Security+ Exam

Demo Version
From
ITCertKeys.com
To
CertsBraindumps.com

Question 1.
What functionality should be disallowed between a DNS server and untrusted node?

A. name resolutions
B. reverse ARP requests
C. system name resolutions
D. zone transfers

Answer: D

Explanation:
Users who can start zone transfers from your server can list all of the records in your zones.

Question 2.
A document written by the CEO that outlines PKI use, management and deployment is a...

A. PKI policy
B. PKI procedure
C. PKI practice
D. best practices guideline

Answer: A

Explanation:
Definition of Policy - course of action, guiding principle, or procedure considered expedient, prudent, or advantageous.

Question 3.
What port does SNMP use?

A. 21
B. 161
C. 53
D. 49

Answer: B

Explanation:
SNMP uses UDP port 161

Question 4.
What port does TACACS use?

A. 21
B. 161
C. 53
D. 49

Answer: A

Explanation:
TACACS uses UDP port 49.

Question 5.
What are the four major components of ISAKMP (Internet Security Association and Key Management Protocol)?

A. Authentication of peers, threat management, communication management, and cryptographic key establishment.
B. Authentication of peers, threat management, communication management, and cryptographic key establishment and management.
C. Authentication of peers, threat management, security association creation and management cryptographic key establishment and management.
D. Authentication of peers, threat management, security association creation and management and cryptographic key management.

Answer: C

Explanation:
The four major functional components of ISAKMP are:
- Authentication of communications peers.
- Threat mitigation.
- Security association creation and management.
- Cryptographic key establishment and management.

Question 6.
The standard encryption algorithm based on Rijndael is known as:

A. AES (Advanced Encryption Standard)
B. 3DES (Triple Data Encryption Standard)
C. DES (Data Encryption Standard)
D. Skipjack

Answer: A

Explanation:
Rijndael is a symmetric-key block cipher. After a competition Rijndael was selected as the successor to DES and became the Advanced Encryption Standard, or AES.

Question 7.
An extranet would be best defined as an area or zone:

A. Set aside for business to store extra servers for internal use.
B. Accessible to the general public for accessing the business' web site.
C. That allows a business to securely transact with other businesses.
D. Added after the original network was built for additional storage.

Answer: C

Explanation:
An extranet is a private network that uses the Internet protocol and the public telecommunication system to securely share part of a business's information or operations with suppliers, vendors, partners, customers, or other businesses. An extranet can be viewed as part of a company's intranet that is extended to users outside the company.

Question 8.
A network attack method that uses ICMP (Internet Control Message Protocol) and improperly formatted MTUs (Maximum Transmission Unit) to crash a target computer is known as a:

A. Man in the middle attack
B. Smurf attack
C. Ping of death attack
D. TCP SYN (Transmission Control Protocol / Synchronized) attack

Answer: C

Explanation:
The Ping of Death attack involved sending IP packets of a size greater than 65,535 bytes to the target computer. IP packets of this size are illegal, but applications can be built that are capable of creating them. Carefully programmed operating systems could detect and safely handle illegal IP packets, but some failed to do this.

Packets that are bigger than the maximum size the underlying layer can handle (the MTU) are fragmented into smaller packets, which are then reassembled by the receiver
For ethernet style devices, the MTU is typically 1500.

A man in the middle attack allows a third party to intercept and replace components of the data stream.

The "smurf" attack, named after its exploit program, is one of the most recent in the category of network- level attacks against hosts. A perpetrator sends a large amount of ICMP echo (ping) traffic at IP broadcast addresses, all of it having a spoofed source address of a victim.

In a TCP SYN attack a sender transmits a volume of connections that cannot be completed. This causes the connection queues to fill up, thereby denying service to legitimate TCP users.

Question 9.
Which systems should be included in a disaster recover plan?

A. All systems.
B. Those identified by the board of directors, president or owner.
C. Financial systems and human resources systems.
D. Systems identified in a formal risk analysis process.

Answer: D

Explanation:
A preliminary risk analysis is performed to identify business critical applications and functions. Once those functions have been identified and documented, we prepared a structured approach to disaster recovery for the organization.

Question 10.
What is the best defence against man in the middle attacks?

A. A firewall
B. Strong encryption
C. Strong authentication
D. Strong passwords

Answer: C

Explanation:
A man in the middle (MITM) attack, means that someone places himself in the communication channel between the two parties already at the time of certificate exchange. When a party sends its public key to the other, the MITM takes this key and replaces it by his own. The other party

thinks the key just received came from the expected sender, but in fact it comes from the MITM. That's the reasons why public keys should be signed by a trusted authority (a.k.a. "trust center" or "certificate authority").

Question 11.
Analyzing log files after an attack has started as an example of:

A. Active detection
B. Overt detection
C. Covert detection
D. Passive detection

Answer: D

Explanation:
Passive intrusion detection systems involve the manual review of event logs and application logs. The inspection involves analysis and detection of attack patterns in event log data.

