

CompTIA Security+ (Edition 2008) Zertifizierung

Prüfungsziele, Prüfungsnummer: SY0-201

EINLEITUNG

CompTIA Security+ (Edition 2008) ist eine herstellerunabhängige Zertifizierung für fachkundige Professionals im Bereich der IT-Sicherheit. Die Zertifizierung ist ein international anerkannter Maßstab für grundlegende Kenntnisse und Fähigkeiten in der IT-Spezialdisziplin "Sicherheit". Sie wird weltweit von Organisationen und Sicherheitsexperten als Gütesiegel eingesetzt.

Die Kenntnisse und Fähigkeiten, die in der Prüfung für CompTIA Security+ abgefragt werden, spiegeln Ergebnisse einer industrieweiten Aufgabenanalyse von IT-Sicherheitsprofis wider und wurden durch eine entsprechende globale Umfrage bestätigt. Letztere wurde zudem genutzt, um die Wissensgebiete der Prüfung zu gewichten. So kann sichergestellt werden, dass die Gewichtung der Themen repräsentativ für die Bedeutung eines Themas in der Praxis ist.

Die Zertifizierung CompTIA Security+ (Edition 2008) eignet sich für IT-Sicherheitspersonal, das:

- über mindestens zwei Jahre Berufserfahrung in der Netzwerkadministration mit Fokus auf Sicherheit verfügt.
- Erfahrung mit der alltäglichen *technischen* Informationssicherheit hat.
- über ein breites theoretisches und praktisches Know-how in Sicherheitsfragen verfügt, einschließlich der unten aufgeführten Wissensgebiete.

Die unten stehende Tabelle zeigt die Wissensgebiete, die im Rahmen der CompTIA Security+ Prüfung abgefragt werden und in welchem Umfang sie dort behandelt werden:

Wissensgebiete	% der Prüfung
1.0 Systemsicherheit	21%
2.0 Netzwerkinfrastruktur	20%
3.0 Zugangskontrolle	17%
4.0 Assessments & Audits	15%
5.0 Kryptografie	15%
6.0 Betriebssicherheit	12%
Gesamt	100%

Anmerkung: Die Stichpunkte, die unter jedem Ziel aufgeführt sind, stellen keine abschließende Liste dar. Beispiele anderer Technologien, Prozesse oder Aufgaben, die sich auf die genannten Ziele beziehen, können in der Prüfung vorkommen, obwohl sie nicht in diesem Dokument erwähnt wurden.

(Eine Auflistung der im Folgenden verwendeten Abkürzungen finden Sie am Ende des Dokuments).

Kursiv gedruckte Prüfungsziele sind Ziele, deren Inhalt sich seit der letzten Version der Security+ Prüfung (Prüfungsziele 2002) geändert haben.

1.0 Systemsicherheit

1.1 Unterscheiden Sie zwischen verschiedenen Systemsicherheitsbedrohungen.

- Erweiterung von Rechten
- Virus
- Wurm
- Trojaner
- Spyware
- Spam
- Adware
- Rootkits
- Botnets
- Logische Bombe

1.2 Erklären Sie die Sicherheitsrisiken, die Systemhardware und Peripheriegeräte betreffen.

- BIOS
- USB Geräte
- Mobiltelefone
- Wechselspeicher
- Am Netzwerk angeschlossene Speicher

1.3 Implementieren Sie Härtungsmethoden für das Betriebssystem, um Arbeitsplatz- und Serversicherheit zu erlangen.

- Hotfixes
- Service Packs
- Patches
- Patch Management
- Gruppenrichtlinien
- Sicherheitsvorlagen
- Konfigurations-Baseline

1.4 Führen Sie die passenden Maßnahmen zur Herstellung der Anwendungssicherheit durch.

- ActiveX
- Java
- Scripting
- Browser
- Speicherüberlauf
- Cookies
- offene SMTP Relais
- Instant Messaging
- P2P
- Eingabevalidierung
- Cross Site Scripting (XSS)

1.5 Setzen Sie Sicherheitsanwendungen ein.

- HIDS
- Persönliche Software Firewalls
- Antivirus

- Antispam
- Popup Blocker

1.6 Erklären Sie den Zweck und die Anwendung der Virtualisierungstechnologie.

2.0 Netzwerkinfrastruktur

2.1 Unterscheiden Sie zwischen den verschiedenen Ports & Protokollen und ihren jeweiligen Bedrohungen und den Minimierungstechniken.

