**Questions/Answers with explanation**

Author: Yassine Yazidi

CEH

01/2023

Volume 1 Assessment Test

# Disclaimer:

This is a personnel work it may be prone to errors so, if there are any issues, or suggestions feel free to address it in the issue section in Github so we can rectify it.

Assessment Test

**1.** Which header field is used to reassemble fragmented IP packets?

**A.** Destination address

**B.** IP identification

**C.** Don’t fragment bit

**D.** ToS field

B. IP identification

Explanation

The IP Identification header field is used to reassemble fragmented IP packets. When an IP packet is too large to be transmitted in a single unit, it may be divided into smaller fragments and sent individually. The receiving host must reassemble these fragments into the original packet in order to process the data correctly.

The IP Identification field is used to help the receiving host determine which fragments belong to the same packet. The value of the IP Identification field is set by the sender and remains the same for all fragments of a single packet. The receiving host uses this field to match the fragments and reassemble them into the original packet.

The IP Identification field is also useful for troubleshooting, as it can help identify whether fragmentation is occurring and the cause of any issues related to fragmentation.

**2.** If you were to see the following in a packet capture, what would you expect was happening? **‘or 1=1;**

**A.** Cross-site scripting

**B.** Command injection

**C.** SQL injection

**D.** XML external entity injection

C. SQL injection

Explanation

The text ' or 1=1;' in a packet capture indicates that a SQL injection attack may be taking place. SQL injection is a type of security vulnerability that occurs when an attacker is able to inject malicious code into a database query. This allows the attacker to gain unauthorized access to sensitive information stored in the database or to execute malicious actions on the system.

In the text ' or 1=1;', the statement ' or 1=1' is a common technique used in SQL injection attacks to bypass login authentication and gain access to the database. The statement evaluates to true, which allows the attacker to gain access to the database. The semicolon at the end of the statement is used to separate the malicious code from any legitimate code that may be present.

SQL injection attacks are a serious security concern and can result in the theft or compromise of sensitive information. It is important to properly validate user input and sanitize any user-supplied data that is used in a database query to prevent SQL injection attacks.

**3.** What method might you use to successfully get malware onto a mobile device?

**A.** Through the Apple Store or Google Play Store

**B.** External storage on an Android

**C.** Third-party app store

**D.** Jailbreaking

C. Third-party app store

Explanation

Mobile malware can be successfully installed onto a device through the use of a third-party app store. Third-party app stores are alternative sources of mobile applications that are not officially approved by the device's operating system provider (such as Apple or Google). These app stores may have a lower level of security and quality control compared to official app stores, and as a result, may contain malware-infected apps that can harm the device.

For example, if an Android user downloads an app from a third-party app store, the app may contain malware that can steal personal information, send premium SMS messages, or display unwanted ads. In some cases, the malware can even gain control of the device and carry out malicious actions without the user's knowledge.

To protect their devices, users should only download apps from official app stores and be cautious when downloading apps from third-party sources. It is also important to regularly update the operating system and installed apps, as updates often include security patches that can prevent malware infections.

**4.** What protocol is used to take a destination IP address and get a packet to a destination on the local network?

**A.** DHCP

**B.** ARP

**C.** DNS

**D.** RARP

B. ARP (Address Resolution Protocol)

Explanation

ARP (Address Resolution Protocol) is a protocol used to map an IP address to a physical (MAC) address on a local network. The purpose of ARP is to translate a destination IP address to the corresponding MAC address of the destination device on the same network.

When a device on a network wants to send a packet to another device, it first checks its ARP cache to see if it has a mapping for the destination IP address. If there is no mapping, the device will broadcast an ARP request to all devices on the network asking for the MAC address of the device with the desired IP address. The device with the matching IP address will respond with its MAC address, which will be used as the destination address for the packet.

ARP is essential for the functioning of local networks, as it allows devices to communicate with each other by mapping IP addresses to physical addresses. Without ARP, each device would need to know the MAC address of every other device on the network, which would be difficult to maintain in larger networks.

**5.** What would be the result of sending the string ‘AAAAAAAAAAAAAAAAA’ into a variable

that has been allocated space for 8 bytes?

**A.** Heap spraying

**B.** SQL injection

**C.** Buffer overflow

**D.** Slowloris attack

C. Buffer overflow

Explanation

A buffer overflow is a type of security vulnerability that occurs when more data is written to a buffer (a region of memory) than the buffer is capable of holding. This extra data can overwrite adjacent memory locations, potentially altering the values stored in those locations or even executing malicious code that has been written into the buffer.

In the example of sending the string "AAAAAAAAAAAAAAAA" into a variable that has been allocated space for 8 bytes, the extra 8 bytes of data would overflow the buffer and overwrite adjacent memory locations. This could cause unpredictable behavior in the program, such as crashes, errors, or even the execution of malicious code.

