complete your programming course about resources, doubts and more!

Cisco

(200-201)

Understanding Cisco Cybersecurity Operations Fundamentals
(CBROPS)

Total: **325 Questions**
Link:

Question: 1

Which event is user interaction?

A. gaining root access
B. executing remote code
C. reading and writing file permission
D. opening a malicious file

Answer: D

Explanation:

The correct answer is **D. opening a malicious file**. User interaction, in the context of security events, refers to actions directly initiated by a human user. Let's analyze why other options are not primary user interactions.

Gaining root access (A) is a privilege escalation, often achieved through exploiting system vulnerabilities.

While a user may attempt this, the act of gaining root itself is typically a consequence of exploitation, not a direct user activity. Executing remote code (B) usually involves exploiting a system weakness to run malicious commands; again, a secondary effect rather than direct user input. Reading and writing file permissions (C) is an action concerning system access rights; while a user may request such changes, the action itself is a system operation. Opening a malicious file (D), however, is a direct and intentional action taken by the user. The user actively clicks, double-clicks, or otherwise initiates the process of opening the file. This makes it the most definitive example of user interaction from the options provided. It is the act of initiating the file execution that represents the user's direct involvement. A user might do this knowingly or unknowingly, but the crucial aspect is that the user is the driving force behind the initial event. This is different from the other options which are more likely consequences of vulnerabilities or other processes.

Supporting Concepts:

User Action: The concept of user interaction in security refers specifically to actions triggered directly by human users.

Attack Vectors: Options A, B, and C are often results of successful attacks exploiting system vulnerabilities rather than direct user interaction.

Human Element: Cybersecurity focuses significantly on the human element, and understanding how users interact with systems is vital for effective security.

Authoritative Links:

NIST Special Publication 800-63-3 Digital Identity Guidelines:https://pages.nist.gov/800-63-3/ (Covers digital identity and authentication, highlighting the role of user actions)
OWASP (Open Web Application Security Project):https://owasp.org/ (Provides information on common web application vulnerabilities, which often involve user interactions as part of the attack vector)

Question: 2

Which security principle requires more than one person is required to perform a critical task?

A. least privilege
B. need to know
C. separation of duties
D. due diligence

Answer: C

Explanation:

The correct answer is **C. separation of duties.** Separation of duties is a security principle that aims to prevent fraud and errors by dividing critical tasks among multiple individuals. This ensures that no single person has enough power or control to compromise a system or process. Requiring multiple people to perform a sensitive operation creates a system of checks and balances, making it more difficult for malicious actors to act unilaterally.

Let's examine why other options are incorrect:

A. Least privilege: This principle focuses on granting users only the minimum access rights necessary to perform their job functions, reducing the potential damage from compromised accounts. It doesn't directly address the need for multiple individuals to complete a single task.

B. Need to know: This principle restricts access to information only to those who require it for their roles. While important, it doesn't address the collaborative aspect of critical tasks.

D. Due diligence: Due diligence is a broad concept that involves the thorough investigation and reasonable care taken to avoid harm or loss. It is more of a process than a specific security principle related to multiple individuals involved in one task.

In summary, separation of duties is the principle specifically designed to address the risk of single points of failure by distributing responsibility, requiring collaboration to complete critical tasks. This strengthens security by making malicious actions more complex to execute.

Authoritative Links for further research:

NIST: https://csrc.nist.gov/glossary/term/separation_of_duties
ISACA: https://www.isaca.org/resources/isaca-journal/past-issues/2018/volume-2/separation-of-duties-the-crucial-control

Question: 3

How is attacking a vulnerability categorized?

A. action on objectives
B. delivery
C. exploitation
D. installation

Answer: C

Explanation:

The correct answer is **C. exploitation**. Exploitation, in the context of cybersecurity, refers to the act of taking advantage of a known vulnerability in a system or application. This is a critical phase in the cyber kill chain where attackers leverage flaws to gain unauthorized access, execute malicious code, or cause damage. Attacking a vulnerability directly corresponds to using that vulnerability's weakness to achieve a malicious goal, making it unequivocally an act of exploitation.

Option A, "action on objectives," comes later in the kill chain; it's what happens after the attacker has gained access. Option B, "delivery," refers to the method of getting malicious code or payloads into a system. Option D, "installation," is a subsequent stage where the malicious components are placed for continued access or execution. Thus, only option C accurately reflects the process of directly targeting and using a vulnerability. Exploitation is a core concept in cybersecurity, signifying the active breach phase. It involves techniques that use vulnerabilities, such as buffer overflows, SQL injection, or cross-site scripting, to achieve an attacker's goal.

For further research, refer to the following authoritative resources:

NIST (National Institute of Standards and Technology) Special Publication 800-16: https://csrc.nist.gov/publications/detail/sp/800-16/final (Specifically look into vulnerability management definitions.)
OWASP (Open Web Application Security Project):https://owasp.org/ (See their section on exploitation and attacks.)
SANS Institute:https://www.sans.org/ (Search for articles relating to vulnerability exploitation).

Question: 4

What is a benefit of agent-based protection when compared to agentless protection?

A. It lowers maintenance costs
B. It provides a centralized platform
C. It collects and detects all traffic locally
D. It manages numerous devices simultaneously

Answer: B

Explanation:

The correct answer is **B. It provides a centralized platform**. Agent-based protection often involves deploying software agents on each endpoint, providing granular visibility and control. These agents communicate with a central management platform, enabling administrators to monitor, configure, and respond to security events across the entire infrastructure from a single location. This centralized approach simplifies security management, improves threat detection capabilities, and ensures consistent policy enforcement. In contrast, agentless solutions typically rely on network monitoring or API interactions, which may lack the detailed endpoint context provided by agents and can be less effective at detecting certain types of threats. While agentless systems might reduce initial deployment and management overhead, they often sacrifice the deeper insights and real-time monitoring afforded by agents. The centralized platform benefit highlights the key advantage of agent-based systems in providing an integrated security management and monitoring experience. This advantage contributes to better security posture visibility and enables prompt incident response by providing a holistic view of security alerts across the entire environment.

Authoritative Link:

Gartner's Security Information and Event Management (SIEM) guide: While not directly about agent-based vs agentless, SIEM solutions often leverage agents for better endpoint data collection and analysis, showcasing the importance of centralized platforms for security management.

https://www.gartner.com/en/information-technology/glossary/security-information-and-event-management-siem

Question: 5

Which principle is being followed when an analyst gathers information relevant to a security incident to determine the appropriate course of action?

A. decision making
B. rapid response
C. data mining

D. due diligence

Answer: A

Explanation:

The correct answer is **A. decision making**. The scenario describes a security analyst gathering information to inform their actions in response to an incident. This directly relates to the principle of decision-making in cybersecurity. Decision-making involves evaluating available data, analyzing risks, and choosing the most appropriate course of action from a range of options. It is not simply about rapidly reacting (rapid response), nor is it solely about uncovering hidden patterns in large datasets (data mining). While due diligence is crucial, it is a broader concept encompassing preventative measures and adhering to established procedures, not the specific act of gathering information to inform an immediate response. In the given context, gathering information is the initial phase of the decision-making process where the analyst gathers details to help make the right call. The analyst uses the collected information to understand the incident fully and thereby enable the next phase: to make a decision. The most accurate representation is that they are in the decision-making process.https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-framework/identifyhttps://www.sans.org/reading-room/whitepapers/incident/incident-response-decision-making-37752

Question: 6

One of the objectives of information security is to protect the CIA of information and systems. What does CIA mean in this context?