- Veraltete Protokolle
- TCP / IP Hijacking
- Null Sessions
- Spoofing
- Man-in-the-middle
- Replay-Angriff
- DOS
- DDOS
- Domain-Kiting
- DNS Poisoning
- ARP Poisoning

2.2 Unterscheiden Sie zwischen Netzwerk-Designelementen und Komponenten.

- DMZ
- VLAN
- NAT
- Netzwerkverbindungen
- NAC
- Subnetting
- Telefonie

2.3 Bestimmen Sie den geeigneten Gebrauch von Netzwerksicherheit-Tools, um die Netzwerksicherheit zu fördern.

- NIDS
- NIPS
- Firewalls
- Proxy Server
- Honeypot
- Internet-Inhaltsfilter
- Protokollanalytiker

2.4 Wenden Sie die passenden Netzwerk-Tools an, um die Netzwerksicherheit zu fördern.

- NIDS
- Firewalls
- Proxy Server
- Internet-Inhaltsfilter
- Protokollanalytiker

2.5 Erklären Sie die Risiken und die Minimierungsmöglichkeiten, die mit Netzwerkgeräten assoziiert werden.

- Erweiterung der Rechte
- Schwache Passwörter

- Back doors
- Standardkonten
- DOS

2.6 Erklären Sie die Risiken und die Minimierungsmöglichkeiten, die mit verschiedenen Übertragungsmedien assoziiert werden.

- Vampirklemme

2.7 Erklären Sie die Risiken und die Minimierungsmöglichkeiten, die mit drahtlosen Netzwerken assoziiert werden.

- Data Emanation
- Wardriving
- SSID Broadcast
- Bluejacking
- Bluesnarfing
- Unbefugte Accesspoints
- Schwache Verschlüsselung

3.0 Zugangskontrolle

3.1 Identifizieren Sie die beste Praxis für Zugangskontrollmethoden und wenden Sie diese an.

- Indirekte Verweigerung
- Die wenigsten Rechte
- Teilung der Aufgaben
- Jobrotation

3.2 Erklären Sie grundlegende Modelle der Zugangskontrolle und deren Unterschiede.

- MAC
- DAC
- Rollen & Regeln basierte Zugangskontrolle

3.3 Organisieren Sie Benutzer und Computer in geeigneten Sicherheitsgruppen und Rollen, indem Sie zwischen den geeigneten Rechten und Privilegien unterscheiden.

3.4 Wenden Sie geeignete Sicherheitskontrollen auf Datei- und Druckressourcen an.

3.5 Vergleichen Sie logische Methoden der Zugangskontrolle und setzen Sie diese ein.

- ACL
- Gruppenrichtlinien
- Passwort Richtlinien
- Domain Passwort Richtlinie
- Benutzernamen und Passwörter
- Tageszeit-Begrenzung
- Erlöschen des Kontos
- Logische Token

3.6 Fassen Sie die verschiedenen Authentifizierungsmodelle zusammen und identifizieren Sie deren Komponenten.

- Eins-, Zwei- und Drei-Faktor-Authentifizierung
- Single Sign-on

3.7 Setzen Sie die verschiedenen Authentifizierungsmodelle ein und identifizieren Sie deren Komponenten.

- Biometrischer Leser
- RADIUS
- RAS
- LDAP
- Remote Access Richtlinien
- Remote Authentifizierung
- VPN
- Kerberos
- CHAP
- PAP
- Wechselseitig
- 802.1x
- TACACS

3.8 Erklären Sie den Unterschied zwischen Identifizierung und Authentifizierung (Identitätsbeweis).

3.9 Erklären Sie physikalische Zugangssicherheitsmethoden und wenden Sie diese an.

- Physikalische Zugangsprotokolle/-listen
- Hardwareschlösser
- Physikalische Zugangskontrolle - Ausweise
- Zutrittskontrolle an den Türen
- Personenschleuse
- Physikalische Token
- Videoüberwachung - Kamertypen und Positionierung

4.0 Assessments & Audits

4.1 Führen Sie eine Risikoeinschätzung und eine Risikominimierung durch.

4.2 Führen Sie eine Verwundbarkeitseinschätzung mit Hilfe gebräuchlicher Tools durch.

- Portscanner
- Verwundbarkeitsscanner (Vulnerability Scanner)
- Protokollanalytiker
- OVAL
- Passwortknacker
- Network Mapper

4.3 Erklären Sie den richtigen Gebrauch von Penetrationstests im Gegensatz zu einem Verwundbarkeitsscan im Rahmen der Verwundbarkeitseinschätzung.

