

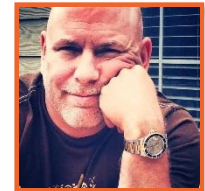
CompTIA Security+ (SY0-401) Network Security

Getting Started

Christopher Rees

<https://www.linkedin.com/in/cdrees>

@cdrees



pluralsight 
hardcore dev and IT training

Series TOC

- **CompTIA Security+ (SY0-401) Network Security**
- CompTIA Security+ (SY0-401) Compliance and Operational Security
- CompTIA Security+ (SY0-401) Threats and Vulnerabilities
- CompTIA Security+ (SY0-401) Application, Data and Host Security
- CompTIA Security+ (SY0-401) Access Control and Identity Management
- CompTIA Security+ (SY0-401) Cryptography

CompTIA Security+ (SY0-401)

■ Getting Started

- What is **CompTIA Security+**
 - Certification body recognized worldwide
 - Demonstrates you have the skills employers need
 - Prepares you for a career as a IT Security professional
- Can be used as an **elective** in many vendor certification tracks



CompTIA Security+

■ About this Course

- Suitable for someone who has passed the **CompTIA Network+ exam**, or who has equivalent knowledge or experience
- Covers **100%** of the CompTIA Security+ SY0-401 exam topics
 - Gives the student a solid understanding of **Security Best Practices**, terminology and concepts
- How the course is laid out
 - What areas (or Domains) are covered
 - 6 Domains total – we'll cover each in depth
- Practical application where appropriate
 - Not just **"teaching to the test"** but also real-world examples and scenarios

Why Become CompTIA Security+ Certified?

- **CompTIA Security+ Certification shows employers you have the skills they need**
 - Businesses small and large lose billions of dollars each year from theft of intellectual property, customer data, loss of consumer or customer trust, etc.
- **Professional Certification that shows your skills and increases marketability**
- **Provides opportunities for advancement!**



How to Become Security+ Certified

- **Study the material in this course**
 - Review until you're comfortable with all the terms and concepts
 - Test yourself with practice questions to ensure you understand how questions will be asked
- **Don't just Memorize Questions!**
 - Very bad idea in that you only remember sentences rather than the underlying concepts
 - Trick questions or questions worded differently will trip you up if you don't understand the concepts
- **Register for the exam**
 - Set a date and work toward that date
 - Go online to <http://www.vue.com/comptia> and register at a local testing center near you

Important! Maximize Your Training

Become a Lifelong Student

Information technology is constantly evolving
and new Security Threats are discovered daily

Have FUN with your Training!

When you enjoy the process, you'll stick with it,
remember more and apply more

Is This **Only Applicable** to Security Professionals?

- Security is **EVERYONE's** Responsibility

- Everyone should strive to keep their data secure
- Network and System Admins should practice security
- AppDev folks should design with security in mind
- Physical security is as much a problem, if not **MORE!**

- Don't **Assume** it's Someone Else's Responsibility

- Most onsite attacks occur because people act like they're supposed to be there
 - People assume if they look like their know when they're doing, they're allowed to be there
 - Don't assume... Question!



Goals for the Course

- Learn about the **6 Security Domains** for CompTIA Security+ Certification
- Understand that security is a **multi-pronged approach**
 - Local
 - Remote
 - Servers
 - Network
 - Wireless
 - Physical
- Have **fun** while learning, **increase** your skills, and help make your company a **safer place!**



Preparing for the Exam

Study the videos

REPEATEDLY

(Watch them in Order if Possible)

Test yourself with
Exam Prep
questions until **90%**

Set a **Date** and
Register for the
Exam



Security+ Domains

Security+ Domains

1.0
Network
Security

2.0
Compliance
and
Operational
Security

3.0
Threats and
Vulnerabilities

4.0
Application,
Data and Host
Security

5.0
Access Control
and Identity
Management

6.0
Cryptography

Security+ Domains

- **1.0 – Network Security**

- Firewalls, routers, switches
- Protocol and Protocol Analyzers
- ACLs, VLAN Management

- **2.0 – Compliance and Operational Security**

- Control Types
- Risk Calculation
- SLAs, Change and Incident Management

- **3.0 – Threats and Vulnerabilities**

- Malware and Viruses
- Personally Identifiable Information (PII)
- Attack Types – DDoS, Social Engineering, Phishing

Security+ Domains

■ 4.0 – Application, Data and Host Security

- Application Controls such as secure coding concepts, Cross Site Scripting
- Device Security and Bring Your Own Device (BYOD) concerns
- Acceptable Use Policies

■ 5.0 – Access Control and Identity Management

- RADIUS, TACACS+, Kerberos, LDAP
- Permissions, Authentication and Authorization
- Tokens, Protocols and Methods

■ 6.0 – Cryptography

- Symmetric vs. Asymmetric
- LAN, WAN, Wireless considerations
- Steganography and other methods to hide/steal data

You Get Certified – Then What?

- **Welcome to the Club!**

- You get the keys to the **Special VIP** IT Security bathrooms
 - Just Kidding 😊
- Industry recognized certification
- Career options and opportunities
 - Systems Security (desktops, servers, storage)
 - Network Security
 - Application Security Specialist
- Most Fortune 500 companies look for certification when hiring
 - Public and Private sector companies look for, and often **require** certification for certain jobs
 - Department of Defense (DoD) mandates that all IT personnel have one or more IT certifications depending on their job function
 - Security+ fulfills that requirement

DoD Directive 8570-1

- Created in 2004 as a response to the events of 9/11
 - Enforce computer and network security within the **Federal Government** and affiliated partners (including contractors)
- Two classifications or “Tracks”
 - IAT – Information Assurance Technical
 - Individual contributors and non-management personnel
 - IAM – Information Assurance Management
 - Personnel with direct and/or indirect-reports
- Created in **2004** with 100% compliance required by **2010**

IAT Level I		IAT Level II		IAT Level III	
A+ Network+ SSCP		GSEC Security+ SSCP		CASP CISA CISSP (or Associate) GCED GCIH	
IAM Level I		IAM Level II		IAM Level III	
CAP GSLC Security+		CAP CASP CISM CISSP (or Associate) GSLC		GSLC CISM CISSP (or Associate)	
CND Analyst	CND Infrastructure Support	CND Incident Responder		CND Auditor	CND-SP Manager
CEH GCIA GCIH	CEH SSCP	CEH CSIH GCFA GCIH		CEH CISA GSNA	CISM CISSP-ISSMP
IASAE I		IASAE II		IASAE III	
CASP CISSP (or Associate) CSSLP		CASP CISSP (or Associate) CSSLP		CISSP-ISSAP CISSP-ISSEP	

Let's Get Started

- **As we go through the course:**
 - Takes notes when necessary so you can go back and review
 - Think how a specific topic or concept could apply to your current job

