**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.

**12.** What has been done to the following string? %3Cscript%3Ealert(‘wubble’);%3C/

script%3E

**A.** Base64 encoding

**B.** URL encoding

**C.** Encryption

**D.** Cryptographic hashing

B. URL encoding

Explanation

The string has undergone URL encoding, which is a process of converting special characters into a format that can be transmitted over the internet. The characters are replaced with a % symbol followed by a two-digit hexadecimal representation of the character. For example, the less-than symbol (<) is encoded as %3C and the greater-than symbol (>) is encoded as %3E. In this case, the string contains a JavaScript script within HTML script tags, which is a security risk if executed in a web browser, hence the encoding.

**13.** What would you get from running the command dig ns domain.com?

**A.** Mail exchanger records for domain.com

**B.** Name server records for domain.com

**C.** Caching name server for domain.com

**D.** IP address for the hostname ns

B. Name server records for domain.com

Explanation

The **dig** command is used to query the Domain Name System (DNS) and retrieve information about various types of records. When you run the command **dig ns domain.com**, you are asking for the name server (NS) records for the domain **domain.com**. The output of the command will include the names and IP addresses of the servers that are responsible for resolving hostnames to IP addresses for the specified domain. This information is important for routing traffic to the correct server and is used by other systems to find the authoritative DNS server for a particular domain.

**14.** What technique would you ideally use to get all of the hostnames associated with a domain?

**A.** DNS query

**B.** Zone copy

**C.** Zone transfer

**D.** Recursive request

C. Zone transfer

Explanation

A zone transfer, also known as a full transfer, is a method to replicate the DNS database of a domain from one server to another. In this context, "zone" refers to a portion of the DNS namespace that is managed by a single administrative entity. A zone transfer allows you to retrieve all of the hostnames associated with a domain by copying the entire zone file from the authoritative DNS server for the domain. This is the ideal technique for getting all of the hostnames for a domain because the zone file contains all of the information about the domain, including the A records that map hostnames to IP addresses. Other techniques, such as DNS queries or recursive requests, can only retrieve information about specific hostnames and may not provide a complete list of all hostnames for a domain.

**15.** If you were to notice operating system commands inside a DNS request while looking at a

packet capture, what might you be looking at?

**A.** Tunneling attack

**B.** DNS amplification

**C.** DNS recursion

**D.** XML entity injection

A. Tunneling attack

Explanation

If you observe operating system commands inside a DNS request in a packet capture, you might be witnessing a tunneling attack. Tunneling refers to the practice of encapsulating one protocol inside another protocol in order to bypass network security restrictions or hide the underlying data. In a DNS tunneling attack, malicious actors encode operating system commands and data into DNS requests and responses. The attacker then uses the DNS infrastructure to exfiltrate data or control a remote system without being detected by network security systems. DNS tunneling is a stealthy and difficult-to-detect technique that can be used to carry out various types of attacks, such as data theft, command and control of malware, and lateral movement within a network. It is important to monitor network traffic and detect unusual DNS activity in order to protect against DNS tunneling attacks.

**16.** What would be the purpose of running a ping sweep?

**A.** You want to identify responsive hosts without a port scan.

**B.** You want to use something that is light on network traffic.

**C.** You want to use a protocol that may be allowed through the firewall.

**D.** All of the above.

A. You want to identify responsive hosts without a port scan.

Explanation

A ping sweep, also known as a ping scan, is a network reconnaissance technique used to identify hosts that are alive and connected to a network. The purpose of running a ping sweep is to find responsive hosts without conducting a full port scan, which can be time-consuming and generate a significant amount of network traffic.

A ping sweep works by sending a series of Internet Control Message Protocol (ICMP) echo requests, also known as pings, to a range of IP addresses on a network. Responsive hosts will send back an ICMP echo reply, allowing the scanner to determine which hosts are alive and available.

Ping sweeps can be useful for network administrators who need to quickly identify the hosts on their network or for security professionals who are conducting an initial assessment of a network. The technique is often used in combination with other tools and techniques to gather information about a network and its hosts.

Note: Due to the nature of ping scans, they may not always be accurate, as some systems may be configured to ignore ICMP traffic, or firewalls may block it.

**17.** How many functions are specified by NIST’s cybersecurity framework?

**A.** 0

**B.** 3

**C.** 5

**D.** 4

C. 5

Explanation

The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) is a set of guidelines and best practices for reducing cybersecurity risk to critical infrastructure in the United States. The NIST CSF specifies 5 functions for achieving this goal:

1. Identify: Developing an understanding of the organization's risk environment and the assets that need to be protected.
2. Protect: Implementing appropriate safeguards to ensure the confidentiality, integrity, and availability of critical assets and information.
3. Detect: Developing and implementing the capability to detect cyber security events and incidents.
4. Respond: Developing and implementing the capability to respond to detected cyber security events and incidents.
5. Recover: Developing and implementing the capability to restore normal system operations as quickly as possible following a cyber security event or incident.

These 5 functions provide a comprehensive and flexible approach to managing cybersecurity risk and are intended to be used as a guide for organizations of all sizes and types, from small businesses to large corporations and government agencies. The NIST CSF provides a common language for communication about cybersecurity risk and can help organizations prioritize and coordinate their cybersecurity efforts.

**18.** What would be one reason not to write malware in Python?

**A.** Python interpreter is slow.

**B.** Python interpreter may not be available.

**C.** There is inadequate library support.

**D.** Python is a hard language to learn.

B. Python interpreter may not be available.

Explanation

Writing malware in Python can be a practical choice for a number of reasons, including its ease of use, large library support, and readability. However, there is also a potential drawback that needs to be considered, which is the availability of the Python interpreter.