A. confidentiality, identity, and authorization

B. confidentiality, integrity, and authorization

C. confidentiality, identity, and availability

D. confidentiality, integrity, and availability

Answer: D

Explanation:

The acronym "CIA," in the context of information security, stands for Confidentiality, Integrity, and Availability. These three principles form the cornerstone of information security and are often referred to as the CIA triad.

Confidentiality ensures that information is accessible only to authorized individuals and prevents unauthorized disclosure. This involves implementing access controls, encryption, and data masking techniques. For example, cloud providers employ access management tools to ensure only the authorized personnel can view sensitive customer data.

Integrity focuses on maintaining the accuracy and completeness of data. This means protecting data from unauthorized modification or deletion. Mechanisms like checksums, hash functions, and version control systems are used to ensure integrity. Cloud services might employ immutable storage to prevent accidental or malicious data changes.

Availability means that authorized users can access information and systems when they need it. This includes measures to prevent service disruptions, like redundancy, failover systems, and disaster recovery plans. In the cloud, techniques like load balancing and geographically dispersed infrastructure enhance the availability of services.

Option D, “confidentiality, integrity, and availability,” accurately reflects the CIA triad, making it the correct answer. Options A, B, and C incorrectly substitute “identity” or “authorization” for the crucial principle of“availability” or "integrity" respectively. These might be related concepts in security but do not form the CIA triad itself.

For further information, research the CIA triad concept. You can explore resources from organizations like NIST (National Institute of Standards and Technology) and SANS Institute:

NIST:https://csrc.nist.gov/glossary/term/cia_triad
SANS Institute:https://www.sans.org/information-security/glossary/cia-triad/These resources provide a deep dive into these fundamental security principles.

Question: 7

What is rule-based detection when compared to statistical detection?

A. proof of a user's identity
B. proof of a user's action
C. likelihood of user's action
D. falsification of a user's identity

Answer: B

Explanation:

The correct answer is **B. proof of a user's action.** Here's a breakdown of why, contrasting rule-based and statistical detection methods:

Rule-based detection relies on predefined rules or signatures. These rules explicitly define what constitutes a security event. For example, a rule might trigger an alert if a specific user attempts to log in from an unusual geographic location or if a particular port receives excessive traffic. The detection is based on a direct match to these predefined patterns or conditions. Therefore, a rule-based detection, when it flags something, provides evidence of that action, making it a "proof of a user's action."

Statistical detection, on the other hand, uses mathematical algorithms to establish normal behavior patterns. It then flags deviations from these established norms as anomalies that might signify a security threat. It doesn't focus on predefined actions but instead on the likelihood or probability of a user's action based on observed data trends. This makes it less about providing a definitive "proof of action" and more about identifying unusual behavior that suggests a potential issue. Thus, Statistical detection would align more with option C, the likelihood of user's action.

Option A, proof of a user’s identity, relates more to authentication processes. Option D, falsification of a user’s identity, deals with a subset of authentication where the identity is deemed not to be genuine, and are both outside the scope of a comparison between rule-based and statistical detection methods.

In summary: Rule-based detection is deterministic, providing concrete evidence of a specific action. Statistical detection is probabilistic, focusing on detecting unusual patterns that may indicate suspicious activity, and is not about providing direct proof.

Authoritative Links for Further Research:

1. **NIST (National Institute of Standards and Technology):** Special Publication 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS). This document explains detection methods. https://csrc.nist.gov/publications/detail/sp/800-94/final

2. **SANS Institute:** Provides detailed resources on cybersecurity including intrusion detection methods.

Explore their research and articles using search terms like "rule-based detection" or "statistical anomaly detection." https://www.sans.org/

Question: 8

A user received a malicious attachment but did not run it.
Which category classifies the intrusion?

A. weaponization
B. reconnaissance
C. installation
D. delivery

Answer: D

Explanation:

The correct answer is **D. delivery**. The scenario describes the stage where a malicious payload (the attachment) is transmitted to the target user. This aligns with the "delivery" phase in the Cyber Kill Chain or similar intrusion models, which focuses on the method used to transmit the malicious content to the victim.

Even though the attachment wasn't executed, the fact it reached the user signifies a successful delivery attempt. The attacker's intent to compromise the system is established by their action of sending the malicious attachment. The other phases do not apply here; 'weaponization' precedes delivery and involves creating the malicious payload; 'reconnaissance' involves gathering information about the target; and 'installation' refers to deploying the malware on the victim's system, which didn't happen here. In essence, delivery is all about getting the malicious payload to the target, and that's what is demonstrated in this question.

Supporting Links:

Cyber Kill Chain:https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html (This link provides information on the Cyber Kill Chain model, which includes the "delivery" phase.)
MITRE ATT&CK Framework:https://attack.mitre.org/ (While this framework doesn't have a strict "delivery" phase, it can help understand various attack techniques that fall within the context of delivery, like Phishing or Drive-by Compromise)

Question: 9

Which process is used when IPS events are removed to improve data integrity?

A. data availability
B. data normalization
C. data signature
D. data protection

Answer: B

Explanation:

The correct answer is **B. data normalization.** Data normalization is the process of structuring data to minimize redundancy and improve data integrity. In the context of Intrusion Prevention System (IPS) events, normalization involves standardizing the format and values of the collected data. This standardization can

include removing duplicate or irrelevant events, ensuring consistent naming conventions, and aligning data with specific schemas. By normalizing IPS event data, security analysts can more efficiently analyze and correlate security incidents, reducing noise and improving the overall quality of security information. While data protection aims to secure data against unauthorized access, and data availability ensures accessibility of data, they are not directly concerned with the specific process of cleaning and structuring data to improve its integrity. Data signature, while related to identifying known patterns, does not involve the specific
manipulation of data to improve its quality. Therefore, normalizing IPS events is the most accurate process for the described scenario.

Further reading on data normalization:

TechTarget - Data Normalization
Wikipedia - Data Normalization
Cisco documentation - Security Data Normalization

Question: 10

An analyst is investigating an incident in a SOC environment. Which method is used to identify a session from a group of logs?

