

# CompTIA Security+ 2008 Edition R2

- **Exam Code:** SY0-201
- **Course Length:** 5 Days

## Course Overview

The CompTIA Security+ certification designates knowledgeable professionals in the field of security, one of the fastest-growing fields in IT. It is an international, vendor-neutral certification that proves competency in system security, network infrastructure, access control and organizational security.

## Audience/ Prerequisites

Although not a prerequisite, it is recommended that CompTIA Security+ candidates have at least two years of technical networking experience, with an emphasis on security. The CompTIA Network+ certification is also recommended.

## Certification Exam

New candidates must take CompTIA exam SY0-201. Professionals who are currently CompTIA Security+ certified under the 2002 exam are eligible to become CompTIA Security+ 2008 certified by taking the bridge exam (BR0-001).

## Course Outline

### Course Introduction

Course Introduction

7 min

### Unit 01 - Mitigating Threats

Topic A: Core System Maintenance  
Primary Causes for Compromised Security  
The Goal - CIA  
Technology Weaknesses  
Configuration Weaknesses  
Human Error and Malice

3h 58m

Securing the Operating System

Microsoft Update

Demo - Windows Update

Windows Update Categories

Update History List

Service Packs

Demo - Installing Service Pack

BIOS Version

BIOS Update

Windows Firewall

Demo - BIOS and Firewall

Tasks Requiring Administrative Privileges

User Account Control Consent

User Account Control Credential

Topic B: Virus and Spyware Management

Viruses

Worms

Trojan Horses

Antivirus Software

Demo - Antivirus

Spyware

Windows Defender

Demo - Spyware

Spybot Search & Destroy

Network AV & Spyware

Demo - Securing Mail

Topic C: Browser Security

Pop-ups

Demo - Managing Pop-ups

Cookies

Cookie Vulnerabilities

Cookie Safeguards

Demo - Managing Cookies

Web Application Security Threats

JavaScript

Simple JavaScript Code

JavaScript Security Holes

ActiveX

ActiveX Vulnerabilities and Safeguards

Java Applets

Signed and Unsigned Applets

CGI

Form Submission

CGI Vulnerabilities and Safeguards

Cross-site Scripting

Buffer Overflow Attacks

Preventing Input Attacks

Demo - Script Weaknesses

Topic D: Social Engineering Threats

Social Engineering

Dumpster Diving  
Online Attacks  
Social Engineering Countermeasures  
Phishing  
Domain Kiting  
Unit 01 Review

## **Unit 02 - Cryptography**

1h 31m

Topic A: Symmetric Cryptography  
Cryptography  
Alice, Bob, and Eve  
ROT13 Cipher  
Keys  
Symmetric Encryption in Action  
Common Symmetric Ciphers  
Demo - Encrypting and Decrypting Data  
Hashes  
Hashing Example  
Uses for Hashes  
MD5 Hash Algorithm  
SHA Algorithm  
Hash Vulnerabilities  
Steganography  
Demo - Steganography  
Topic B: Public Key Cryptography  
Public Key Cryptography  
Asymmetric Encryption in Action  
Common Asymmetric Ciphers  
Demo - Public Key Encryption  
Digital Signatures  
Signature Process  
Features of Signatures  
Digital Certificates  
Certificate Types  
Demo - Examining Certificates  
Public Key Infrastructure  
Certificate Policy  
Certificate Practice Statement  
Trust Models  
Single Authority Trust Model  
Hierarchical Trust Model  
Web of Trust Model  
Single- and Dual-key Certificates  
Unit 02 Review

## **Unit 03 - Authentication Systems**

2h 22m

Topic A: Authentication  
3 Steps to Secure Resources  
Usernames and Passwords  
Password Protection

Strong Passwords  
Multiple passwords  
Run As Administrator  
Demo - Identifying Components of Authentication  
Authentication Factors  
One-factor Authentication  
Two-factor Authentication  
Three-factor Authentication  
Network Monitor Data  
Demo - Network Monitor  
Active Directory Services and Features  
Demo - Installing Active Directory  
Demo - Joining a Domain  
Topic B: Hashing  
Authentication Protocols  
Encryption  
Weak Keys  
Mathematical Attacks  
Birthday Attack  
Password Guessing  
SAM and System Files  
Demo - Password Cracking  
Topic C: Authentication Systems  
Preventing Impersonation  
Identity Proofing  
Single Sign-on  
Kerberos  
Kerberos System Composed Of  
Kerberos Data Types  
Kerberos Authentication Process  
Cross-realm Authentication  
Kerberos Security Weaknesses  
CHAP  
PAP  
EAP  
Mutual Authentication  
Unit 03 Review

## **Unit 04 - Messaging Security**

1h 38m

Topic A: E-mail Security  
E-mail Vulnerabilities  
Spam  
Hoaxes and Chain Letters  
Hoax – Company Reputation Issue  
Phishing  
Hoax Countermeasures  
SMTP Open Relays  
E-mail Server Security  
Demo - Configure Security on Email Server  
Secure E-mail

