CompTIA Security+ Exam Notes

Compiled By Examnotes.com

Abstract:

This study guide will help prepare you for your Security+ Beta exam. Never rely on only one source of information to prepare for a single exam, please use the guide as a way to add to your research and study.

CompTIA Security+ Certification
Security+ is a vendor-neutral certification exam currently under development that covers the foundations of information security.

Financial losses due to computer breaches average $1.5 million per company. Theft and destruction of intellectual property takes place despite the presence of firewalls, encryption and corporate edicts. Neither technologies nor policies alone offer effective information security. The IT industry must have a well-trained work force to effectively combat hackers and decrease financial losses.

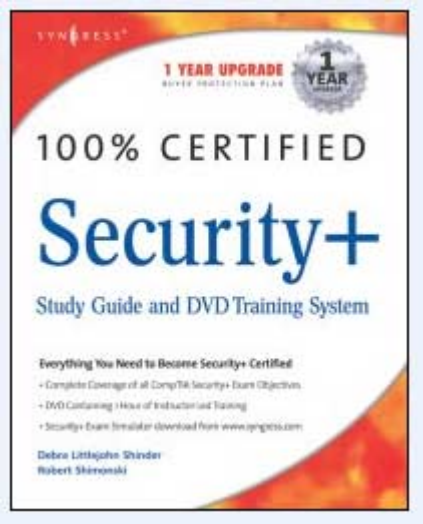
As a representative of the IT industry, CompTIA responded to the need for a knowledgeable security workforce by creating and hosting a committee of industry experts to build the Security+ certification exam:

- **Learn More About the CompTIA Security+ Exam**
  Get your answers here! Learn more about the CompTIA Security+ certification exam including exam development information and the answers to frequently asked questions.
- **Security+ Beta Exam Information**
  Be a part of the CompTIA Security+ Beta exam and become Security+ certified at a lower cost. Get all of the details on participating in the Security+ Beta test.

Also: Please look over and read Study Notes on the CIW Security Exam, which covers most of the topics listed in Security+

The following publication will aid in your studies. It will be one of the first Security+ guides on the market, written by certification AND working security specialists… it guarantees to prepare you for the real exam.

Security+ Study Guide and DVD Training System



What you need to know

Blueprint details are as follows. Make sure you go over all objectives, memorize what is on the test, and do further research to answer the items you don't know.

General Security Concepts

Access Control

MAC/DAC/RBAC – know the differences between Mandatory Access Control, Discretionary Access Control and Rule based Access Control. DO not configure Rule based with Role based.

Authentication

Know how to configure authentication for you systems. Know the differences between each authentication type and what type of cryptology is used with each.

- Kerberos – a ticket based system
- CHAP – CHAP is more secure than PAP
- Certificates – know why certificates are used. A certificate authority in a PKI system with issue certificates to guarantee authenticity
- Username/Password – standard authentication method
- Tokens – RSA SecurID is an example. Remember that one time passwords can be used
- Multi-Factor – instead of one factor of authentication, you can have 2 or more like using username and passwords with a biometrics system.
- Biometrics – hand scanning, retina scans and Smartcards for authentication

Non-essential Services and Protocols - Disabling unnecessary systems / process / programs

Simple – disable what you don't need to that your systems wont be exploited based on running services and protocols you are not using

Attacks

- DOS/DDOS – a denial of service attack is when you attack a system to block usage from legitimate systems. The legitimate systems are given a denial of service. DDOS is the distributed form where the attack comes from multiple locations.
- Back Door – a back door left in a program where the software creator (or hacker) sneaks in by
- Man in the Middle – a hacker can get in the middle of a session and eavesdrop of poison the conversation
- Replay – capturing data and replaying it for exploitation – like replaying a password to enter a system
- TCP/IP Hijacking – taking over a TCPIP session
- Weak Keys, Mathematical and Birthday attacks are all cytological attacks used to break ciphers
- Password Guessing – the act of guessing passwords to enter a system
- Brute Force – an onslaught attack that doesn't stop until the password is cracked. Will use any combination known to crack the password
- Dictionary – using a dictionary file to crack easy passwords
- Software Exploitation – exploiting bugs and known flaws

Social Engineering

The act of tricking users into giving up system information

WLAN

- A wireless LAN is one in which a mobile user can connect to a local area network (LAN) through a wireless (radio) connection
- A standard, **IEEE 802.11**, specifies the technologies for wireless LANs
- The standard includes an encryption method, the **Wired Equivalent Privacy** algorithm
- Wi-Fi is the popular term for a high-frequency wireless local area network (**WLAN**)
- Wi-Fi is specified in the **802.11b** specification from the Institute of Electrical and Electronics Engineers (IEEE) and is part of a series of wireless specifications together with **802.11, 802.11a, and 802.11g**
- All four standards use the Ethernet protocol and CSMA/CA (carrier sense multiple access with collision avoidance) for path sharing
- The 802.11b (Wi-Fi) operates in the 2.4 GHz range offering data speeds up to 11 megabits per second
- The modulation used in 802.11 has historically been phase-shift keying (PSK).
- The modulation method selected for 802.11b is known as complementary code keying (CCK), which allows higher data speeds and is less susceptible to multipath-propagation interference

