

Security+ 2008 Training

6 Sessions –

12 Hours of Interactive Training

Develop your understanding of network administration by gaining a certifiable knowledge of Security+ by CompTIA. Learn how to secure and manage all facets of your network from CPU cycles to software used by individuals or across a network. Security+ is the next level to attain certification for every IT network administrator. This course will prepare you to pass the CompTIA® Security+ certification exam SY0-201.

Benefits

- Implement and maintain an effective security strategy within your company's network infrastructure
- Our courses meet or exceed all CompTIA® certification objectives for exam SY0-201
- Learn the knowledge of systems security, network infrastructure, access control, assessments and audits

Session 1

Section A: Introduction

- Prerequisites
- Knowledge Domains
- Security Importance
- Applications

Section B: Security Requirements

- Requirements
- Classification
- Due Care
- Due Diligence
- Due Process
- User Education
- HR Security

Section C: Security Threats

- Understanding Threats
- Viruses and Worms
- Trojans, Spyware, and Malware
- Rootkits
- Spam Filtering
- Botnets

Section D: Privilege Escalation

- Initial Entry
- Escalation Methods
- After Escalation
- Performing a Logic Bomb

Section E: Hardware Security Risks

- BIOS
- USB Devices
- Removable Storage
- Cell Phones

Section F: Network Vulnerabilities

- Vulnerable Devices
- Weak Passwords
- Backdoors
- Denial of Service
- Vampire Taps

Section G: Infrastructure Risks

- Old Protocols
- TCP/IP Issues
- Null Sessions
- Spoofing
- Man-in-the-Middle

Session 2

Section A: Wireless Vulnerabilities

- Wireless LANs
- Wi-Fi
- Data Emanation
- War Driving
- Default Behaviors
- Rogue APs
- Hijacking

Section B: Wireless Encryption

- Encryption Cracking
- WEP
- Authentication
- Understanding WEP
- WEP Key Problems
- Weak Initialization Vectors

Section C: Personal Device Security

- Portable Devices
- Bluejacking
- Bluesnarfing
- Blackjacking
- Laptops

Section D: Authentication Fundamentals

- Identification
- Authentication
- One Factor
- Multiple Factors
- Single Sign-On

Section E: Authentication Hardware

- Thumb Scanners
- FAR and FRR
- Smart Cards
- RFID

Section F: Authentication Protocols

- Understanding Protocols
- PAP and CHAP
- LAN Manager
- NTLM
- NTLMv2

Section G: Advanced Authentication Protocols

- Kerberos
- Kerberos Tickets

Session 3

Section A: ACLs

- Managing Folder Access
- Network Resource Permissions

Section B: Access Control Methods

- MAC
- DAC
- RBAC
- Least Privilege
- Implicit Deny
- Duty Separation

Section C: Remote Access Security

- Remote Access
- RA Encryption
- RA Authentication
- Enabling RAS
- RAS Authentication Options

Section D: Physical Security

- Understanding Physical Security
- Affecting Factors
- Access Control
- Facility Access Checklist
- Internal Access Checklist
- Network Access Checklist

Section E: OS Hardening

- Patches
- Service Packs
- Patch Management
- Linux Hardening
- Windows Hardening
- Creating Security Templates
- Security Analysis

Section F: Application Security

- Buffer Overflows
- Dependencies
- Stack-Based Overflows
- Heap-Based Overflows
- After the Attack
- Countermeasures
- Instant Messaging
- P2P Networks

Section G: Web Application Security

- Web Servers

- Replay Attacks
- DDoS
- DNS Vulnerabilities
- ARP Poisoning

- Kerberos Access
- LDAP
- 802.1X/RADIUS
- TACACS
- RAS

Section H: Users, Groups, and Roles

- Active Directory
- Users
- Groups
- Group Strategy
- Guidelines
- Roles

Section I: Authorization Models

- Group Policy Editor
- Password Policies
- Lockout Policies
- Creating Accounts
- Account Parameters