A. sequence numbers
B. IP identifier
C. 5-tuple
D. timestamps

Answer: C

Explanation:

The correct answer is C, the 5-tuple. A 5-tuple is a fundamental concept in network traffic analysis and is crucial for identifying unique sessions within a stream of logs. It consists of the source IP address, the destination IP address, the source port, the destination port, and the protocol used (e.g., TCP or UDP). This combination of five elements uniquely defines a specific communication flow between two endpoints. When analyzing logs, the 5-tuple allows an analyst to trace the complete path of data exchanged during a particular communication event, thus enabling them to identify a specific session. Sequence numbers (A) are used to ensure data ordering within a specific TCP stream, not to identify entire sessions across logs. The IP identifier (B) is a field in the IP header used for fragment reassembly and isn't reliable for session tracking across different logs. While timestamps (D) help in ordering events, they don't uniquely define a session, as many different sessions can occur within the same time period. Using the 5-tuple is the most accurate method for linking related events, enabling analysts to reconstruct an entire communication session from the logs and gain a comprehensive understanding of an incident. The 5-tuple approach is widely used in network security monitoring and log analysis tools, highlighting its importance in incident response and cybersecurity investigations.

Further Research:

Cisco Documentation on Network Security:https://www.cisco.com/c/en/us/solutions/security.html (While not directly on 5-tuple, this provides context for Cisco security principles)
Wireshark User's Guide (explains 5-tuple in packet analysis):
https://www.wireshark.org/docs/wsug_html_chunked/ChAdvFiltering.html
SANS Institute: Understanding Network Traffic Analysis:https://www.sans.org/reading-room/whitepapers/detection/understanding-network-traffic-analysis-32758 (General resource discussing network analysis, includes 5-tuple importance)

Question: 11

What is a difference between SOAR and SIEM?

A. SOAR platforms are used for threat and vulnerability management, but SIEM applications are not

B. SIEM applications are used for threat and vulnerability management, but SOAR platforms are not

C. SOAR receives information from a single platform and delivers it to a SIEM

D. SIEM receives information from a single platform and delivers it to a SOAR

Answer: A

Explanation:

The correct answer is **A. SOAR platforms are used for threat and vulnerability management, but SIEM applications are not.**

Here's a detailed justification:

SIEM (Security Information and Event Management) primarily focuses on collecting, aggregating, and analyzing security logs and event data from various sources across an organization's IT infrastructure. It helps in detecting security incidents, generating alerts, and providing a centralized view of security events. SIEMs excel at correlation and analysis of vast amounts of security-related data, but typically don't directly handle remediation actions or vulnerability management.

SOAR (Security Orchestration, Automation, and Response) builds upon the capabilities of SIEM by automating and orchestrating incident response workflows. SOAR platforms integrate with various security tools and systems to automate tasks such as threat investigation, containment, and remediation. SOAR platforms are well suited for threat and vulnerability management because they can automate the process of finding a threat or vulnerability. They can also automate the process of handling vulnerabilities.

Therefore, SOAR platforms are specifically designed to automate and streamline incident response and security operations, including aspects of threat and vulnerability management, whereas SIEM solutions are primarily focused on log aggregation, correlation, and alerting. SOAR platforms leverage intelligence from a SIEM, and uses it to run a playbook to remediate an incident or fix a vulnerability.

Options B, C, and D are incorrect because:

Option B: SIEM applications are not primarily used for threat and vulnerability management.

Option C and D: These options incorrectly describe the information flow between SIEM and SOAR. SIEM typically feeds security event data to SOAR, not the other way around.

Further Reading:

SIEM:https://www.ibm.com/topics/siem
SOAR:https://www.ibm.com/topics/security-orchestration-automation-response-soar
Difference between SIEM and SOARhttps://www.paloaltonetworks.com/cyberpedia/what-is-a-security-orchestration-automation-and-response-soar

Question: 12

What is the difference between mandatory access control (MAC) and discretionary access control (DAC)?

A. MAC is controlled by the discretion of the owner and DAC is controlled by an administrator

B. MAC is the strictest of all levels of control and DAC is object-based access

C. DAC is controlled by the operating system and MAC is controlled by an administrator

D. DAC is the strictest of all levels of control and MAC is object-based access

Answer: B

Explanation:

The correct answer is **B. MAC is the strictest of all levels of control and DAC is object-based access.** Here's why:

Mandatory Access Control (MAC) is a security model where access permissions are based on a system of security labels assigned to both users and data. These labels represent sensitivity levels (e.g., "Confidential," "Secret," "Top Secret"). The operating system enforces these labels strictly, preventing access even if the user believes they have permission. MAC is considered the most restrictive because it overrides user discretion and ensures access adheres to pre-defined security policies. It's often implemented in high-security environments like government or military systems.

Discretionary Access Control (DAC), on the other hand, is based on the owner's discretion. The owner of a resource (e.g., a file, a database) decides who can access it and what actions they can perform. DAC relies on access control lists (ACLs) that specify permissions for each user or group. This model is more flexible but also more prone to errors if the owner isn't diligent with permission management. DAC is object-based because access control is directly tied to the specific resource (object).

Therefore, option B accurately reflects the fundamental difference: MAC enforces strict, system-wide policies, making it the highest level of control, while DAC grants access at the discretion of the resource owner on a per-object basis.

Here are some authoritative resources for further learning:

National Institute of Standards and Technology (NIST):
https://csrc.nist.gov/glossary/term/mandatory_access_control (MAC definition)
National Institute of Standards and Technology (NIST):
https://csrc.nist.gov/glossary/term/discretionary_access_control (DAC definition)
IBM Documentation:https://www.ibm.com/docs/en/zvm/7.2?topic=security-mandatory-access-control-mac (MAC explanation)
Microsoft Documentation:https://learn.microsoft.com/en-us/windows/security/identity-protection/access-control/access-control (General access control overview, includes both MAC and DAC)

Question: 13

What is the practice of giving employees only those permissions necessary to perform their specific role within an organization?

A. least privilege

B. need to know

C. integrity validation

D. due diligence

Answer: A

Explanation:

The correct answer is **A. least privilege**.

The principle of least privilege dictates that users, processes, and systems should only be granted the minimum level of access necessary to perform their legitimate functions. This security practice aims to limit the potential damage that can occur if an account is compromised or a user acts maliciously or accidentally.

By restricting access, the blast radius of a security incident is significantly reduced. For example, a user responsible for data entry shouldn't have administrative rights to the database system, preventing them from accidentally deleting records or making unauthorized changes.

Option B, "need to know," is closely related but focuses on access to specific information rather than overall permissions. Need-to-know ensures individuals only have access to data essential for their tasks. While intertwined with least privilege, it's a narrower concept dealing with data access specifically. Options C and D, "integrity validation" and "due diligence," are important security practices but not directly related to granting access based on job roles. Integrity validation focuses on ensuring data hasn't been tampered with, and due diligence refers to the responsible actions an organization takes to maintain security.

In summary, least privilege is about restricting permissions to the absolute minimum required for a user's role. This principle is fundamental to building a secure and robust system by limiting access and thus minimizing potential harm from security incidents.

For further research, consult the following resources:

NIST Special Publication 800-53:https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final (See section on Access Control)
OWASP (Open Web Application Security Project):https://owasp.org/www-project-top-ten/ (Often mentions least privilege in relation to access control and security best practices.)
SANS Institute:https://www.sans.org/ (SANS provides various security courses and whitepapers, many of which cover the principle of least privilege)

Question: 14

What is the virtual address space for a Windows process?