- Unless adequately protected, a Wi-Fi wireless LAN can be susceptible to access from the outside by unauthorized users, some of who have used the access as a free Internet connection
- The activity of locating and exploiting security-exposed wireless LANs is commonly known as war driving.
- War driving is the act of locating and possibly exploiting connections to wireless local area networks while driving around a city or elsewhere. To do war driving, you need a vehicle, a computer (which can be a laptop), a wireless Ethernet card set to work in promiscuous mode, and some kind of an antenna which can be mounted on top of or positioned inside the car
- Companies that have a wireless LAN are urged to add security safeguards such as the Wired Equivalent Privacy (WEP) encryption standard, the setup and use of a virtual private network (VPN) or IPsec, and a firewall or DMZ
- Wired Equivalent Privacy (WEP) is a security protocol, specified in the IEEE Wireless Fidelity (Wi-Fi) standard, 802.11b that is designed to provide a wireless local area network (WLAN) with a level of security and privacy comparable to what is usually expected of a wired LAN.
- WEP seeks to establish protection to that offered by the wired network's physical security measures by encrypting data transmitted over the WLAN.
- Data encryption protects the vulnerable wireless link between clients and access points; once this measure has been taken, other typical LAN security mechanisms such as password protection, end-to-end encryption, virtual private networks (VPNs), and authentication can be put in place to ensure privacy
- A research group from the University of California at Berkeley recently published a report citing "major security flaws" in WEP that left WLANs using the protocol vulnerable to attacks (called wireless equivalent privacy attacks).
- The Wireless Ethernet Compatibility Alliance (WECA) claims that WEP - which is included in many networking products - was never intended to be the sole security mechanism for a WLAN, and that, in conjunction with traditional security practices, it is very effective

802.11

- 802.11 is a family of specifications for wireless local area networks (WLANs) developed by a working group of the Institute of Electrical and Electronics Engineers (IEEE)
- There are currently four specifications in the family: 802.11, 802.11a, 802.11b, and 802.11g
- All four use the Ethernet protocol and CSMA/CA (carrier sense multiple access with collision avoidance) for path sharing.
- The most recently approved standard, 802.11g, offers wireless transmission over relatively short distances at up to **54 megabits per second** (Mbps) compared with the **11 megabits per second** of the 802.11b standard
- Like 802.11b, 802.11g operates in the 2.4 GHz range and is thus compatible with it.

AAA

- Authentication, authorization, and accounting (AAA) is a term for a framework for intelligently controlling access to computer resources, enforcing policies, auditing usage, and providing the information necessary to bill for services
- These combined processes are considered important for effective network management and security

- As the first process, authentication provides a way of identifying a user, typically by having the user enter a valid user name and valid password before access is granted
- The process of authentication is based on each user having a unique set of criteria for gaining access
- The AAA server compares a user's authentication credentials with other user credentials stored in a database
- If the credentials match, the user is granted access to the network
- If the credentials are at variance, authentication fails and network access is denied.
- Authentication, authorization, and accounting services are often provided by a dedicated AAA server, a program that performs these functions
- A current standard by which network access servers interface with the AAA server is the Remote Authentication Dial-In User Service (RADIUS) or Tacacs+

PKI

- A PKI (public key infrastructure) enables users of a basically unsecure public network such as the Internet to securely and privately exchange data and money through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority
- The public key infrastructure provides for a digital certificate that can identify an individual or an organization and directory services that can store and, when necessary, revoke the certificates
- The public key infrastructure assumes the use of public key cryptography, which is the most common method on the Internet for authenticating a message sender or encrypting a message
- A public key infrastructure consists of:
    - A certificate authority (CA) that issues and verifies digital certificate. A certificate includes the public key or information about the public key
    - A registration authority (RA) that acts as the verifier for the certificate authority before a digital certificate is issued to a requestor
    - One or more directories where the certificates (with their public keys) are held
    - A certificate management system

Asymmetric and Symmetric

- Asymmetric cryptography is cryptography in which a pair of keys is used to encrypt and decrypt a message so that it arrives securely
- A user requests a public and private key pair.
- A user who wants to send an encrypted message can get the intended recipient's public key from a public administrator.
- When the recipient gets the message, they decrypt it with their private key, which no one else should have access to.
- This process is known as a public key infrastructure.
- In symmetric cryptography, the same key is used for both encryption and decryption.
- This approach is simpler but less secure since the key must be communicated to and known at both sender and receiver locations

