and cybersecurity frameworks.
* **Threats, Vulnerabilities, and Mitigations (22%)** – Attack types, vulnerabilities, risk assessments, and threat intelligence.
* **Security Architecture (18%)** – Network security, cloud security, and system hardening.
* **Security Operations (28%)** – Incident response, forensics, logging, SIEMs, and security controls.
* **Security Program Management and Governance (20%)** – Security policies, risk management, compliance (GDPR, HIPAA, NIST).

**2. How to Prepare for the Security+ Exam**

**📖 Step 1: Study the Right Materials**

✅ **CompTIA Security+ Study Guide (by CompTIA or Darril Gibson)** – These books cover all exam domains in detail.
✅ **CompTIA Security+ Exam Objectives** – Download the official objectives to understand exactly what’s tested.
✅ **Professor Messer’s Security+ Videos** (Free) – High-quality YouTube lectures explaining key concepts.
✅ **Jason Dion’s Practice Exams (Udemy)** – Great for realistic practice and identifying weak areas.
✅ **CompTIA Labs (or TryHackMe/HTB Labs)** – Hands-on practice for security tools and techniques.

**📝 Step 2: Create a Study Plan**

Allocate **6-8 weeks** for preparation, depending on your experience level.

📅 **Week 1-2: Foundations**

* Read a **Security+ study guide** and take notes.
* Watch **Professor Messer’s videos** for an overview of key concepts.

📅 **Week 3-4: Deep Dive into Domains**

* Focus on **encryption, network security, and threat mitigation** (major focus areas).
* Use **CompTIA labs** or set up a virtual lab (Kali Linux, Wireshark, Metasploit).
* Take **chapter quizzes** to reinforce learning.

📅 **Week 5-6: Practice Tests & Weak Areas**

* Take **full-length practice exams** to simulate test conditions.
* Review wrong answers and revisit weak areas.
* Memorize **key ports, encryption standards, and security frameworks**.

📅 **Week 7-8: Final Review & Exam Readiness**

* Revisit **hard topics** like PKI, SIEMs, and incident response.
* Take **final mock exams** until consistently scoring 85% or higher.
* Review **exam objectives** to ensure full coverage.

**🎯 Step 3: Master Key Security+ Concepts**

✔ **Understand the CIA Triad** – Confidentiality, Integrity, Availability.
✔ **Know Security Tools** – Firewalls, IDS/IPS, SIEM, encryption protocols, and VPNs.
✔ **Learn Attack Types** – Phishing, malware, social engineering, SQL injection, XSS.
✔ **Understand Compliance Frameworks** – NIST, ISO 27001, HIPAA, GDPR.
✔ **Know Ports & Protocols** – SSH (22), RDP (3389), DNS (53), HTTPS (443), etc.

**3. Exam Day Strategy: How to Pass the Security+ Exam**

📌 **Expect Performance-Based Questions (PBQs)** – These test hands-on skills like configuring firewalls or analyzing logs. Answer them **first** to avoid time pressure later.

📌 **Use the Process of Elimination** – If unsure, eliminate incorrect answers to improve your odds.

📌 **Manage Your Time Wisely** – With 90 questions in 90 minutes, spend **<1 min per question** and mark difficult ones to revisit later.

📌 **Think Like an Analyst** – Many questions ask what action to take. Choose the **most secure, least disruptive option**.

**Final Thoughts: Is Security+ Worth It?**

Absolutely! Security+ is:
✅ **A great entry point for cybersecurity careers**
✅ **A requirement for many DoD and government jobs**
✅ **A strong foundation for advanced certs (CISSP, CEH, etc.)**
✅ **A valuable credential in the growing cybersecurity industry**

With the right preparation, **you can pass Security+ on your first attempt**. Stay focused, practice hands-on skills, and don’t just memorize—**understand the concepts**.

**Are you studying for Security+ or recently passed? Share your experience and tips below!** 🚀🔐 #CyberSecurity #SecurityPlus #CompTIA #ITCertifications