A. physical location of an object in memory
B. set of pages that reside in the physical memory
C. system-level memory protection feature built into the operating system
D. set of virtual memory addresses that can be used

Answer: D

Explanation:

The correct answer is D, which defines a virtual address space as the set of virtual memory addresses a process can use. A virtual address space is a fundamental concept in modern operating systems, including Windows. Each process receives its own isolated virtual address space, which is a contiguous range of memory locations from the process's perspective. This space is not directly tied to physical RAM; instead, the operating system manages the mapping between virtual addresses and physical memory using a page table.

Options A, B, and C are not accurate definitions of virtual address space. Option A, describing the physical location of an object in memory, refers to a physical address rather than a virtual one. Option B, the set of pages in physical memory, describes the physical RAM usage and not a process's isolated memory view.

Option C, a system-level memory protection feature, is related to the broader memory management mechanisms, but doesn't specifically define virtual address space.

Virtual address space allows multiple processes to run concurrently without interfering with each other's memory. Each process believes it has exclusive access to its own address range. The OS and hardware work together to translate the virtual addresses used by processes into physical RAM addresses. This translation mechanism enables memory protection, allowing the OS to isolate each process and prevent unauthorized access to other process's data. Virtual address space also allows processes to use more memory than physically available through techniques like paging or swapping. This is achieved by storing less frequently used parts of process memory on disk, bringing them back into physical RAM as needed.

For further research on virtual address space and operating system memory management, you can refer to these authoritative links:

1. **Operating System Concepts by Abraham Silberschatz, Peter Baer Galvin, and Greg Gagne:** A classic textbook that provides comprehensive coverage on virtual memory and process management concepts.
2. **Microsoft Windows Internals by Mark Russinovich, David A. Solomon, and Alex Ionescu:** Offers a deep dive into the internals of the Windows operating system, including memory management mechanisms.
3. **OSDev Wiki:** A community-driven resource with detailed information about operating system design and implementation, including memory management. (https://wiki.osdev.org/)
4. **Wikipedia page on Virtual Memory:** Offers a good overview of the concept and related technologies. (https://en.wikipedia.org/wiki/Virtual_memory)

Question: 15

Which security principle is violated by running all processes as root or administrator?

A. principle of least privilege

B. role-based access control

C. separation of duties

D. trusted computing base

Answer: A

Explanation:

The correct answer is A, the principle of least privilege. Running all processes as root or administrator directly violates this core security principle. The principle of least privilege dictates that users, processes, or programs should only have the minimum access rights necessary to perform their required functions. Granting root or administrator privileges to every process means each has unlimited control over the system, including the ability to modify critical configurations, access any data, and potentially cause significant damage if compromised or malfunctioning. This broad access elevates the risk of both accidental and intentional harm to the system.

If a process with such elevated privileges is compromised by malicious actors, the impact will be much greater than if the process was operating under restricted permissions. Malware could use these rights to escalate privileges, spread within the system, and cause extensive harm. Additionally, errors or unintended consequences in a privileged process could easily compromise the overall system security and stability. Role-based access control (B), while important, is not directly violated by running all as root/admin, as that principle focuses on assigning privileges based on roles. Separation of duties (C) is also not directly violated by such practices, although it would make it very difficult to enforce this separation because every process would have the same powerful rights. The trusted computing base (D) is a different concept, referring to the hardware, software, and firmware components that provide a secure foundation; granting all processes high privileges does not directly impact the TCB itself. The core issue here is the excess of privilege and the failure to restrict access to only what is needed.

For further research, consider exploring these links:

NIST SP 800-53: A comprehensive framework for information security, which includes discussions of the principle of least privilege. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
OWASP (Open Web Application Security Project): Provides a wealth of resources on security principles, including least privilege. https://owasp.org/
Principle of Least Privilege: A broad overview of the concept.
https://en.wikipedia.org/wiki/Principle_of_least_privilege

Question: 16

What is the function of a command and control server?

A.It enumerates open ports on a network device
B.It drops secondary payload into malware
C.It is used to regain control of the network after a compromise
D.It sends instruction to a compromised system

Answer: D

Explanation:

The correct answer is **D. It sends instruction to a compromised system.** A command and control (C2) server acts as the central hub for attackers to maintain control over compromised devices or systems, often forming part of a botnet. Once a system is infected with malware, it typically establishes a connection to the C2 server.

This connection allows the attacker to send commands to the compromised host, directing it to perform malicious activities such as launching distributed denial-of-service (DDoS) attacks, stealing data, or installing additional malware. Option A, enumerating open ports, is more related to network reconnaissance. Option B, dropping secondary payloads, might be an action commanded by the C2 server but is not the server's core function. Option C, regaining control after a compromise, could be a consequence of C2 server usage, not its primary purpose. The C2 server maintains ongoing communication, facilitating remote control of infected devices. In essence, it's the communication lifeline for malicious actors to orchestrate their attacks after the initial compromise. Without C2 infrastructure, many types of sophisticated attacks would be significantly more difficult to execute.

Authoritative Links for further research:

NIST Special Publication 800-83, Guide to Malware Incident Prevention and Handling:
https://csrc.nist.gov/publications/detail/sp/800-83/rev-1/final (Search for "command and control" within this document)
Mitre ATT&CK Framework:https://attack.mitre.org/techniques/ (Search for Command and Control Tactics) **SANS Institute:**https://www.sans.org/ (Search the site for articles on C2 infrastructure)

Question: 17

What is the difference between deep packet inspection and stateful inspection?

A.Deep packet inspection is more secure than stateful inspection on Layer 4
B.Stateful inspection verifies contents at Layer 4 and deep packet inspection verifies connection at Layer 7
C.Stateful inspection is more secure than deep packet inspection on Layer 7
D.Deep packet inspection allows visibility on Layer 7 and stateful inspection allows visibility on Layer 4

Answer: D

Explanation:

Okay, let's break down the difference between deep packet inspection (DPI) and stateful inspection, and why option D is the correct answer.

Stateful inspection, at its core, tracks the state of network connections. It examines traffic at Layer 4 (the transport layer) of the OSI model, specifically focusing on TCP and UDP session information. It uses this information to determine if a packet is part of an established, legitimate connection. Think of it as a traffic cop verifying if a car is allowed on the road based on its license plate (connection details). It doesn't delve into the actual contents of the packet payload.

Deep packet inspection (DPI), in contrast, goes much deeper. It examines the actual data within the packet payload, analyzing information up to Layer 7 (the application layer). DPI can identify specific applications, protocols, and even potentially malicious content. It's like the traffic cop also checking the car's registration, insurance, and driver's license to confirm legitimacy and uncover potential issues. This provides a much more granular level of visibility and control.

Therefore, the key distinction lies in the depth of analysis. Stateful inspection tracks connections at Layer 4, while DPI analyzes the application-level data at Layer 7. Option D accurately reflects this distinction by stating that DPI allows visibility at Layer 7, and stateful inspection allows visibility at Layer 4. Option A is incorrect because the level of security is not a direct relationship of which Layer is being investigated, Option B has the layers in correct for each type of inspection, and option C also incorrectly claims that stateful is more secure at layer 7 which it doesn't inspect.