4.4 Benutzen Sie Überwachungstools auf Systemen und Netzwerken und entdecken Sie Anomalien im Bereich der Sicherheit.

- Leistungsmonitor
- Systemmonitor

- Leistungsbasiswert
- Protokollanalytiker

4.5 Vergleichen Sie verschiedene Arten von Überwachungsmethoden und grenzen Sie diese voneinander ab.

- Verhaltensbasiert
- Signaturbasiert
- Anomaliebasiert

4.6 Führen Sie adäquate Protokollierungsmaßnahmen durch und werten Sie die Ergebnisse aus.

- Sicherheitsanwendung
- DNS
- System
- Leistung
- Zugang
- Firewall
- Antivirus

4.7 Führen Sie regelmäßige Audits der Systemsicherheitseinstellungen durch.

- Benutzerzugänge und -rechte überprüfen
- Speicher- und Rückhalteverfahren
- Gruppenrichtlinien

5.0 Kryptografie

5.1 Erklären Sie allgemeine kryptografische Konzepte.

- Schlüsselmanagement
- Steganografie
- Symmetrische Schlüssel
- Asymmetrische Schlüssel
- Vertraulichkeit
- Integrität und Verfügbarkeit
- Unleugbarkeit
- Komparative Stärke von Algorithmen
- Digitale Signaturen
- Verschlüsselung der ganzen Platte
- Trusted Platform Module (TPM)
- Einseitige vs. beidseitige Zertifikate
- Gebrauch bewährter Technologien

5.2 Erklären Sie grundlegende Hashing-Konzepte und ordnen Sie verschiedene Algorithmen den richtigen Anwendungen zu.

- SHA
- MD5
- LANMAN
- NTLM

5.3 Erklären Sie grundlegende Verschlüsselungsverfahren und ordnen Sie verschiedene Algorithmen den richtigen Anwendungen zu.

- DES
- 3DES

- RSA
- PGP
- Elliptische Kurve
- AES
- AES256
- One-Time-Pad
- Übertragungsverschlüsselung (WEP, TKIP etc.)

5.4 Erklären Sie Protokolle und implementieren Sie diese.

- SSL/TLS
- S/MIME
- PPTP
- HTTP vs. HTTPS vs. SHTTP
- L2TP
- IPSEC
- SSH

5.5 Erklären Sie die Kernkonzepte von Kryptografie mit Hilfe öffentlicher Schlüssel.

- Public Key Infrastructure (PKI)
- Recovery Agent
- Öffentlicher Schlüssel
- Privater Schlüssel
- Certificate Authority (CA)
- Registrierung
- Schlüsselurkunde
- Certificate Revocation List (CRL)
- Trust Modelle

5.6 Implementieren Sie PKI und ein Zertifikatmanagement.

- Public Key Infrastructure (PKI)
- Recovery Agent
- Öffentlicher Schlüssel
- Privater Schlüssel
- Certificate Authority (CA)
- Registrierung
- Schlüsselurkunde
- Certificate Revocation List (CRL)

6.0 Betriebssicherheit

6.1 Erklären Sie Redundanzplanung und ihre Komponenten.

- Hot Site
- Cold Site
- Warm Site
- Backup Aggregat
- Single point of failure
- RAID
- Ersatzteile
- Redundante Server
- Redundante ISP
- USV
- Redundante Verbindungen

6.2 Führen Sie ein Prozedere für das Disaster Recovery ein.

- Planung
- Disaster Recovery Übungen
- Backup Techniken und Praktiken - Speicher
- Schemata
- Wiederherstellung

6.3 Differenzieren Sie geeignete Vorgehensweisen als Reaktion auf einen Zwischenfall und führen Sie diese aus.

- Forensik
- Überwachungskette
- Helfer vor Ort
- Schadens- und Verlustkontrolle
- Bericht - Bekanntmachung

6.4 Identifizieren und erklären Sie zutreffende Vorschriften und betriebliche Richtlinien.

- Sichere Entsorgung von Computern
- Annehmbare Benutzungsrichtlinien
- Passwortkomplexität
- Änderungsmanagement
- Klassifizierung von Informationen
- Vorgeschriebener Urlaub
- Personenbezogene Daten (PII)
- Erforderliche Sorgfalt
- Erforderliche Gewissenhaftigkeit
- Erforderliche Vorgehensweise
- SLA
- Sicherheitsbezogene Personal-Regeln
- Benutzeraufklärung und Bewusstseinstraining