Malware is often designed to be executed on a target system without the user's knowledge, and in many cases, the target system may not have the Python interpreter installed. In such cases, the malware will not be able to run, rendering it useless.

For this reason, when writing malware, it is important to consider the environment in which it will be executed and choose a programming language that is commonly available in that environment. For example, malware written in C or Assembly language is more likely to run on a wider range of systems, as these languages are lower-level and can run directly on the underlying hardware without the need for an interpreter.

In conclusion, the availability of the Python interpreter is one reason that malware authors may choose to use a different programming language for their malicious code.

**19.** If you saw the following command line, what would you be capturing?

tcpdump -i eth2 host 192.168.10.5

**A.** Traffic just from 192.168.10.5

**B.** Traffic to and from 192.168.10.5

**C.** Traffic just to 192.168.10.5

**D.** All traffic other than from 192.168.86.5

B. Traffic to and from 192.168.10.5

Explanation

The command **tcpdump -i eth2 host 192.168.10.5** is used to capture network traffic on the network interface **eth2** for the host with IP address **192.168.10.5**.

The option **-i eth2** specifies the network interface to listen on. The **host 192.168.10.5** filter expression captures traffic to and from the specified host IP address.

In other words, **tcpdump -i eth2 host 192.168.10.5** captures both incoming and outgoing network traffic between the specified host and any other device on the network, including all IP protocols, such as TCP, UDP, and ICMP.

It should be noted that this capture only includes traffic that is transmitted or received on the specified network interface, and will not capture traffic on other network interfaces or any other network segments.

**20.** What is Diffie-Hellman used for?

**A.** Key management

**B.** Key isolation

**C.** Key exchange

**D.** Key revocation

C. Key exchange

Explanation

Diffie-Hellman is a cryptographic algorithm used for secure communication over the internet. It enables two parties to establish a shared secret key over an insecure communication channel, without any prior shared information. The key exchange is done through public key cryptography, where each party publicly agrees on a large prime number and a generator, then calculates a public value. The shared secret key is derived from these public values and can be used for encryption and decryption of messages.

**21.** Which social engineering principle may allow a phony call from the help desk to be effective?

**A.** Social proof

**B.** Imitation

**C.** Scarcity

**D.** Authority

D. Authority

Explanation

The principle of Authority refers to a person's tendency to trust and comply with those who hold a position of power or authority, such as a help desk representative or someone claiming to be from a company's technical support team. By exploiting this principle, a malicious actor can trick victims into divulging sensitive information or performing actions that compromise their security.

**22.** How do you authenticate with SNMPv1?

**A.** Username/password

**B.** Hash

**C.** Public string

**D.** Community string

D. Community string

Explanation

SNMPv1 uses a simple authentication mechanism known as the Community String. The community string acts as a shared password between the SNMP agent (a device that provides information) and the SNMP manager (a device that collects and monitors information). The community string is transmitted in cleartext and does not provide any confidentiality or encryption for the data being transmitted. This makes SNMPv1 vulnerable to eavesdropping and tampering, and it is recommended to use a more secure version of SNMP, such as SNMPv3, which provides better security features such as authentication and encryption.

**23.** What is the process Java programs identify themselves to if they are sharing procedures over the network?

**A.** RMI registry

**B.** RMI mapper

**C.** RMI database

**D.** RMI process

A. RMI registry

Explanation

In Java, the Remote Method Invocation (RMI) registry is a registry service that allows Java programs to identify and locate remote objects that are available for communication over the network. The RMI registry acts as a lookup service for RMI clients, allowing them to discover the remote objects that are available and obtain a reference to the remote object's stub (a local representation of the remote object).

When a Java program wants to share its procedures over the network, it must first register the remote object with the RMI registry. This involves creating an instance of the remote object and binding it to a unique name in the registry. The RMI client can then look up the remote object by its name and obtain a reference to its stub, which it can use to invoke methods on the remote object as if it were local.

The RMI registry provides a central point of control for the distribution of remote objects, allowing RMI clients to dynamically discover and access remote objects without the need for manual configuration or pre-existing knowledge of the objects' locations.

**24.** What do we call an ARP response without a corresponding ARP request?

**A.** Is-at response

**B.** Who-has ARP

**C.** Gratuitous ARP

**D.** IP response

C. Gratuitous ARP

Explanation

A gratuitous ARP is an ARP response that is broadcast without a corresponding ARP request. It is used to update the ARP caches of other devices on a network in response to a change in the mapping of an IP address to a physical address.

For example, if a device's IP address changes or if it comes online for the first time, it may send a gratuitous ARP to update the ARP caches of other devices on the network with its new IP-to-physical address mapping. This ensures that other devices on the network are aware of the device's current address and can communicate with it directly, rather than sending packets through a default gateway or sending ARP requests to resolve the device's address.

Gratuitous ARPs are typically used to detect and resolve ARP cache conflicts, to detect duplicates of the same IP address on a network, and to update ARP caches in response to network changes. They can also be used maliciously to conduct ARP cache poisoning attacks.

**25.** What are the three times that are typically stored as part of file metadata?

**A.** Moves, adds, changes

**B.** Modified, accessed, deleted

**C.** Moved, accessed, changed

**D.** Modified, accessed, created

D. Modified, accessed, created

Explanation

File metadata is information that is stored about a file in addition to its content. This metadata can include various properties of the file, such as its size, type, and location.

The three times that are typically stored as part of file metadata are:

1. Modified: the time when the file's content was last changed.
2. Accessed: the time when the file was last read or opened.
3. Created: the time when the file was first created.

This information can be useful for various purposes, such as tracking the history of a file's changes, determining when a file was last used, and searching for files based on their creation or modification date. The exact information that is stored as part of file metadata depends on the file system and operating system being used, but modified, accessed, and created times are common among many file systems.