CCST Networking – Module 15 Quiz

Questions

1. What type of network attack launches an exploit against a newly discovered vulnerability, before the developer can patch the vulnerability?

    a. phishing attack
    b. DDoS attack
    c. zero-day attack
    d. social engineering attack

2. A user on your network received a text message containing a link that took them to a malicious site. The user has been a victim of what type of social engineering attack?

    a. phishing
    b. spear phishing
    c. vishing
    d. smishing

3. Which of the following best describes the difference between a DoS and a DDoS attack?

    a. A DoS attack targets a single victim, while a DDoS attack targets multiple victims.
    b. A DoS attack is sourced from a single location, while a DDoS attack is sourced from multiple locations.
    c. A DoS attack uses a Command and Control Server, while a DDoS attack does not.
    d. A DoS attack leverages a botnet of infected devices while a DDoS attack does not.

4. Which of the following best describes a rogue access point that appears to be a legitimate wireless access point (e.g., has a matching SSID to a legitimate wireless access point)?

    a. evil twin
    b. spoofing
    c. deauthentication
    d. brute force

5. Which component of the CIA Triad does hashing primarily contribute?

    a. While hashing does add a layer of security, it does not directly impact any of the three components of the CIA Triad.
    b. Confidentiality

c. Integrity
d. Availability

6. Which security appliance can monitor traffic in-line and compare that traffic to a database of well-known attack signatures?

    a. IDS sensor
    b. Firewall
    c. IPS sensor
    d. ISE

7. Which of the following encryption standards is used for asymmetric encryption?

    a. 3DES
    b. RSA
    c. DES
    d. AES

8. You are considering which type of AAA server to install. Which of the following is a characteristic of a TACACS+ server but not a characteristic of a RADIUS server?

    a. industry-standard
    b. uses TCP instead of UDP
    c. performs a one-way challenge response
    d. encrypts the password but not the entire packet

9. When logging into your bank account, you enter your username and password. However, instead of being immediately logged in, you're instructed to enter a code that was texted to your smartphone. Only after entering that code are you successfully logged into your bank account. What type of authentication have you just performed?

    a. Single Sign-On
    b. Kerberos
    c. IEEE 802.1X
    d. MFA

10. What was the first wireless security standard to require support for the AES (Advanced Encryption Standard) algorithm?

    a. WEP
    b. WPA
    c. WPA2
    d. WPA3

11. You're setting up a wireless router for use within your company. On that wireless router, you configure a wireless network that you don't want advertised to visitors. What feature will you select while configuring your wireless router to suppress the advertisement of this wireless network name?

    a. No WPS
    b. Hide SSID
    c. OFDMA
    d. TWT

Questions and Answers

1. What type of network attack launches an exploit against a newly discovered vulnerability, before the developer can patch the vulnerability?

    a. phishing attack
    b. DDoS attack
    c. zero-day attack
    d. social engineering attack

    Answer: c

    Explanation: A vulnerability typically refers to a flaw in a secured system, while a threat (or exploit) typically refers to software that can take advantage of that vulnerability. An exploit launched against a newly discovered vulnerability, before the developer has patched the vulnerability, is called a "zero-day attack."

    Video Reference: Threats vs. Vulnerabilities

2. A user on your network received a text message containing a link that took them to a malicious site. The user has been a victim of what type of social engineering attack?

    a. phishing
    b. spear phishing
    c. vishing
    d. smishing

    Answer: d

    Explanation: Phishing occurs when an attacker sends e-mail to a large population, where the e-mail is attempting to have a user disclose confidential information, visit a website, download an application, or open a document (which might contain malware).

    Spear Phishing is a variant of phishing where the attack target is a single user or a small group of users, and where the e-mail mentions details about their target, thus making the e-mail more believable.

    Smishing performs phishing via text messaging (i.e., SMS (Short Message Service)), typically containing a link that directs the attack target to a malicious site.

    Vishing performs phishing via telephone (i.e., voice phishing), where the attacker could collect information about their target or where the attacker directs the user to perform specific actions.

Video Reference: Social Engineering Attacks

3. Which of the following best describes the difference between a DoS and a DDoS attack?

    a. A DoS attack targets a single victim, while a DDoS attack targets multiple victims.
    b. A DoS attack is sourced from a single location, while a DDoS attack is sourced from multiple locations.
    c. A DoS attack uses a Command and Control Server, while a DDoS attack does not.
    d. A DoS attack leverages a botnet of infected devices while a DDoS attack does not.

    Answer: b

    Explanation: A Denial of Service (DoS) attack overwhelms a targeted system with a large volume of requests, causing it to consume its resources to the point where it can't perform its intended function.

    The same is true for a Distributed Denial of Service (DDoS) attack. However, a DDoS attack can be more impactful than a DoS attack because a DDoS attack is sourced from multiple systems in multiple locations.

    Specifically, with a DDoS attack, an attacker infects multiple computers around the internet with malware to form a botnet of infected devices. Then, when the attacker is ready to launch their DDoS attack, they tell a command and control server to reach out to the botnet and instruct all of those infected devices to simultaneously attack the victim.

    Video Reference: Denial of Service Attacks

4. Which of the following best describes a rogue access point that appears to be a legitimate wireless access point (e.g., has a matching SSID to a legitimate wireless access point)?

    a. evil twin
    b. spoofing
    c. deauthentication
    d. brute force

    Answer: a

    Explanation: A rogue access point is any unauthorized access point installed on a network. For example, an attacker might connect a rogue access point to an Ethernet port in a network and then hide that access point behind a piece of furniture. That might allow the attacker to go outside the building while having wireless connectivity to the network.

