Vendor: CompTIA

Exam Code:JK0-022

Exam Name: CompTIA Security+ Certification

Version: Demo

QUESTION 1

Which of the following ports and protocol types must be opened on a host with a host-based firewall to allow incoming SFTP connections?

A. 21/UDP

B. 21/TCP

C. 22/UDP

D. 22/TCP

Correct Answer: D

SSH uses TCP port 22. All protocols encrypted by SSH, including SFTP, SHTTP, SCP, SExec, and slogin, also use TCP port 22.

Incorrect Answers:

A, C: FTP ,and SSH do not make use of UDP ports.

B: FTP uses TCP port 21.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 51.

QUESTION 2

Which of the following would satisfy wireless network implementation requirements to use mutual authentication and usernames and passwords?

A. EAP-MD5

B. WEP

C. PEAP-MSCHAPv2

D. EAP-TLS

Correct Answer: C

PEAP-MS-CHAP v2 is easier to deploy than EAP-TLS or PEAP-TLS because user authentication is accomplished via password-base credentials (user name and password) rather than digital certificates or smart cards.

Incorrect Answers:

A: MD5 has been employed in a wide selection of cryptographic applications, and is also commonly used to verify data integrity.

B: Usernames and passwords are not required for WEP authentication.

D: Authenticated wireless access design based on Extensible Authentication Protocol Transport Level Security (EAP-TLS) can use either smart cards or user and computer certificates to authenticate wireless access clients. EAP-TLS does not use usernames and passwords for authentication.

References:

https://technet.microsoft.com/en-us/library/dd348500(v=ws.10).aspx https://technet.microsoft.com/en-us/library/dd348478(v=ws.10).aspx http://en.wikipedia.org/ wiki/MD5

QUESTION 3

It has been discovered that students are using kiosk tablets intended for registration and scheduling to play games and utilize instant messaging. Which of the following could BEST eliminate this issue?

A. Device encryption

B. Application control

C. Content filtering

D. Screen-locks

Correct Answer: B

QUESTION 4

A security analyst has been notified that trade secrets are being leaked from one of the executives in the corporation. When reviewing this executive\\'s laptop they notice several pictures of the employee\\'s pets are on the hard drive and on a cloud storage network. When the analyst hashes the images on the hard drive against the hashes on the cloud network they do not match.

Which of the following describes how the employee is leaking these secrets?

A. Social engineering

B. Steganography

C. Hashing

D. Digital signatures

Correct Answer: B

Steganography is the process of hiding one message in another. Steganography may also be referred to as electronic watermarking. It is also the process of hiding a message in a medium such as a digital image, audio fi le, or other fi le. In theory, doing this prevents analysts from detecting the real message. You could encode your message in another file or message and use that file to hide your message.

Incorrect Answers:

A: Social engineering is the process by which intruders gain access to your facilities, your network, and even your employees by exploiting the generally trusting nature of people. A social engineering attack may come from someone posing as a vendor, or it could take the form of an email from a (supposedly) traveling executive who indicates that they

have forgotten how to log on to the network or how to get into the building over the weekend.

C: Hashing refers to the hash algorithms used in Cryptography.

D: Digital Signatures is used to validate the integrity of the message and the sender.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 248, 255, 261, 355, 414

QUESTION 5

Which of the following types of attacks involves interception of authentication traffic in an attempt to gain unauthorized access to a wireless network?

A. Near field communication

B. IV attack

C. Evil twin

D. Replay attack

Correct Answer: B

An initialization vector is a random number used in combination with a secret key as a means to encrypt data. This number is sometimes referred to as a nonce, or "number occurring once," as an encryption program uses it only once per session. An initialization vector is used to avoid repetition during the data encryption process, making it impossible for hackers who use dictionary attack to decrypt the exchanged encrypted message by discovering a pattern. This is known as an IV attack. A particular binary sequence may be repeated more than once in a message, and the more it appears, the more the encryption method is discoverable. For example if a one-letter word exists in a message, it may be either "a" or "I" but it can\\'t be "e" because the word "e" is non-sensical in English, while "a" has a meaning and "I" has a meaning. Repeating the words and letters makes it possible for software to apply a dictionary and discover the binary sequence corresponding to each letter. Using an initialization vector changes the binary sequence corresponding to each letter, enabling the letter "a" to be represented by a particular sequence in the first instance, and then represented by a completely different binary sequence in the second instance.

WEP (Wireless Equivalent Privacy) is vulnerable to an IV attack. Because RC4 is a stream cipher, the same traffic key must never be used twice. The purpose of an IV, which is transmitted as plain text, is to prevent any repetition, but a 24-bit IV is not long enough to ensure this on a busy network. The way the IV was used also opened WEP to a related key attack. For a 24-bit IV, there is a 50% probability the same IV will repeat after 5000 packets.

Incorrect Answers:

A: Near field communication (NFC) is a set of short-range wireless technologies, typically requiring a distance of 10 cm or less. NFC operates at 13.56 MHz on ISO/IEC 18000-3 air interface and at rates ranging from 106 kbit/s to 424 kbit/s.