- Communications
- Common Attacks
- Web Applications
- ActiveX and Java
- XSS
- Browser Options
- Cookies
- Input Validation

Section H: E-mail Security

- E-mail Protocols
- E-mail Threats
- E-mail Authentication
- Confidentiality
- SMTP Relay
- Spam Solutions

Session 4

Section A: Client Security Solutions

- avast Software
- Spam Filtering
- Pop-Up Blocking
- Personal Firewalls
- HIDS

Section B: Virtualization and Security

- Virtualization Defined
- Benefits
- Scenarios
- Virtual PC
- Hyper-V
- VMware
- Planning
- Security Issues

Section C: Network Firewalls

- Understanding Firewalls
- Firewall Types
- Firewall Installation
- Well Known Ports
- Port Blocking

Section D: Network Security Design

- Subnetting
- Virtual LANs
- Connecting Networks
- DMZ
- NAT
- NAC

Section E: Telephony Security

- Traditional PBX
- VoIP
- SIP Security
- H.323 Security

Section F: Intrusion Detection and Prevention

- Intrusion Monitoring
- IDS Solutions
- Detection Methods
- IPS Solutions
- IPS Detection States
- Intrusion Indications
- IDS Implementations
- Intrusion Responses
- Honey pots

Section G: Controlling Internet Access

- Proxy Servers
- Internet Filters
- Creating a Firewall Rule

Section H: Protocol Analyzers

Session 5

Section A: Wireless Network Security

- War Driving
- SSID Issues
- Rogue APs
- Weak Encryption
- Configuring WPA

Section B: Monitoring Systems

- Performance Tools
- Task Manager
- Performance Snap-In
- Baselines
- Creating a Baseline
- Creating a Second Baseline
- Comparing Baselines with Excel

Section C: Scanning the Network

- Port Scanning
- Angry IP Scanner
- Scanning Devices
- Service Enumeration
- Configuring Zenmap GUI
- Nmap Scanning

Section D: Vulnerability Scanning

- Sectools.org
- OVAL
- National Vulnerability Database
- Password Cracker
- Pen Testing

Section E: Logging and Auditing

- Importance of Logs
- DNS Logs
- System Logs
- Performance Logs
- Access Logs
- Firewall Logs
- Antivirus Logs
- Auditing

Section F: Cryptography 101

- Encryption
- Simple Encryption
- CIA
- Non-Repudiation
- Whole Disk
- Key Management
- Steganography
- Encryption Testing
- TPM

Section G: Encryption Algorithms

- Encryption Types
- Key Factors
- DES

Session 6

Section A: Encryption Protocols and Hashing

- Hashing
- Hashing Protocols
- Digital Signatures
- SSL/TLS
- TLS Goals
- SSL Operations
- PPTP
- L2TP
- IPsec
- HTTP Solutions
- SSH

Section B: Public Key Cryptography

- Certificates
- PK Cryptography
- PKI Components
- PKI Processes

Section C: Risk Assessments

- Risk Management
- Asset Identification
- Threat Identification
- Risk Assessment
- Risk Tracking

Section D: Redundancy Planning

- Failure Points
- RAID
- Spare Parts
- Redundant Servers
- Redundant ISP
- Power Supply
- Spare Sites

Section E: Incident Response

- Incident Defined
- IR Process
- First Responders
- Computer Forensics
- Chain of Custody
- Reporting
- Damage Control

Section F: Disaster Recovery

- Planning
- Backup Practices
- Backup Methods
- Backup Types
- Media Rotation
- Restoration
- DR Exercises

Section G: Social Engineering

- Definition

- Installing Wireshark
- Capturing E-mail Logon
- Creating HTTP Filter
- Viewing Passwords

- 3DES
- RSA
- ECC
- PGP
- AES
- RC4
- Secure Transfer
- One-Time Pad

- Example Attacks
- Dumpster Diving
- Passive Attacks
- Inside/Outside Attacks
- Reverse
- Phishing Attacks

Section H: Security Policies

- Importance
- General Policies
- Functional Policies
- sans.org