Question 12.
Which of the following steps in the SSL (Secure Socket Layer) protocol allows for client and server authentication, MAC (Mandatory Access Control) and encryption algorithm negotiation, and selection of cryptographic keys?

A. SSL (Secure Sockets Layer) alert protocol.
B. SSL (Secure Sockets Layer) change cipher spec protocol.
C. SSL (Secure Sockets Layer) record protocol.
D. SSL (Secure Sockets Layer) handshake protocol.

Answer: D

Explanation:
SSL Handshake Protocol

- run before any application data is transmitted
- provides mutual authentication
- establishes secret encryption keys
- establishes secret MAC keys

Question 13.
Which of the following correctly identifies some of the contents of an user's X.509 certificate?

A. User's public key, object identifiers, and the location of the user's electronic identity.
B. User's public key, the CA (Certificate Authority) distinguished name, and the type of symmetric algorithm used for encryption.
C. User's public key, the certificate's serial number, and the certificate's validity dates.
D. User's public key, the serial number of the CA (Certificate Authority) certificate, and the CRL (Certificate Revocation List) entry point.

Answer: B

Explanation:
The X.509 standard defines what information can go into a certificate, and describes how to write it down (the data format). All X.509 certificates have the following data, in addition to the signature:

Version Serial Number The entity that created the certificate, the CA, is responsible for assigning it a serial number to distinguish it from other certificates it issues. Signature Algorithm Identifier Issuer Name The X.500 name of the entity that signed the certificate. This is normally a CA. Using this certificate implies trusting the entity that signed this certificate. Validity Period Subject Name Subject Public Key Information This is the public key of the entity being named, together with an algorithm identifier which specifies which public key crypto system this key belongs to and any associated key parameters.

Question 14.
An organization is implementing Kerberos as its primary authentication protocol. Which of the following must be deployed for Kerberos to function properly?

A. Dynamic IP (Internet Protocol) routing protocols for routers and servers.
B. Separate network segments for the realms.
C. Token authentication devices.
D. Time synchronization services for clients and servers.

Answer: D

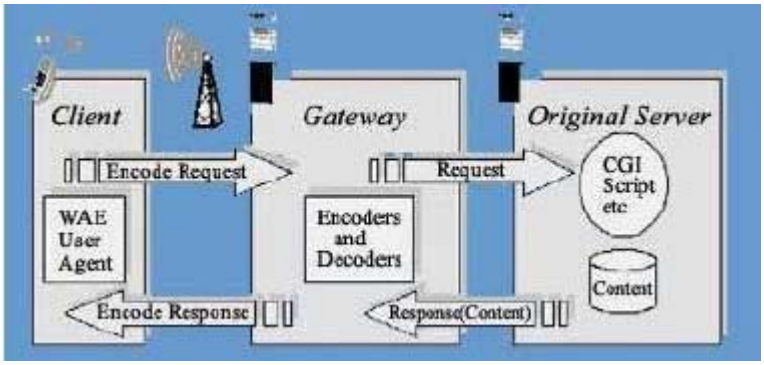
Explanation:
Time synchronization is crucial because Kerberos uses server and workstation time as part of the authentication process.

Question 15.
The WAP (Wireless Application Protocol) programming model is based on the following three elements:

A. Client, original server, WEP (Wired Equivalent Privacy)
B. Code design, code review, documentation
C. Client, original server, wireless interface card
D. Client, gateway, original server

Answer: D

Explanation:
WAPprogramming model:



Question 16.
Privileged accounts are most vulnerable immediately after a:

A. Successful remote login.
B. Privileged user is terminated.
C. Default installation is performed.

D. Full system backup is performed.

Answer: B

Explanation:
A fired domain admin could easily RAS or VPN in and wreck havoc if his/her privileged account is not disabled.

Question 17.
What is the most common method used by attackers to identify the presence of an 801.11b network?

A. War driving
B. Direct inward dialing
C. War dialing
D. Packet driving

Answer: A

Explanation:
War driving is the practice of literally driving around looking for free connectivity from Wi-Fi networks.

Option B does not apply.

In war dialing combinations of numbers are tested to find network back doors via modem.

Option D does not apply.

Question 18.
The most effective way an administrator can protect users from social engineering is:

A. Education
B. Implement personal firewalls.
C. Enable logging on at user's desktops.
D. Monitor the network with an IDS (Intrusion Detection System)

Answer: A

Explanation:
Social engineering: An outside hacker's use of psychological tricks on legitimate users of a computer system, in order to gain the information (usernames and passwords) he needs to gain access to the system.

Question 19.
Which of the following is the best description of "separation of duties"?

A. Assigning different parts of tasks to different employees.
B. Employees are granted only the privileges necessary to perform their tasks.
C. Each employee is granted specific information that is required to carry out the job function.
D. Screening employees before assigning them to a position.

Answer: A

Explanation:
A task needs several people involved as a method of checks and balances.

Question 20.
What fingerprinting technique relies on the fact that operating systems differ in the amount of information that is quoted when ICMP (Internet Control Message Protocol) errors are encountered?