Key Points:

Stateful Inspection (Layer 4): Focuses on connection tracking, validating established connections. It's faster but provides less granular detail.

Deep Packet Inspection (Layer 7): Examines packet contents, enabling application-level filtering and detection of malicious activity. It is more resource intensive but provides more detailed control.

Authoritative Links for Further Research:

Cisco: Firewall Technologies - Stateful Inspection vs Deep Packet Inspection:
https://www.cisco.com/c/en/us/td/docs/security/asa/asa912/configuration/firewall/asa-firewall-cli/stateful.html
Fortinet: Stateful Inspection vs. Deep Packet Inspection:
https://www.fortinet.com/resources/cyberglossary/stateful-vs-deep-packet-inspection **Wikipedia: Deep Packet Inspection:**https://en.wikipedia.org/wiki/Deep_packet_inspection

Question: 18

Which evasion technique is a function of ransomware?

A.extended sleep calls
B.encryption
C.resource exhaustion
D.encoding

Answer: B

Explanation:

The correct answer is **B. encryption**. Ransomware, by its very nature, relies on encryption as its core operational technique. It encrypts the victim's files, rendering them inaccessible without the decryption key.

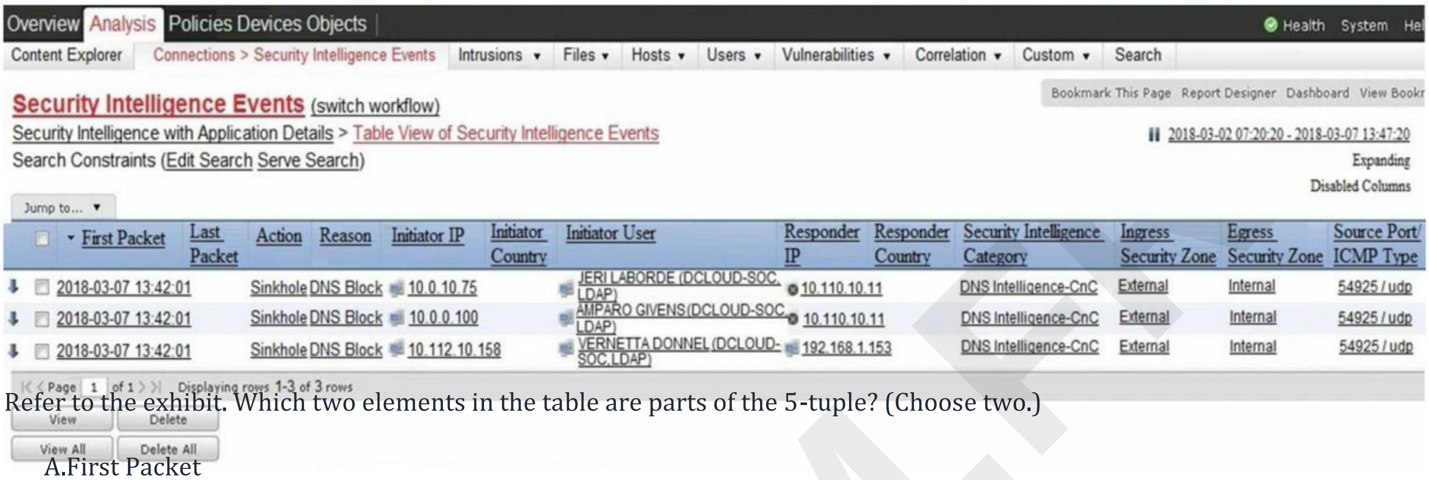
This act of encryption is the primary method used to hold data hostage, demanding a ransom payment for its release. Other evasion techniques like extended sleep calls (A) and resource exhaustion (C) are commonly used by malware for other purposes, such as delaying detection or disrupting systems, but they are not intrinsic functions of ransomware's core operational goal. Encoding (D), while a common technique, primarily changes the format of data for transmission or storage and not to render the original data unusable without a key. Resource exhaustion may be a side effect, but is not a primary function of ransomware itself. The encryption process is precisely what enables ransomware to monetize attacks.

Therefore, encryption is the key evasive tactic intrinsic to ransomware's modus operandi by preventing access to the data without a valid key and demanding a ransom for its release.

Authoritative Links for Further Research:

CISA (Cybersecurity and Infrastructure Security Agency) - Ransomware:https://www.cisa.gov/ransomware **NIST (National Institute of Standards and Technology) - Ransomware Risk Management:**
https://www.nist.gov/itl/applied-cybersecurity/ransomware-risk-management
ENISA (European Union Agency for Cybersecurity) - Ransomware Attacks:
https://www.enisa.europa.eu/topics/threat-landscape/ransomware-attacks

Question: 19



Security Intelligence Events (switch workflow)
Security Intelligence with Application Details > Table View of Security Intelligence Events
Search Constraints (Edit Search Serve Search)

2018-03-02 07:20:20 - 2018-03-07 13:47:20
Expanding
Disabled Columns

First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Initiator User	Responder IP	Responder Country	Security Intelligence Category	Ingress Security Zone	Egress Security Zone	Source Port/ ICMP Type
2018-03-07 13:42:01		Sinkhole	DNS Block	10.0.10.75		JERI LABORDE (DCLOUD-SOC, LDAP)	10.110.10.11		DNS Intelligence-CnC	External	Internal	54925 / udp
2018-03-07 13:42:01		Sinkhole	DNS Block	10.0.0.100		AMPARO GIVENS(DCLOUD-SOC, LDAP)	10.110.10.11		DNS Intelligence-CnC	External	Internal	54925 / udp
2018-03-07 13:42:01		Sinkhole	DNS Block	10.112.10.158		VERNETTA DONNEL (DCLOUD-SOC,LDAP)	192.168.1.153		DNS Intelligence-CnC	External	Internal	54925 / udp

Page 1 of 1 Displaying rows 1-3 of 3 rows

Refer to the exhibit. Which two elements in the table are parts of the 5-tuple? (Choose two.)

