Eccouncil

(ICS-SCADA)

ICS-SCADA Cyber Security

Total: **75 Questions**

Link:

MYEXAM.FR

The correct answer is C, Confidentiality. The Authentication Header (AH) is a security protocol within the IPsec suite that provides data integrity, authentication, and anti-replay protection for IP packets. Its primary goal is to ensure that the data received is the same as the data sent and that the sender is who they claim to be.

Specifically, AH protects against replay attacks using a sequence number field. This sequence number prevents attackers from capturing and retransmitting packets. Authentication is achieved through cryptographic hashing of the packet's data and header fields, ensuring the packet's origin is verifiable. Data integrity is also enforced through these cryptographic hashes, validating that the packet hasn't been tampered with in transit.

However, AH does not provide confidentiality or encryption. It does not encrypt the data payload, meaning the contents of the packet are still visible to anyone who intercepts it. Its focus is solely on authentication and integrity. If confidentiality is required, the Encapsulating Security Payload (ESP) protocol is used, often in conjunction with AH. ESP encrypts the data and also offers integrity and authentication features.

Therefore, confidentiality is the component that is not part of the Authentication Header (AH).

Supporting Resources:

RFC 4302 - IP Authentication Header: https://datatracker.ietf.org/doc/html/rfc4302 - Provides the technical specification for the Authentication Header.
IPsec - Wikipedia: https://en.wikipedia.org/wiki/IPsec - Provides a general overview of the IPsec protocol suite and its components.

Question: 4

How many main score areas are there in the CVSS?

A. 2
B. 4
C. 3
D. None of these

Answer: C

Explanation:

The correct answer is C. 3 because the Common Vulnerability Scoring System (CVSS) comprises three main score areas: Base, Temporal, and Environmental.

The Base score represents the intrinsic characteristics of a vulnerability that are constant over time and across user environments. It reflects the severity of the vulnerability itself, considering factors such as attack vector, attack complexity, privileges required, user interaction, scope, confidentiality impact, integrity impact, and availability impact.

The Temporal score represents the characteristics of a vulnerability that change over time but not across user environments. These factors include exploitability, remediation level, and report confidence. This score adjusts the Base score based on the current state of exploit techniques and availability of patches or workarounds.

The Environmental score represents the characteristics of a vulnerability that are specific to a user's environment. It allows organizations to customize the CVSS score based on the importance of the affected IT

A. Echo request
B. Echo start
C. Echo recall
D. Echo reply

Answer: A

Explanation:

The correct answer is A, Echo request, because ICMP (Internet Control Message Protocol) type 8 packets are specifically designated for initiating a ping operation. A "ping" is a fundamental network diagnostic tool used to test the reachability of a host on an IP network. The process involves sending an ICMP Echo request to the target host and waiting for an ICMP Echo reply. The originating host sends an ICMP type 8 packet (Echo request), and if the target is reachable and configured to respond, it replies with an ICMP type 0 packet (Echo reply).

ICMP itself is crucial for network diagnostics and control, operating at the network layer (Layer 3) of the OSI model. In cloud environments, ICMP is vital for troubleshooting connectivity issues within virtual networks and between cloud resources and external networks. For example, you might use ping from a virtual machine in AWS to check its connectivity to another EC2 instance or to the internet. Properly configured firewalls or security groups are imperative, and will often allow ICMP packets necessary for network troubleshooting, but may restrict them to prevent certain attacks.

The Echo request/reply mechanism allows network administrators to verify that a device is online and responsive. The round-trip time (RTT) calculated from sending the Echo request and receiving the Echo reply gives an indication of the network latency.

The other options are incorrect. There is no "Echo start" or "Echo recall" ICMP type. While an "Echo reply" (ICMP type 0) is related, it represents the response to the Echo request, not the initial request itself. In ICS-SCADA (Industrial Control Systems - Supervisory Control and Data Acquisition) environments, understanding network protocols like ICMP is critical for security professionals to monitor network traffic, identify anomalies, and ensure the availability and reliability of critical infrastructure systems. Malicious actors may exploit ICMP for reconnaissance or denial-of-service attacks, making it essential to properly monitor and filter ICMP traffic within ICS networks.

Authoritative links for further research:

1. **RFC 792 - Internet Control Message Protocol:** https://datatracker.ietf.org/doc/html/rfc792
2. **ICMP Types:** https://www.iana.org/assignments/icmp-parameters/icmp-parameters.xhtml

Question: 7

What step of the malware infection installs the malware on the target?

A. Drive-by
B. Init
C. Dropper
D. Stager

Answer: C

question. These RIRs are crucial for the proper functioning of the internet, as they maintain databases linking domain names with their respective owners. These databases are queried during processes like WHOIS lookups, which reveal registration information. Knowing which RIR is responsible for which region is fundamental in understanding internet governance and cybersecurity investigations. If you want to find out who owns a domain registered in Europe, you need to check the RIPENCC database. For instance, understanding RIR responsibilities is essential when investigating the source of malicious activity originating from a specific region, allowing cybersecurity professionals to trace the origin effectively.