6.5 Erklären Sie die Wichtigkeit von Umgebungskontrollen.

- Feuerbekämpfung
- HVAC
- Schirmung

6.6 Erklären Sie das Konzept von Social Engineering und wie man dessen Risiken minimieren kann.

- Phishing
- Hoaxes
- Shoulder Surfing
- Dumpster Diving
- Benutzeraufklärung und Bewusstseinstraining

SECURITY+ AKRONYME

3DES	Triple Digital Encryption Standard
ACL	Access Control List
AES	Advanced Encryption Standard
AES256	Advanced Encryption Standards 256bit
AH	Authentication Header
ALE	Annualized Loss Expectancy
ARO	Annualized Rate of Occurrence
ARP	Address Resolution Protocol
AUP	Acceptable Use Policy
BIOS	Basic Input / Output System
BOTS	Network Robots
CA	Certificate Authority
CAN	Controller Area Network
CCTV	Closed-circuit television
CHAP	Challenge Handshake Authentication Protocol
CRL	Certification Revocation List
DAC	Discretionary Access Control
DDOS	Distributed Denial of Service
DES	Digital Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DLL	Dynamic Link Library
DMZ	Demilitarized Zone
DNS	Domain Name Service (Server)
DOS	Denial of Service
EAP	Extensible Authentication Protocol
ECC	Elliptic Curve Cryptography
FTP	File Transfer Protocol
GRE	Generic Routing Encapsulation
HIDS	Host Based Intrusion Detection System
HIPS	Host Based Intrusion Prevention System
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over SSL
HVAC	Heating, Ventilation Air Conditioning
ICMP	Internet Control Message Protocol
ID	Identifikation
IM	Instant Messaging
IMAP4	Internet Message Access Protocol v4
IP	Internet Protokoll
IPSEC	Internet Protocol Security
IRC	Internet Relay Chat

ISP	Internet Service Provider
KDC	Key Distribution Center
L2TP	Layer 2 Tunneling Protocol
LANMAN	Local Area Network Manager
LDAP	Lightweight Directory Access Protocol
MAC	Mandatory Access Control / Media Access Control
MAC	Message Authentication Code
MAN	Metropolitan Area Network
MD5	Message Digest 5
MSCHAP	Microsoft Challenge Handshake Authentication Protocol
MTU	Maximum Transmission Unit
NAC	Network Access Control (Netzwerkzugangskontrolle)
NAT	Network Address Translation
NIDS	Network Based Intrusion Detection System
NIPS	Network Based Intrusion Prevention System
NOS	Network Operating System (Netzwerkbetriebssystem)
NTFS	New Technology File System
NTLM	New Technology LANMAN
NTP	Network Time Protocol
OS	Betriebssystem
OVAL	Open Vulnerability Assessment Language
PAP	Password Authentication Protocol
PAT	Port Address Translation
PBX	Private Branch Exchange
PGP	Pretty Good Privacy
PII	Personally Identifiable Information (Personenbezogene Daten)
PKI	Public Key Infrastructure
PPP	Point-to-point Protocol
PPTP	Point to Point Tunneling Protocol
RAD	Rapid application development
RADIUS	Remote Authentication Dial-in User Server
RAID	Redundant Array of Inexpensive Disks
RAS	Remote Access Server
RBAC	Role Based Access Control
RBAC	Role Based Access Control
RSA	Rivest, Shamir, & Adleman
S/MIME	Secure / Multipurpose internet Mail Extensions
SCSI	Small Computer System Interface
SHA	Secure Hashing Algorithm
SHTTP	Secure Hypertext Transfer Protocol
SLA	Service Level Agreement
SLE	Single Loss Expectancy
SMTF	Simple Mail Transfer Protocol

SNMP	Simple Network Management Protocol
SPIM	Spam over Internet Messaging
SSH	Secure Shell
SSL	Secure Sockets Layer
SSO	Single Sign On
STP	Shielded Twisted Pair
TACACS	Terminal Access Controller Access Control System
TCP/IP	Transmission Control Protocol / Internet Protocol
TKIP	Temporal Key Integrity Protocol
TKIP	Temporal Key Interchange Protocol
TLS	Transport Layer Security
TPM	Trusted Platform Module
USV	Unterbrechungsfreie Stromversorgung
URL	Universal Resource Locator
USB	Universal Serial Bus
UTP	Unshielded Twisted Pair
VLAN	Virtual Local Area Network
VoIP	Voice over IP
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access