Encryption  
Hash Function  
PGP Symmetric Encryption Methods  
PGP Certificates  
S/MIME  
X.509 Certificates  
X.509 Certificate Content  
S/MIME Trust Model  
PGP and S/MIME Differences  
To Install and Configure PGP  
Restricting Permissions to Messages  
Sending Restricted Messages  
Digitally Signed Message  
Demo - Digital Signatures  
Encrypting Messages  
Topic B: Messaging and Peer-to-peer Security  
Instant Messaging  
IM Risks  
Cell Phone SMS  
Blocking IM  
Corporate IM  
Intrusion Detection  
Packet Sniffing  
Additional IM Features  
IM Client Security  
Legal Issues  
Demo - Configure IM Client Security  
Unit 04 Review

## **Unit 05 - User and Role Based Security**

2h 4m

Topic A: Security Policies  
Group Policy Settings  
Local GPO Types  
GPO Editor  
Local Computer GPO Nodes  
Policy Properties Dialog Box  
Demo - Creating Console to Manage Local Security Policies  
Container Types  
Types of Domain GPOs  
GPOs Applied in this Order  
Demo - GPMC  
Windows Applications Configured with Group Policies might Include  
Device Installation Policy Settings  
Internet Explorer 7 Policy Settings  
IE8 Features  
Demo - Implementing GPO's  
Security Templates  
Windows Vista Security Guide Templates  
Demo - Analyzing Windows Vista Computer Security  
Topic B: Securing File and Print Resources

File and Print Security  
Groups  
Demo - Groups  
File System Security  
Permissions  
Demo - Permissions  
Access Control Models  
Printer Permissions  
Demo - Securing Printer Resources  
Unit 05 Review

## **Unit 06 - Public Key Infrastructure**

2h 3m

Topic A: Key Management and Life Cycle  
Management  
Setup and Initialization Phase  
Administration Phase  
Cancellation and History Phase  
Administrative Responsibilities  
Topic B: Setting up a Certificate Server  
Microsoft Certificate Services  
AD Integration Options  
CA Role  
Demo - Installing Stand Alone Root Certificate Authority  
Demo - Installing Enterprise Subordinate CA  
Demo - Implementing File Based Requests  
Demo - Managing Your Certificate Server  
User Certificates  
Demo - Requesting User Certificate  
Certificate Revocation  
Demo - Revoking a Certificate  
Key Escrow and Recovery  
Key Recovery Agents  
Demo - Enabling EFS Recovery Agent Template  
Demo - Enrolling Recovery Agent Certificate  
Demo - Enabling Key Archival  
Demo - Re-enrolling All Certificates  
Topic C: Web Server Security with PKI  
Secure Web Servers  
Commercial Certificate  
Demo - Requesting and Installing Web Server Certificate  
Demo - Enabling SSL for Certificate Server Web Site  
HTTPS Connections  
Demo - Certificate Requests over the Web  
Unit 06 Review

## **Unit 07 - Access Security**

1h 19m

Topic A: Biometric Systems  
Biometric Devices  
Topic B: Physical Access Security  
Physical Access Security Protects

Protection  
Locks  
Other Physical Security Measures  
Surveillance  
Logging  
Topic C: Peripheral and Component Security  
Vulnerable Peripherals  
Securing Peripherals  
Demo - Mitigating Security Risks of Peripherals  
Topic D: Storage Device Security  
File Encryption  
Demo - File Encryption  
Whole Disk Encryption  
BitLocker Hardware Requirements  
BitLocker Authentication Modes  
BitLocker Life Cycle  
BitLocker Recovery  
Unit 07 Review

## **Unit 08 - Ports and Protocols**

1h 48m

Topic A: TCP/IP Review  
Internet Protocol Suite  
IPv4 Classes  
IP Classes by Binary  
IPv4 Header  
CIDR and NAT  
IPv6 Header  
IPv6 Scopes  
IPv6 Address Types  
Demo - Looking at Addressing  
Topic B: Protocol-based Attacks  
DoS Attacks  
TCP 3-way Handshake  
SYN Flood Defense  
Smurf Attack  
Ping of Death Attacks  
Demo - Syn Flood Protect  
DDoS Attacks  
DDoS Attack Protection  
Man-in-the-middle Attacks  
Spoofing  
IP Address Spoofing  
Demo - Port Scanning  
ARP Poisoning  
Demo - Checking the Arp Cache  
Spoofing Attacks  
Replay Attacks  
TCP/IP Hijacking  
Unit 08 Review