Here are some authoritative links for further research:

RIPE NCC: https://www.ripe.net/
AFRINIC: https://www.afrinic.net/
LACNIC: https://www.lacnic.net/
ARIN: https://www.arin.net/

These links provide detailed information about each RIR's responsibilities, services, and geographical coverage.

Question: 10

Which component of the IT Security Model is attacked with interruption?

A. Confidentiality
B. Availability
C. Authentication
D. Integrity

Answer: B

Explanation:

The correct answer is Availability. Interruption, in the context of the IT Security Model, specifically targets the accessibility and operational readiness of systems and data. An interruption attack aims to make a resource unavailable or unusable, thus directly impacting availability. This differs from attacks on confidentiality, which aim to expose sensitive information, or attacks on integrity, which aim to corrupt or alter data. Authentication, which verifies the identity of users or systems, is also not the primary target of interruption.

Consider a Denial-of-Service (DoS) attack on an ICS-SCADA system. The goal isn't to steal confidential process data (confidentiality), alter setpoints (integrity), or spoof a legitimate operator (authentication). Instead, the attacker floods the control network with traffic, overwhelming the communication channels and preventing authorized operators from accessing critical control interfaces or receiving sensor data. This directly halts or hinders the operation of the ICS-SCADA system, rendering it unavailable.

Another example is ransomware targeting an ICS server. While data might eventually be corrupted (integrity impact as a secondary effect), the immediate impact is the inaccessibility of the server and its services, severely impacting availability. The primary aim is to disrupt operations until a ransom is paid. Therefore, an interruption attack's core purpose is to deny access to services or resources, which aligns directly with the concept of availability in the IT Security Model.

In ICS-SCADA, any attack that prevents operators from monitoring processes, issuing commands, or receiving alerts is an interruption attack. These attacks can have severe consequences, including process shutdowns, equipment damage, and even safety hazards. Safeguarding the availability of ICS-SCADA systems is

OSINT involves gathering information from publicly available sources. In the context of ICS/SCADA systems, this means actively searching the internet for details about the target infrastructure. Unlike the other options, OSINT is specifically designed to collect publicly accessible information, which often reveals crucial details.

Enumeration focuses on directly querying a system to glean information about its resources, such as user accounts and shares. It is an active process that interacts directly with the target, and thus may trigger alarms in a production ICS/SCADA environment.

Scanning is a technical process used to identify active hosts, services, and open ports on a network. While scanning can reveal operating systems and some applications, it's not as effective for vendor identification as OSINT and carries a higher risk of detection.

Surveillance involves observing the target environment. While direct observation could reveal some information, it's much less efficient than OSINT when trying to identify specific software or hardware vendors.

OSINT techniques, such as searching vendor websites, public databases (like Shodan), industry forums, news articles, and social media, can provide significant insights into the specific applications and vendors used in an ICS/SCADA environment. This information helps attackers build a profile of the target infrastructure without directly interacting with it, making it a lower-risk reconnaissance method. Manufacturers often publicly list their ICS/SCADA products, security advisories, and software versions.

For example, searching for the name of a utility company's control center and combining it with terms like "SCADA" or "ICS" might lead to press releases, project announcements, or conference presentations that mention the specific vendor providing the control system software. Similarly, public databases such as Shodan contain information about connected devices, sometimes revealing the vendor and model of ICS/SCADA components. Security advisories published by vendors themselves often disclose product names and versions.

Therefore, OSINT is the most effective and lowest-risk method for identifying the applications and vendors used in an ICS/SCADA environment, by leveraging publicly available data to create a comprehensive understanding of the target.

Authoritative links for further research:

SANS Institute - Introduction to OSINT: https://www.sans.org/reading-room/whitepapers/intelligence/introduction-open-source-intelligence-osint-33801
NIST Special Publication 800-82 - Guide to Industrial Control Systems (ICS) Security: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-82r2.pdf (While it doesn't focus solely on OSINT, it provides excellent context for ICS/SCADA security principles).

Question: 14

Which of the following is a component of an IDS?

A. All of these
B. Respond
C. Detect
D. Monitor

Answer: A

Explanation:

than was the case. The core impact was on the PLC software and their operating parameters, ultimately causing equipment failure within the larger system they controlled. The other named options are less specific regarding the general class of device targeted by the attack.

Further information:

Symantec's Analysis: https://www.symantec.com/connect/blogs/w32stuxnet-dossier
Wired Article: https://www.wired.com/2011/03/ff_stuxnet/
Wikipedia: https://en.wikipedia.org/wiki/Stuxnet

Question: 17

What is the size in bytes of the TCP sequence number in the header?

A. 2
B. 1
C. 3
D. 4

Answer: D

Explanation:

The correct answer, D (4), is justified by the structure of the TCP header. The TCP header contains essential information for reliable data transfer over an IP network, and a crucial part of this is the sequence number. This sequence number is a 32-bit field. Since each byte is composed of 8 bits, a 32-bit field requires 4 bytes of storage (32 bits / 8 bits/byte = 4 bytes).