Buffer overflows are often caused by insufficient bounds checking in code that handles user-supplied data. To prevent buffer overflows, it is important to validate user input and ensure that buffers are allocated a size that is sufficient to hold the maximum amount of data that they are expected to receive. This can be done by using secure programming techniques, such as bounds checking and input validation, or by using libraries or tools that automatically enforce these security measures.

**6.** If you were to see the subnet mask 255.255.248.0, what CIDR notation (prefix) would you use to indicate the same thing?

**A.** /23

**B.** /22

**C.** /21

**D.** /20

C. /21

Explanation

The CIDR notation (prefix) represents the number of bits used for the network portion of an IP address. The subnet mask 255.255.248.0 is a way of representing the same information in dotted decimal notation.

To convert from subnet mask to CIDR notation, count the number of contiguous 1's in the subnet mask, starting from the leftmost position. In this case, the subnet mask 255.255.248.0 has 21 contiguous 1's. Thus, the CIDR notation for this subnet mask is /21.

**7.** What is the primary difference between a worm and a virus?

**A.** A worm uses polymorphic code

**B.** A virus uses polymorphic code

**C.** A worm can self-propagate

**D.** A virus can self-propagate

C. A worm can self-propagate.

Explanation

Worms are self-replicating malware that can spread across networks without user interaction. They can exploit vulnerabilities in operating systems, software, and network configurations to propagate. Unlike viruses, worms do not need to attach themselves to a host program and can operate independently.

A virus, on the other hand, is a type of malicious software that requires human intervention to spread. It attaches itself to a legitimate program or file and infects the host when executed. Unlike worms, viruses cannot self-propagate and depend on users to spread the infection.

**8.** How would you calculate risk?

**A.** Probability \* loss

**B.** Probability \* mitigation factor

**C.** (Loss + mitigation factor) \* (loss/probability)

**D.** Probability \* mitigation factor

A. Probability \* loss.

Explanation

Risk is often calculated as the product of probability and loss. This is a simplified way of expressing the likelihood of an adverse event occurring and the potential impact it may have. The formula represents the expected loss or harm that can be expected to result from the risk event. The higher the probability and the greater the potential loss, the higher the risk. This approach allows organizations to prioritize and manage risks by focusing on those that have the greatest potential impact.

**9.** How does an evil twin attack work?

**A.** Phishing users for credentials

**B.** Spoofing an SSID

**C.** Changing an SSID

**D.** Injecting four-way handshakes

B. Spoofing an SSID.

Explanation

An evil twin attack is a type of wireless eavesdropping attack where an attacker creates a fake wireless access point (AP) with a similar name (SSID) to a legitimate one, in an attempt to trick users into connecting to it. The attacker then monitors and captures all the data transmitted by the unsuspecting users, including sensitive information such as passwords, credit card numbers, and other confidential data.

In this attack, the fake AP functions as the "evil twin" of the real AP, essentially mimicking its behavior and appearing as a legitimate network to users. When users connect to the evil twin, they may be unaware that their data is being intercepted and transmitted to the attacker.

Evil twin attacks are a serious threat to wireless networks and users, as they can be difficult to detect and prevent. It's important to be vigilant and follow best practices to secure your wireless networks and protect against evil twin attacks.

**10.** In order to remove malware in the network before it gets to the endpoint, you would use which of the following?

**A.** Antivirus

**B.** Application layer gateway

**C.** Unified threat management appliance

**D.** Stateful firewall

C. Unified threat management appliance.

Explanation

A unified threat management (UTM) appliance is a hardware or software device that integrates multiple security functions into one single solution. This appliance can provide multiple layers of security, such as firewall, antivirus, intrusion detection and prevention, VPN, and web filtering, to protect the network from threats.

By deploying a UTM appliance at the network perimeter, an organization can prevent malware from reaching endpoints and causing damage. The UTM appliance can inspect incoming traffic, block malicious traffic, and alert administrators to potential threats. This can help organizations to stop malware outbreaks before they spread and reduce the overall risk to the network.

UTM appliances are often used as an efficient and cost-effective way to secure a network, especially for small and medium-sized businesses that may not have the resources or expertise to implement multiple separate security solutions.

**11.** What is the purpose of a security policy?

**A.** Providing high-level guidance on the role of security

**B.** Providing specific direction to security workers

**C.** Increasing the bottom line of a company

**D.** Aligning standards and practices

D. Aligning standards and practices.

Explanation

A security policy is a formalized written document that outlines an organization's approach to security. Its primary purpose is to align standards, procedures, and practices in order to ensure the confidentiality, integrity, and availability of information assets. The security policy sets the overall tone and direction for an organization's security efforts, serving as a reference point for all stakeholders.

The security policy provides a framework for making security-related decisions and reduces the risk of security incidents. It defines acceptable use of resources and outlines the responsibilities and accountabilities of employees, contractors, and third-party vendors. The security policy also helps to ensure that all security-related activities are consistent with the organization's goals and objectives.

Having a clear and comprehensive security policy is critical for an organization, as it helps to create a culture of security, facilitates effective risk management, and provides a basis for making informed decisions about security-related investments.