## **Unit 09 - Network Security**

2h 9m

Topic A: Common Network Devices

OSI Reference Model

Repeaters, Hubs, Switches

Switch Security

Routers

Route Selection

Router State Management

NAT/PAT

Port Address Translation

Firewalls and Proxies

Firewall Categories

Security Issues

Overcoming Weaknesses

Topic B: Secure Network Topologies

Security Zones

Intranet Zone

Perimeter Network

DMZ Options

Screened Host

Bastion Host

Three-homed Firewall

Back-to-back Firewall

Dead Zone

Traffic Filtering

IPSec Encryption

Topic C: Browser-related Network Security

Browser Security

Phishing Filter

Security Zones

Levels Per Zone

Custom Security Settings

Security Settings

Cookies

Demo - IE Configuration

Topic D: Virtualization

Virtual Computers

Citrix XenServer

Unit 09 Review

## **Unit 10 - Wireless Security**

55m

Topic A: Wi-Fi Network Security

802.11 Standard

802.11 Family

802.11 Networking

Wireless Security

Wireless Vulnerabilities

Wi-Fi Scanners

Warchalking Symbols

Router Software

Configuration Options  
Transmission Encryption  
Demo - WAP  
Topic B: Non-PC Wireless Devices  
Mobile Device Security  
Infrastructure Issues  
Unit 10 Review

## **Unit 11 - Remote Access Security**

1h 33m

Topic A: Remote Access  
AAA  
RADIUS  
RADIUS Authentication  
Realms  
RADIUS Security  
RADIUS Benefits  
Diameter  
Diameter Improvements  
LDAP and Remote Access  
LDAP Security  
LDAP Authentication/Authorization  
TACACS+  
TACACS+ versus RADIUS  
802.1x  
Network Policy Server (NPS)  
Demo - Installing Network Policy and Access Services  
Demo - Configuring an NPS Network Policy  
Demo - Configuring NPS Accounting  
Topic B: Virtual Private Networks  
Virtual Private Networks  
VPN Technologies  
VPN Security Models  
VPN Protocols  
PPTP versus L2TP  
IPsec Protocols  
Encryption Modes  
Secure Shell (SSH)  
VPN Solutions  
Demo - Installing Routing and Remote Access Services  
Demo - Enabling VPN  
Demo - Configuring NPS to Provide RADIUS Authentication  
Service Provider Tunneling  
Demo - Making a VPN Connection  
Unit 11 Review

## **Unit 12 - Auditing, Logging, and Monitoring**

1h 10m

Topic A: System Logging  
Event Viewer  
Windows Server 2008 Event Viewer  
Events

Event Types  
Event Details  
Demo - Viewing Event Logs  
Device and Application Logging  
Topic B: Server Monitoring  
Monitoring  
Reliability and Performance  
Performance Monitor  
Counters and Objects  
Demo - Performance Monitor  
Data Collector Sets  
Viewing DCS Reports  
Demo - Data Collector Sets  
Auditing  
Policies and Human Factors  
Unit 12 Review

### **Unit 13 - Vulnerability Testing**

1h 44m

Topic A: Risk and Vulnerability Assessment  
Risk Analysis  
OS Hardening  
MBSA  
Demo - MBSA  
Vulnerability Scanners  
Penetration Testing  
OVAL  
OVAL Scan Report  
Demo - OVAL  
Nessus  
Nessus Scan Report  
Demo - Nessus  
Topic B: IDS and IPS  
Intrusion Detection  
Events  
NIDS  
IDScenter for Snort  
Example Snort Rule  
Demo - Installing and Monitoring with Snort IDS  
HIDS  
HIDS Advantages over NIDS  
Honey pots  
Honey pot Examples  
Honey pot Deployment  
Topic C: Forensics  
Computer Forensics  
Evidence Gathering Principles  
Chain of Custody  
Unit 13 Review

## **Unit 14 - Organizational Security**

58m

Topic A: Organizational Policies

Security Policy Content

Acceptable Use

Due Care

Privacy

Separation of Duties

Need to Know

Password Management

Service Level Agreements

Disposal and Destruction

Human Resource Policies

Hiring

Employee Review and Maintenance

Post-employment

Code of Ethics

Incident Response Policy

Incident Response Policy Includes

Preparation

Detection

Containment

Eradication

Recovery

Follow-up

Change Management

Change Documentation

Topic B: Education and Training

Education

Communication

User Awareness

Types of Training

Topic C: Disposal and Destruction

Disposal of Electronics

Disposal of Computer Equipment

Data Security and Destruction

Unit 14 Review

## **Unit 15 - Business Continuity**

1h 5m

Topic A: Redundancy Planning

RAID Levels

Nested RAID

Utility Services

Alternate Sites

Disaster or Service Failure

Disaster Recovery Plan Documents

Threats

Disaster Recovery Team

Business Impact Assessment

Contingency Plan

Documentation

Topic B: Backups  
Backup Frequency  
Backup Tools  
Backup Types  
Backup Media  
Backup Storage  
Data Restoration  
Demo - Backup  
Windows Recovery Environment  
Grandfather Method  
Tower of Hanoi  
Incremented Media Backup  
Backup Storage  
Topic C: Environmental Controls  
Fire Extinguisher Classes  
Fire Extinguisher Contents  
Extinguisher Label  
Safety Guidelines  
Unit 15 Review  
Course Closure

**Total Duration:** 26h 25m