Malware

www.sarc.com

- Malware (for "malicious software") is programming or files that are developed for the purpose of doing harm.
- Malware includes computer viruses, worms, and Trojan horses.
- A virus is a piece of programming code usually disguised as something else that causes some unexpected and usually undesirable event
- A virus is often designed so that it is automatically spread to other computer users
- Viruses can be transmitted as attachments to an e-mail note, as downloads, or be present on a diskette or CD
- The source of the e-mail note, downloaded file, or diskette you've received is often unaware of the virus
- Generally, there are three main classes of viruses:
    - File infectors
    - System or boot-record infectors
    - Macro viruses
- The best protection against a virus is to know the origin of each program or file you load into your computer or open from your e-mail program and make sure you have updated virus protection software, engines and definitions on your systems

Nonrepudiation

- In general, Nonrepudiation is the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated
- On the Internet, the digital signature is used not only to ensure that a message or document has been electronically signed by the person that purported to sign the document, but also, since a digital signature can only be created by one person, to ensure that a person cannot later deny that they furnished the signature
- Since no security technology is absolutely foolproof, some experts warn that the digital signature alone may not always guarantee Nonrepudiation
- It is suggested that multiple approaches be used, such as capturing unique biometric information and other data about the sender or signer that collectively would be difficult to repudiate

Smurfing

- Smurfing is the attacking of a network by exploiting Internet Protocol (IP) broadcast addressing and certain other aspects of Internet operation
- The exploit of smurfing, as it has come to be known, takes advantage of certain known characteristics of the Internet Protocol (IP) and the Internet Control Message Protocol (ICMP)
- ICMP is used by network nodes and their administrators to exchange information about the state of the network

- ICMP can be used to ping other nodes to see if they are operational. An operational node returns an echo message in response to a ping message.
- A smurf program builds a network packet that appears to originate from another address (this is known as spoofing an IP address)
- The packet contains an ICMP ping message that is addressed to an IP broadcast address, meaning all IP addresses in a given network
- The echo responses to the ping message are sent back to the "victim" address. Enough pings and resultant echoes can flood the network making it unusable for real traffic
- One way to defeat smurfing is to disable IP broadcast addressing at each network router since it is seldom used

Social Engineering

- In computer security, social engineering is a term that describes a non-technical kind of intrusion that relies heavily on human interaction and often involves tricking other people to break normal security procedures
- A social engineer runs what used to be called a "con game". For example, a person using social engineering to break into a computer network would try to gain the confidence of someone who is authorized to access the network in order to get them to reveal information that compromises the network's security
- They might call the authorized employee with some kind of urgent problem; social engineers often rely on the natural helpfulness of people as well as on their weaknesses

DDOS

- On the Internet, a distributed denial-of-service (DDoS) attack is one in which a multitude of compromised systems attack a single target, thereby causing denial of service for users of the targeted system
- The flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to the system to legitimate users.

Disaster Recovery (Hot / Cold Site)

- A hot site is a commercial disaster recovery service that allows a business to continue computer and network operations in the event of a computer or equipment disaster
- A cold site is a similar type of disaster recovery service that provides office space, but the customer provides and installs all the equipment needed to continue operations

Infrastructure Security

Devices

- Firewalls – used to filter traffic and create a choke point into your infrastructure
- Routers – used to route packets… can also be fixed with ACL's of access control lists for security
- Switches – you can configure VLANs on them for security. VLANs will separate broadcast domains and subnets and you can apply security that way
- Wireless – wireless systems are very vulnerable to attack. You must know how to apply encryption to secure these systems
- Modems – modems allow for dial in access to your infrastructure. Know they are susceptible to war dialing an exploitation
- VPN – virtual private networks… used to encrypt personal data over an unsecure medium like the Internet
- IDS – intrusion detection systems used for host and network based intrusion detection

Security Topologies

- DMZ – Demilitarized Zone used to create an isolated segment for public access into your infrastructure
- Extranet – usually a VPN based connection from business partners to your company for exchanging business data

Education – Training of end users, executives and HR

- User Awareness – make sure you users are aware of the dangers of hackers and exploitation especially in secure environments
- Education – educating them is the best way… they are generally the weakest link in your security infrastructure
- Online Resources – make sure personnel know how to find information online especially for research purposes

Documentation

- You must have network documentation in times of security planning and disaster recover
- You will also need a security policy / and a disaster recovery plan for you infrastructure.

Last Study Tips

This exam is not hard… it just covers a lot of information. You may want to wait until you have a study guide to read from if you are seriously going to approach this exam. There is a lot tested on cryptology for example and if you don't know PKI and Encryption types like the back of you hand, you may be wasting your money. Its not a hard exam, but don't take it too lightly – you may be surprised on what you are expected to know. Good luck.