NFC always involves an initiator and a target; the initiator actively generates an RF field that can power a passive target. This enables NFC targets to take very simple form factors such as tags, stickers, key fobs, or cards that do not require

batteries. NFC peer-to-peer communication is possible, provided both devices are powered. NFC tags contain data and are typically read-only, but may be rewriteable. They can be custom- encoded by their manufacturers or use the

specifications provided by the NFC Forum, an industry association charged with promoting the technology and setting

key standards. The tags can securely store personal data such as debit and credit card information, loyalty program data,

PINs and networking contacts, among other information. The NFC Forum defines four types of tags that provide different communication speeds and capabilities in terms of configurability, memory, security, data retention and write

endurance. Tags currently offer between 96 and 4,096 bytes of memory. NFC does not involve interception of authentication traffic in an attempt to gain unauthorized access to a wireless network. This is not what is described in the question.

Therefore, this answer is incorrect.

C: An evil twin, in the context of network security, is a rogue or fake wireless access point (WAP) that appears as a genuine hotspot offered by a legitimate provider. In an evil twin attack, an eavesdropper or hacker fraudulently creates this

rogue hotspot to collect the personal data of unsuspecting users. Sensitive data can be stolen by spying on a connection or using a phishing technique.

For example, a hacker using an evil twin exploit may be positioned near an authentic Wi-Fi access point and discover the service set identifier (SSID) and frequency. The hacker may then send a radio signal using the exact same frequency

and SSID. To end users, the rogue evil twin appears as their legitimate hotspot with the same name. Evil twin does not involve interception of authentication traffic in an attempt to gain unauthorized access to a wireless network.

Therefore, this answer is incorrect.

D: A replay attack (also known as playback attack) is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an adversary who intercepts

the data and retransmits it, possibly as part of a masquerade attack by IP packet substitution (such as stream cipher attack). For example: Suppose Alice wants to prove her identity to Bob. Bob requests her password as proof of identity,

which Alice dutifully provides (possibly after some transformation like a hash function); meanwhile, Eve is eavesdropping on the conversation and keeps the password (or the hash). After the interchange is over, Eve (posing as Alice) connects

to Bob; when asked for a proof of identity, Eve sends Alice\\'s password (or hash) read from the last session, which Bob accepts thus granting access to Eve.

Replay attacks are used for impersonation rather than attempting to gain unauthorized access to a wireless network. Therefore, this answer is incorrect.

References: http://www.techopedia.com/definition/26858/initialization-vector http://en.wikipedia.org/wiki/Near_field_communication http://www.techopedia.com/definition/5057/evil-twin http://en.wikipedia.org/wiki/Replay_attack

---

QUESTION 6

A network administrator noticed various chain messages have been received by the company.

Which of the following security controls would need to be implemented to mitigate this issue?

A. Anti-spam

B. Antivirus

C. Host-based firewalls

D. Anti-spyware

Correct Answer: A

A spam filter is a software or hardware solution used to identify and block, filter, or remove unwanted messages sent via email or instant messaging (IM).

Incorrect Answers:

B: Antivirus software is used to protect systems against viruses, which are a form of malicious code designed to spread from one system to another.

C: A host-based firewall is installed on a client system and is used to protect the client system from the activities of the user as well as from communication from the network or Internet. It does not block email messages or instant messaging (IM) messages.

D: Spyware monitors a user\\'s activity and uses network protocols to reports it to a third party without the user\\'s knowledge. This is usually accomplished using a tracking cookie.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 18-19, 161-162, 300 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 246

QUESTION 7

A system administrator has concerns regarding their users accessing systems and secured areas using others\\' credentials. Which of the following can BEST address this concern?

A. Create conduct policies prohibiting sharing credentials.

B. Enforce a policy shortening the credential expiration timeframe.

C. Implement biometric readers on laptops and restricted areas.

D. Install security cameras in areas containing sensitive systems.

Correct Answer: C

Biometrics is an authentication process that makes use of physical characteristics to establish identification. This will prevent users making use of others credentials.

Incorrect Answers:

A: Policies need to be implemented and making use of biometrics would be to a way to prohibit sharing credentials.

B: This is still granting the same type of access that is already being abused with a time limit the only difference.

D: Security cameras are used to surveil and record; not to prevent access.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 375

QUESTION 8

A security specialist has been asked to evaluate a corporate network by performing a vulnerability assessment. Which of the following will MOST likely be performed?