The sequence number plays a vital role in TCP's reliability mechanisms. It identifies the order of data segments sent from the source to the destination. This allows the receiver to reassemble the data correctly, even if packets arrive out of order. Without a sufficient size for the sequence number, large data transfers could experience "sequence number wrap-around" issues, where the same sequence number is used multiple times, leading to confusion and data corruption. A 32-bit sequence number provides a large address space, mitigating the risk of these wrap-around issues, particularly crucial in high-bandwidth networks. The larger the number of possible sequence numbers, the longer it takes for a sequence number to repeat.

The TCP header also uses an acknowledgement number, which is also 32-bits and thus 4 bytes. This is used by the receiver to acknowledge the receipt of packets based on their sequence numbers. The correct sequence number size guarantees reliable in-order delivery, which is necessary for applications like web browsing, email, and file transfer.

The importance of the 32-bit sequence number is standardized across the internet. Any alteration of this size would break compatibility. These network protocol details remain consistent in cloud computing environments as well because applications residing on cloud infrastructure rely on these same protocols to communicate.

Further research:

RFC 793 (Transmission Control Protocol): https://datatracker.ietf.org/doc/html/rfc793 - This is the foundational document that defines the TCP protocol. Section 3.1 describes the TCP Header format, clearly showing the 32-bit sequence number field.
TCP Header Fields: https://www.geeksforgeeks.org/tcp-header/ - A simplified explanation of all header fields.

Question: 19

Which of the following can be used to view entire copies of web sites?

A. Wayback machine
B. Google Cache
C. Netcraft
D. Bing offline

Answer: A

Explanation:

The Wayback Machine is the correct answer because it's explicitly designed to archive web pages and allow users to view historical versions of websites. It takes snapshots of websites at different points in time and stores them in its archive, effectively creating a "time machine" for the web.

Google Cache, while allowing you to view a cached version of a specific webpage, does not provide a comprehensive historical archive of the entire website's structure and content over time. It's typically used to access a webpage when the original server is unavailable or slow. The cached version is simply the most recent crawl Google's bot has made.

Netcraft provides information about websites, including hosting infrastructure, technologies used, and security certificates. While useful for analysis, it does not store complete historical copies of websites like the Wayback Machine. It's more about website profiling and internet security monitoring.

Bing offline doesn't exist as a dedicated service. While Bing's search engine crawls and indexes websites, it doesn't provide a separate feature for viewing offline or archived versions of entire websites in the same manner as the Wayback Machine. It leverages its index to provide search results, which might include cached versions of pages, but not comprehensive historical snapshots.

Therefore, the Wayback Machine stands out as the dedicated tool for accessing archived copies of websites as a whole, making it the most appropriate answer.

Further research:

Internet Archive's Wayback Machine: https://archive.org/web/

Question: 20

The NIST SP 800-53 defines how many management controls?

A. 6
B. 9
C. 5
D. 7

Answer: B

Explanation:

(ICS) security and data integrity).
OWASP (Open Web Application Security Project): https://owasp.org/ (While primarily web-focused, OWASP's resources on data validation and input sanitization are relevant to preventing modification attacks).

Question: 23

Which of the following is required to determine the correct Security Association?

A. SPI
B. Partner IP address
C. Protocol
D. All of these

Answer: D

Explanation:

The correct answer, D (All of these), is accurate because SPI (Security Parameters Index), Partner IP address, and Protocol are all crucial components in establishing and identifying a Security Association (SA) within security protocols like IPSec. An SA is a simplex (one-way) logical connection providing secure communication between two entities. To properly identify which SA to use for a particular packet, the receiving system needs to compare the SPI, the source (partner) IP address, and the protocol used (e.g., AH, ESP) against its stored SA database. The SPI is a unique identifier chosen by the receiving end of the SA, distinguishing one SA from potentially multiple SAs to the same destination. The partner IP address identifies the originator of the secured traffic. Finally, the protocol specifies the security mechanism applied (Authentication Header or Encapsulating Security Payload). Without all three pieces of information, the system cannot reliably determine which SA applies, potentially leading to security breaches or communication failures. Each element acts as a filter: first, the IP address narrows down the possible SAs, then the protocol further refines the selection, and finally, the SPI provides the specific SA key. Therefore, all three parameters are necessary for precise SA identification.

Here are some authoritative links for further research:

1. **RFC 2401 - Security Architecture for the Internet Protocol:** https://datatracker.ietf.org/doc/html/rfc2401 - This RFC describes the fundamental architecture of IPsec, including the Security Association.
2. **RFC 7296 - Internet Key Exchange Protocol Version 2 (IKEv2):** https://datatracker.ietf.org/doc/html/rfc7296 - IKEv2 is the protocol used to establish SAs in IPsec.
3. **Cisco - Understanding IPsec Security Associations:** https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/111533-ipsec-security-associations.html - Explains IPsec SAs in practical networking scenarios.