A.First Packet

B.Initiator User

C.Ingress Security Zone

D.Source Port

E.Initiator IP

Answer: DE

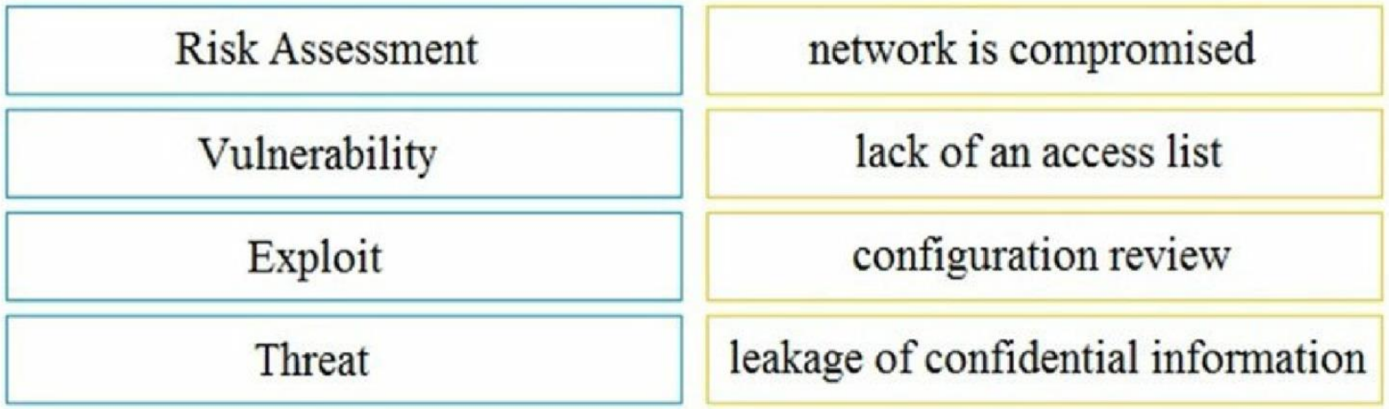
Explanation:

5-Tuple: The tuple (source IP address, source port, destination IP address, destination port, transport protocol).source: https://www.ietf.org/rfc/rfc6146.txtSo D, E are right answer

Question: 20

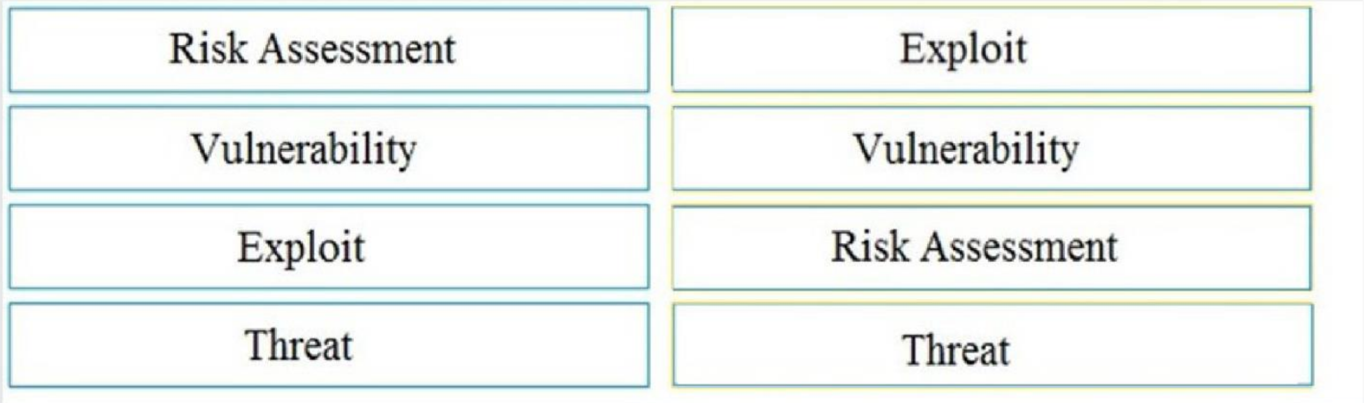
DRAG DROP -
Drag and drop the security concept on the left onto the example of that concept on the right.

Select and Place:



Risk Assessment	network is compromised
Vulnerability	lack of an access list
Exploit	configuration review
Threat	leakage of confidential information

Answer:



Risk Assessment	Exploit
Vulnerability	Vulnerability
Exploit	Risk Assessment
Threat	Threat

Explanation:

Exploitlack of an access list => Vulnerability configuration review => Risk Assessmentleakage of condidential information => Threat

Question: 21 What is the difference between statistical detection and rule-based detection models?

A.Rule-based detection involves the collection of data in relation to the behavior of legitimate users over a period of time
B.Statistical detection defines legitimate data of users over a period of time and rule-based detection defines it on an IF/THEN basis
C.Statistical detection involves the evaluation of an object on its intended actions before it executes that behavior
D.Rule-based detection defines legitimate data of users over a period of time and statistical detection defines it on an IF/THEN basis

Answer: B

Explanation:

The correct answer is **B: Statistical detection defines legitimate data of users over a period of time and rule-based detection defines it on an IF/THEN basis.**

Here's a detailed explanation:

Statistical detection, also known as anomaly detection, establishes a baseline of normal system or user behavior over time. It analyzes data patterns, such as resource utilization, network traffic, and user activity, to create a profile of what's considered typical. Deviations from this established baseline, beyond a defined threshold, trigger alerts as potentially malicious activities. This approach is valuable for identifying new or unknown threats because it focuses on deviations rather than predefined patterns.

Rule-based detection, conversely, operates on preconfigured rules or signatures. These rules are defined based on known attack patterns, specific file hashes, or other identifiable characteristics of malicious behavior. When a system event matches a rule, an alert is generated. This method is efficient at detecting known threats quickly but can be easily bypassed by novel attacks that don't match the existing rule set.

Option A is incorrect because rule-based detection doesn’t collect data on user behavior over time; it relies on predefined rules. Option C is incorrect; statistical detection doesn’t evaluate intended actions; it looks at deviations from normal behavior. Option D reverses the definitions of rule-based and statistical detection, making it incorrect.

In essence, statistical detection learns from normal behavior to flag deviations, while rule-based detection relies on predefined patterns to identify matches. Both methods are crucial components of a comprehensive cybersecurity strategy, each addressing different aspects of threat detection. Statistical detection can pick up subtle changes indicative of advanced persistent threats or zero-day exploits that rule-based systems might miss. Rule-based systems provide high accuracy on known threats. Choosing which method to implement depends on factors like environment and the trade-offs between accuracy and completeness.

Authoritative Links:

NIST Special Publication 800-83, Guide to Malware Incident Prevention and Handling: https://csrc.nist.gov/publications/detail/sp/800-83/final - Provides a comprehensive view of incident response, including detection strategies.

SANS Institute:https://www.sans.org/ - SANS offers numerous resources on cybersecurity, including articles and courses that cover detection methodologies.

OWASP:https://owasp.org/ - OWASP provides information about web application security, including how rule-based systems can help secure them.

Question: 22

What is the difference between a threat and a risk?

A. Threat represents a potential danger that could take advantage of a weakness, while the risk is the likelihood of a compromise or damage of an asset.

B. Risk represents the known and identified loss or danger in the system, while threat is a non-identified impact of possible risks.

C. Risk is the unintentional possibility of damages or harm to infrastructure, while the threats are certain and intentional.

D. Threat is a state of being exposed to an attack or a compromise, while risk is the calculation of damage or potential loss affecting the organization from an exposure.

Answer: A

Explanation:

Option A correctly differentiates between threat and risk in the cybersecurity context. A **threat** is a potential danger or action that could exploit a vulnerability or weakness within a system, network, or organization.