A. Identify vulnerabilities, check applicability of vulnerabilities by passively testing security controls.

B. Verify vulnerabilities exist, bypass security controls and exploit the vulnerabilities.

C. Exploit security controls to determine vulnerabilities and misconfigurations.

D. Bypass security controls and identify applicability of vulnerabilities by passively testing security controls.

Correct Answer: A

We need to determine if vulnerabilities exist by passively testing security controls. A vulnerability scan is the automated process of proactively identifying security vulnerabilities of computing systems in a network in order to determine if and where a system can be exploited and/or threatened. While public servers are important for communication and data transfer over the Internet, they open the door to potential security breaches by threat agents, such as malicious hackers. Vulnerability scanning employs software that seeks out security flaws based on a database of known flaws, testing systems for the occurrence of these flaws and generating a report of the findings that an individual or an enterprise can use to tighten the network\\'s security. Vulnerability scanning typically refers to the scanning of systems that are connected to the Internet but can also refer to system audits on internal networks that are not connected to the Internet in order to assess the threat of rogue software or malicious employees in an enterprise.

Incorrect Answers:

B: Verifying vulnerabilities exist, bypassing security controls and exploiting the vulnerabilities describes an attack on the system or a penetration test. Penetration testing evaluates an organization\\'s ability to protect its networks, applications,

computers and users from attempts to circumvent its security controls to gain unauthorized or privileged access to protected assets. A penetration test can test one method at a time of accessing one system at a time. A vulnerability scan can

scan for all vulnerabilities on multiple systems and is therefore a better answer.

Therefore, this answer is incorrect.

C: Exploiting security controls to determine vulnerabilities and misconfigurations would be a slow and manual way of performing a vulnerability assessment. A vulnerability scan is an automated process of scanning for all vulnerabilities on

multiple systems and is therefore a better answer. Therefore, this answer is incorrect.

D: We need to first identify any vulnerabilities before we can check the applicability of the vulnerabilities. Therefore, this answer is incorrect.

References: http://www.webopedia.com/TERM/V/vulnerability_scanning.html

---

QUESTION 9

When performing the daily review of the system vulnerability scans of the network Joe, the administrator, noticed several security related vulnerabilities with an assigned vulnerability identification number. Joe researches the assigned vulnerability identification number from the vendor website. Joe proceeds with applying the recommended solution for identified vulnerability.

Which of the following is the type of vulnerability described?

A. Network based

B. IDS

C. Signature based

D. Host based

Correct Answer: C

A signature-based monitoring or detection method relies on a database of signatures or patterns of known malicious or unwanted activity. The strength of a signature-based system is that it can quickly and accurately detect any event from its

database of signatures.

Incorrect Answers:

A: A network-based IDS (NIDS) watches network traffic in real time. It\\'s reliable for detecting network-focused attacks, such as bandwidth-based DoS attacks.

B: An intrusion detection system (IDS) is an automated system that either watches activity in real time or reviews the contents of audit logs in order to detect intrusions or security policy violations.

C: A host-based IDS (HIDS) watches the audit trails and log fi les of a host system. It\\'s reliable for detecting attacks directed against a host, whether they originate from an external source or are being perpetrated by a user locally logged in to the host.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 21.

QUESTION 10

A company provides secure wireless Internet access for visitors and vendors working onsite. Some of the vendors using older technology report that they are unable to access the wireless network after entering the correct network information. Which of the following is the MOST likely reason for this issue?

A. The SSID broadcast is disabled.

B. The company is using the wrong antenna type.

C. The MAC filtering is disabled on the access point.

D. The company is not using strong enough encryption.

Correct Answer: A

When the SSID is broadcast, any device with an automatic detect and connect feature is able to see the network and can initiate a connection with it. The fact that they cannot access the network means that they are unable to see it.

Incorrect Answers:

B: The antenna type deals with signal strength and direction. It will not have a bearing on whether technology is older.

C: The network information is being given to the vendors, therefore MAC filtering is not the issue.

D: The network information is being given to the vendors, therefore encryption is not the issue.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 61.

QUESTION 11

Which of the following would allow the organization to divide a Class C IP address range into several ranges?

A. DMZ

B. Virtual LANs

C. NAT

D. Subnetting

Correct Answer: D

Subnetting is a dividing process used on networks to divide larger groups of hosts into smaller collections.

Incorrect Answers:

A: The DMZ is a buffer network between the public untrusted Internet and the private trusted LAN. Often a DMZ is deployed through the use of a multihomed firewall.

B: A virtual local area network (VLAN) is a hardware-imposed network segmentation created by switches.

C: NAT serves as a basic firewall by only allowing incoming traffic that is in response to an internal system\\'s request.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 39,

---

QUESTION 12

Everyone in the accounting department has the ability to print and sign checks. Internal audit has asked that only one group of employees may print checks while only two other employees may sign the checks. Which of the following concepts would enforce this process?

A. Separation of Duties

B. Mandatory Vacations

C. Discretionary Access Control

D. Job Rotation

Correct Answer: A

Separation of duties means that users are granted only the permissions they need to do their work and no more.

Incorrect Answers:

B: A mandatory vacation policy requires all users to take time away from work to refresh.

C: Discretionary Access Control makes allowance for flexibility on access control within the company which is to be avoided in this scenario.

D: Rotating jobs would mean that all the employees will at any one time still have authority to sign checks.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 25, 151, 153