A. TCP (Transmission Control Protocol) options.
B. ICMP (Internet Control Message Protocol) error message quenching.
C. Fragmentation handling.
D. ICMP (Internet Control Message Protocol) message quoting.

Answer: D

Explanation:
ICMP Message quoting: The ICMP quotes back part of the original message with every ICMP error message. Each operating system will quote definite amount of message to the ICMP error messages. The peculiarity in the error messages received from various types of operating systems helps us in identifying the remote host's OS.

Question 21.
A common algorithm used to verify the integrity of data from a remote user through a the creation of a 128-bit hash from a data input is:

A. IPSec (Internal Protocol Security)
B. RSA (Rivest Shamir Adelman)
C. Blowfish
D. MD5 (Message Digest 5)

Answer: D

Explanation:
The MD5 hashing algorithm that creates a 128-bit hash value.

Question 22.
What is the best method of defence against IP (Internet Protocol) spoofing attacks?

A. Deploying intrusion detection systems.
B. Creating a DMZ (Demilitarized Zone).
C. Applying ingress filtering to routers.
D. Thee is not a good defense against IP (Internet Protocol) spoofing.

Answer: C

Explanation:
IP Spoofing attacks that take advantage of the ability to forge (or "spoof") IP address can be prevented by implementing Ingress and Egress filtering on the network perimeter.

Question 23.
A server placed into service for the purpose of attracting a potential intruder's attention is known as a:

A. Honey pot
B. Lame duck
C. Teaser
D. Pigeon

Answer: A

Explanation:
A honeypot is a system which uses fake server and send alarms when some "bad guy" try to exploit some bug. The goal is to learn how black-hats probe for and exploit a system. By learning their tools and methods, you can then better protect your network and systems.

Question 24.
Which one of the following would most likely lead to a CGI (Common Gateway Interface) security problem?

A. HTTP (Hypertext Transfer Protocol) protocol.
B. Compiler or interpreter that runs the CGI (Common Gateway Interface) script.
C. The web browser.
D. External data supplied by the user.

Answer: D

Explanation:
CGI scripts can present security holes in two ways:

1. They may intentionally or unintentionally leak information about the host system that will help hackers break in.
2. Scripts that process remote user input, such as the contents of a form or a "searchable index" command, may be vulnerable to attacks in which the remote user tricks them into executing commands.

Question 25.
The primary DISADVANTAGE of symmetric cryptography is:

A. Speed
B. Key distribution
C. Weak algorithms
D. Memory management

Answer: B

Explanation:
In symmetric encryption the message can be encrypted and decrypted using the same key.

Question 26.
Missing audit log entries most seriously affect an organization’s ability to:

A. Recover destroyed data.
B. Legally prosecute an attacker.
C. Evaluate system vulnerabilities.
D. Create reliable system backups.

Answer: C

Explanation:
The audit trail lets you detect suspicious activity from both outsiders and insiders and provides you with important evidence to use against intruders.

Question 27.

Which of the following provides privacy, data integrity and authentication for handles devices in a wireless network environment?

A. WEP (Wired Equivalent Privacy)
B. WAP (Wireless Application Protocol)
C. WSET (Wireless Secure Electronic Transaction)
D. WTLS (Wireless Transport Layer Security)

Answer: D

Explanation:
Short for Wireless Transport Layer Security. WTLS is the security layer of the WAP, providing privacy, data integrity and authentication for WAP services.

Not A: WEP is one of the most popular features available for a Wireless LAN. It is used to encrypt and decrypt data signals transmitted between Wireless LAN devices. In essence, WEP makes a wireless LAN link as secure as a wired link. However, WTLS

Question 28.
The system administrator concerned about security has designated a special area in which to place the web server away from other servers on the network. This area is commonly known as the?

A. Honey pot
B. Hybrid subnet
C. DMZ (Demilitarized Zone)
D. VLAN (Virtual Local Area Network)

Answer: C

Explanation:
A Demilitarized Zone is used by a company that wants to host its own Internet services without sacrificing unauthorized access to its private network.

Question 29.
Which encryption scheme relies on both the sender and receiver to use different keys to encrypt and decrypt messages?

A. Symmetric
B. Blowfish
C. Skipjack
D. Asymmetric

Answer: D

Explanation:
Asymmetric Encryption is a form of Encryption where keys come in pairs. What one key encrypts, only the other can decrypt.

In symmetric encryption the message can be encrypted and decrypted using the same key.

Blowfish is a symmetric block cipher that can be used as a drop-in replacement for DES or IDEA.

Skipjack is the encryption algorithm contained in the Clipper chip, and it was designed by the NSA.

Question 30.
A honey pot is _____.

A. A false system or network to attract attacks away from your real network.
B. A place to store passwords.
C. A sage haven for your backup media.
D. Something that exist only in theory.

Answer: A

Explanation:
A honey pot is a computer system on the Internet that is expressly set up to attract and "trap" people who attempt to penetrate other people's computer systems.