Think of it as the 'what could happen'. For example, a piece of malware or a malicious actor attempting unauthorized access constitutes a threat. Conversely, **risk** is the likelihood of that threat actually materializing and causing harm or damage to an asset, along with the potential impact of that harm. It combines the probability of the threat occurring with the severity of its consequences. It's the 'what is the likelihood and impact'. For instance, a vulnerability in a cloud storage service (threat) combined with a high likelihood of attackers targeting that vulnerability to steal sensitive data (risk) creates a significant security concern.

Option B is incorrect because it reverses the definitions; risk is not a known loss or danger, but a possibility of loss. Option C incorrectly states that risks are unintentional and threats are certain. Both risks and threats can stem from intentional or unintentional actions. Option D is also wrong as threats are not just a state of exposure, but the source of potential harm, and risk is more encompassing than just the calculation of damage.

Risk management involves assessing and mitigating potential threats. A high risk arises when there is a significant threat with a high likelihood of occurring and potentially causing serious damage. By understanding both threat and risk, security professionals can prioritize their efforts to strengthen their defenses, implement appropriate security controls, and minimize the impact of potential security breaches. A crucial part of understanding risk involves assessing the value of the asset under threat. Assets with high value, such as critical customer data in a cloud-based database, would have a higher risk rating when considering threats like data breaches.

Authoritative Links:

1. **NIST (National Institute of Standards and Technology) - Risk Management Framework:** https://csrc.nist.gov/projects/risk-management - NIST provides comprehensive guidelines and standards on risk management, including definitions of threats and risks.
2. **SANS Institute - Understanding Threats and Risks:**https://www.sans.org/ - SANS offers numerous cybersecurity courses and articles explaining threats, risks, and vulnerability management. Search for "understanding threats and risks" on their site.
3. **ENISA (European Union Agency for Cybersecurity):**https://www.enisa.europa.eu/ - ENISA publications often detail the latest threats and risk assessment methodologies used in cybersecurity.

Question: 23

Which attack method intercepts traffic on a switched network?

A.denial of service

B.ARP cache poisoning

C.DHCP snooping

D.command and control

Answer: B

Explanation:

The correct answer is B, ARP cache poisoning. Here's why: ARP (Address Resolution Protocol) cache poisoning is a type of attack that exploits the way networks resolve IP addresses to MAC addresses. In a switched network, devices use ARP to find the physical (MAC) address associated with an IP address on the local network. ARP cache poisoning involves sending falsified ARP messages to a switch or host, associating a malicious MAC address with a legitimate IP address. This redirection effectively intercepts network traffic destined for the legitimate IP as the traffic is now incorrectly directed to the attacker's machine.

Denial of service (A) aims to disrupt service availability, not directly intercept traffic. DHCP snooping (C) is a security feature that prevents unauthorized DHCP servers, it does not intercept normal traffic flow. Command and control (D) refers to attacker communication with compromised systems, not an interception method itself. Therefore, ARP cache poisoning is the only method listed that directly manipulates network addressing to intercept traffic. This makes it a common attack on local area networks due to the exploitable nature of

ARP's trust-based protocol. It is often used in man-in-the-middle scenarios.

Further Reading:

Cisco - Understanding ARP and ARP Poisoning
OWASP - ARP Poisoning

Question: 24

What does an attacker use to determine which network ports are listening on a potential target device?

A.man-in-the-middle
B.port scanning
C.SQL injection
D.ping sweep

Answer: B

Explanation:

The correct answer is B. Port scanning is the technique attackers utilize to discover which network ports on a target device are actively accepting connections. This is a fundamental reconnaissance step in a cyberattack. Attackers send various probe packets to different ports on the target system. The responses, or lack thereof, reveal whether a specific port is open, closed, or filtered. Open ports indicate the presence of a network service or application that can potentially be exploited. This information is crucial for attackers to identify vulnerabilities and subsequently craft specific attack vectors. While a man-in-the-middle (MITM) attack intercepts communications between two parties, and SQL injection manipulates database queries, and a ping sweep identifies active hosts on a network, none of these directly reveal open ports. Port scanning tools like Nmap are widely used for this purpose. By analyzing the responses from the target, attackers can determine the services running and the potential entry points into the system. This information helps them select the right exploitation methods. Therefore, port scanning is the primary method for identifying listening ports.

Authoritative Links:

Nmap Official Website:https://nmap.org/ (Provides details on port scanning techniques)
OWASP (Open Web Application Security Project) - Port Scanning:https://owasp.org/www-project-top-ten/ (General resource on security threats including port scanning)
SANS Institute - Port Scanning Techniques:https://www.sans.org/reading-room/whitepapers/detection/port-scan-detection-33944 (Provides a technical perspective on port scanning)

Question: 25

What is a purpose of a vulnerability management framework?

A. identifies, removes, and mitigates system vulnerabilities
B. detects and removes vulnerabilities in source code
C. conducts vulnerability scans on the network
D. manages a list of reported vulnerabilities

Answer: A

Explanation:

The correct answer, A, is the most comprehensive and accurately reflects the core purpose of a vulnerability management framework. Such a framework is designed to be a holistic approach to identifying, removing, and mitigating system vulnerabilities. It's not just about finding flaws but also about the entire lifecycle of addressing them. Vulnerability management frameworks utilize various tools and processes such as vulnerability scanning, penetration testing, and patch management to ensure the ongoing security of systems.

Option B is too narrow, focusing solely on source code vulnerabilities, which is just one aspect of a broader threat landscape. Option C describes vulnerability scanning, which is a tool used within a vulnerability management framework, not the framework itself. Option D is too limited, focusing only on tracking reported issues. While managing a list of vulnerabilities is part of the process, it does not encapsulate the entire scope of a framework.

A well-designed vulnerability management framework helps organizations proactively minimize risk by continuously assessing and remediating weaknesses in their infrastructure, applications, and systems. This process is essential to preventing cyberattacks that could exploit these vulnerabilities. Cloud environments, with their complexity and reliance on various interconnected components, particularly benefit from a structured approach to vulnerability management. Furthermore, a robust framework contributes to regulatory compliance, as many standards and laws require organizations to maintain a secure operating environment.

Authoritative links for further research:

NIST Special Publication 800-40, Revision 3: Guide to Enterprise Patch Management Planning https://csrc.nist.gov/publications/detail/sp/800-40/rev-3/final (While focusing on patch management, it's relevant to vulnerability management)
SANS Institute: Various resources on vulnerability management: https://www.sans.org/ (Search for "vulnerability management")
OWASP (Open Web Application Security Project): Provides information on application security and vulnerabilities: https://owasp.org/

Question: 26

A network engineer discovers that a foreign government hacked one of the defense contractors in their home country and stole intellectual property. What is the threat agent in this situation?

A.the intellectual property that was stolen

B.the defense contractor who stored the intellectual property

C.the method used to conduct the attack

D.the foreign government that conducted the attack

Answer: C

Explanation:

The correct answer is **D. the foreign government that conducted the attack**.