However, an attacker might install a rogue access point in an attempt to capture login credentials from users. To do that, they might give the rogue access point the same wireless network name (i.e., the same SSID) as a legitimate wireless network. That might cause some users to connect to the rogue access point, which could capture their login credentials as the users attempt to log into the network. Such a rogue access point using the same SSID as a corporate wireless network is called an "evil twin."

Video Reference: Other Common Attacks

5. Which component of the CIA Triad does hashing primarily contribute?

    a. While hashing does add a layer of security, it does not directly impact any of the three components of the CIA Triad.
    b. Confidentiality
    c. Integrity
    d. Availability

Answer: c

Explanation: Hashing does not encrypt data, but rather runs the data through an algorithm to create a "hash digest." This hash digest can be thought of much like a fingerprint of the data.

If two parties independently run the same hashing algorithm on a data string and produce the same hash digest, that gives them some assurance the data did not get modified in transit. This helps ensure the integrity of the data, rather than ensuring the confidentiality or availability of the data.

Video Reference: 3 Goals of Network Security

6. Which security appliance can monitor traffic in-line and compare that traffic to a database of well-known attack signatures?

    a. IDS sensor
    b. Firewall
    c. IPS sensor
    d. ISE

Answer: c

Explanation: A firewall has a set of rules specifying what traffic is allowed in and out of specific firewall interfaces.

Cisco Identity Services Engine (ISE) can be used to define policies for user access to a network, based on the user's identity, regardless of their physical location.

An Intrusion Detection System (IDS) sensor receives a copy of traffic coming into a network and can react if that traffic is deemed to be potentially harmful. A reaction might be for the IDS sensor to instruct a firewall to create a rule blocking traffic from the offending IP address.

An Intrusion Prevention System (IPS) sensor sits in-line with traffic entering a network and can compare that traffic against a database of well-known attack signatures. If traffic is thought to be malicious, the IPS sensor can instantly drop the traffic, before it reaches its target.

Video Reference: Security Appliances

7. Which of the following encryption standards is used for asymmetric encryption?

    a. 3DES
    b. RSA
    c. DES
    d. AES

    Answer: b

    Explanation: Symmetric encryption standards, such as DES, 3DES, and AES use shared keys, where each party in the encrypted conversation has identical key strings used for encrypting and decrypting data.

    However, asymmetric encryption, such as the encryption used by RSA, can use a public/private key pair. Data encrypted with a device's public key can only be decrypted by that device's private key. Similarly, data encrypted with a device's private key can only be decrypted by that device's public key.

    Video Reference: Encryption

8. You are considering which type of AAA server to install. Which of the following is a characteristic of a TACACS+ server but not a characteristic of a RADIUS server?

    a. industry-standard
    b. uses TCP instead of UDP
    c. performs a one-way challenge response
    d. encrypts the password but not the entire packet

    Answer: b

Explanation: While RADIUS is a standard, TACACS+ is Cisco-proprietary. Also, TACACS+ uses TCP for communication, while RADIUS uses UDP.

TACACS+ separates the AAA (Authentication, Authorization, and Accounting) functions, while RADIUS combines them. Additionally, TACACS+ performs a two-way challenge response, where both parties authenticate one another, while RADIUS only performs a one-way challenge response, where a server authenticates a client, but the client does not authenticate the server.

Finally, TACACS+ encrypts entire packets, while RADIUS only encrypts passwords.

Video Reference: Securing User Accounts

9. When logging into your bank account, you enter your username and password. However, instead of being immediately logged in, you're instructed to enter a code that was texted to your smartphone. Only after entering that code are you successfully logged into your bank account. What type of authentication have you just performed?

    a. Single Sign-On
    b. Kerberos
    c. IEEE 802.1X
    d. MFA

Answer: d

Explanation: Multi-Factor Authentication (MFA) adds a layer of security to logins by requiring a two or more authentication requirements to be met. These requirements are called "factors" and can include things such as: something a user knows (e.g., a password), something a user has (e.g., a smartphone), something a user is (e.g., fingerprint scanner), where a user is (i.e., geofencing), or what a user does (e.g., drawing a pattern on a smart device).

Video Reference: Multi-Factor Authentication

10. What was the first wireless security standard to require support for the AES (Advanced Encryption Standard) algorithm?

    a. WEP
    b. WPA
    c. WPA2
    d. WPA3

Answer: c

Explanation: The Wired Equivalent Privacy (WEP) standard used RC4 (with a 24-bit initialization vector) for encryption.

Wi-Fi Protected Access (WPA) used TKIP for encryption, which was also based on RC4, but used a 48-bit initialization vector.

WPA2 supported TKIP, for backwards compatibility, but required that AES (Advanced Encryption Standard) encryption be supported.

While WPA3 also requires support for AES, it was released years after the release of WPA2.

Video Reference: Wireless Security Options

11. You're setting up a wireless router for use within your company. On that wireless router, you configure a wireless network that you don't want advertised to visitors. What feature will you select while configuring your wireless router to suppress the advertisement of this wireless network name?

    a. No WPS
    b. Hide SSID
    c. OFDMA
    d. TWT

Answer: b

Explanation: WPS (Wi-Fi Protected Setup) simplifies the process of connecting a device to a wireless network. Specifically, you can press the WPS button on the back of a wireless router and then select the WPS option on the device you wish to connect to the network. If your wireless router has a "No WPS" configuration option, that option disables the WPS feature.

A wireless network name is also known as an SSID (Service Set Identifier). If you don't want a wireless network name broadcast to all wireless devices, you can select the "Hide SSID" option.

OFDMA (Orthogonal Frequency-Division Multiple Access) and TWT (Target Wake Time) can be used on Wi-Fi 6 networks to allow wireless clients to communicate at nearly the same time.

Video Reference: Securing a Home Wireless Router