A threat agent is the entity that carries out a threat. In cybersecurity, this refers to the individual, group, or organization responsible for launching an attack. Options A, B, and C describe elements related to the attack but are not the attackers themselves. Option A, the intellectual property, is the asset being targeted, not the threat agent. Option B, the defense contractor, is the victim of the attack. Option C, the method used for the attack, refers to the tools and techniques employed, not the entity initiating it. The foreign government, as the perpetrator of the hacking incident, is the active agent initiating the malicious activity. They are the source of the threat, making option D the correct identification of the threat agent in this scenario. Understanding the nature of threat agents is crucial for effective threat modeling and risk assessment in cybersecurity.

Identifying the specific threat agent (e.g., state-sponsored actor, hacktivist group, insider threat) allows security professionals to better tailor security controls and responses. This also allows better intelligence gathering.

For further research on threat agents, you can refer to:

1. **NIST Special Publication 800-30, Guide for Conducting Risk Assessments:** https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final (This document provides a comprehensive framework for risk assessment, including the identification of threat sources.) 2. **OWASP (Open Web Application Security Project):**https://owasp.org/ (OWASP provides resources on various security topics, including information on threat agents and attack vectors.)

Question: 27

What is the practice of giving an employee access to only the resources needed to accomplish their job?

A.principle of least privilege

B.organizational separation

C.separation of duties

D.need to know principle

Answer: A

Explanation:

The correct answer is A, principle of least privilege. This security practice mandates granting users only the minimum necessary access rights to perform their job functions. It aims to limit the potential damage an attacker can cause if a user account is compromised or a user acts maliciously or accidentally, which can be a big concern in cloud environments. By restricting access, organizations reduce their attack surface and control the spread of malware or unauthorized data exfiltration. In contrast, organizational separation often refers to dividing teams or departments, while separation of duties involves assigning critical tasks to different users to prevent fraud. The need-to-know principle is closely related but emphasizes access to specific information, not necessarily resources. Although they might seem similar, the principle of least privilege focuses broadly on the resources or privileges available to the user, while need to know is often targeted at data. The principle of least privilege is crucial for cloud security because it ensures that even if one part of the system is compromised, the damage can be limited to that specific area.

Here are some authoritative links for further research:

NIST (National Institute of Standards and Technology) Special Publication 800-53: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final - This publication details security and privacy controls, including those related to access control and the principle of least privilege.

OWASP (Open Web Application Security Project):https://owasp.org/www-project-top-ten/ - OWASP provides valuable insights into common vulnerabilities and security best practices, where the principle of least privilege is often highlighted as a key strategy.

Cloud Security Alliance (CSA):https://cloudsecurityalliance.org/ - The CSA offers guidance and resources on cloud security, including best practices for access management.

Question: 28

Which metric is used to capture the level of access needed to launch a successful attack?

A.privileges required

B.user interaction

C.attack complexity

D.attack vector

Answer: A

Explanation:

The correct metric for assessing the level of access needed for a successful attack is **privileges required**. This metric directly measures the permissions or level of access an attacker needs to compromise a system or network. It focuses on the necessary user rights, administrative credentials, or system-level access needed to execute malicious actions. Attack complexity, while related, describes how intricate the attack method is, not the level of access needed. User interaction, refers to the user's actions in an attack while attack vector describes the method by which the attacker gains entry. Privileges required is the most granular and accurate metric when analyzing what type of access an attacker must possess to carry out their objectives. For example, needing administrator privileges to install malware signifies a high privilege requirement. Identifying privilege requirements enables security professionals to implement appropriate controls like least privilege access and role-based access control. These practices mitigate risks by restricting unnecessary access and limiting the potential damage an attacker can inflict. By evaluating privilege needs, security teams can strategically harden systems and networks.

Authoritative Links for further research:

NIST Special Publication 800-30, Guide for Conducting Risk Assessments: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final (While not directly defining "privileges required," this NIST guide discusses the importance of identifying and mitigating access-related risks in risk assessments.)
OWASP (Open Web Application Security Project) Top Ten:https://owasp.org/www-project-top-ten/ (OWASP emphasizes the significance of controlling access and privileges in web application security.)
SANS Institute:https://www.sans.org/ (SANS provides a variety of cybersecurity training courses and articles focusing on access control, privilege management, and security best practices.)

Question: 29

What is the difference between an attack vector and an attack surface?

A.An attack surface identifies vulnerabilities that require user input or validation; and an attack vector identifies vulnerabilities that are independent of user actions.

B.An attack vector identifies components that can be exploited; and an attack surface identifies the potential path an attack can take to penetrate the network.

C.An attack surface recognizes which network parts are vulnerable to an attack; and an attack vector identifies which attacks are possible with these vulnerabilities.

D.An attack vector identifies the potential outcomes of an attack; and an attack surface launches an attack using several methods against the identified vulnerabilities.

Answer: C

Explanation:

Okay, let's break down why option C is the correct answer.

An **attack surface** represents the total sum of all points where an attacker could potentially try to enter or extract data from a system or network. It's about identifying which parts of your infrastructure are exposed and potentially vulnerable. Think of it as the perimeter of your network that an attacker could probe. This includes things like open ports, web applications, user interfaces, and even employee behavior.

On the other hand, an **attack vector** is the specific method or path that an attacker uses to exploit a vulnerability and gain access to your system. It's the technique or tool used to carry out an attack. For example, an attack vector could be a phishing email, a SQL injection on a website, or exploiting a vulnerability in an operating system.

Therefore, option C correctly distinguishes the two. The attack surface identifies what is vulnerable, while the attack vector describes how those vulnerabilities can be exploited. The other options misrepresent the relationship and definitions of these terms. Option A confuses the dependencies; Option B reverses the meanings, and option D incorrectly defines their roles in an attack.

Further research can be conducted on these topics at the following links:

NIST Glossary: https://csrc.nist.gov/glossary/term/attack_surface
OWASP (Open Web Application Security Project):https://owasp.org/www-project-top-ten/ (Provides information on various attack vectors)

In essence, understanding the attack surface helps you identify vulnerabilities and potential entry points. Knowing the possible attack vectors helps you plan mitigation strategies and secure your infrastructure.

Question: 30

Which metric in CVSS indicates an attack that takes a destination bank account number and replaces it with a different bank account number?

A.integrity
B.confidentiality
C.availability
D.scope

Answer: A

Explanation:

The correct answer is **A. Integrity**.

CVSS (Common Vulnerability Scoring System) assesses vulnerabilities based on several metrics. Integrity, in the context of CVSS, refers to the trustworthiness and correctness of data. When an attacker replaces a destination bank account number with a different one, they are directly manipulating the data, rendering it untrustworthy and incorrect. This is a clear breach of integrity because the data is no longer in its intended or original state. Confidentiality focuses on preventing unauthorized disclosure of information, which isn't the core issue here. Availability deals with ensuring access to resources when needed, also not directly relevant to this scenario. Scope refers to the impact of a vulnerability on components beyond the affected entity, which isn't applicable in this particular data manipulation case. Therefore, the core issue is the alteration of data, making **integrity** the appropriate metric within CVSS to describe the attack.

For more information on CVSS and its metrics, please refer to the following resource:

FIRST (Forum of Incident Response and Security Teams) CVSS:https://www.first.org/cvss/

Question: 31

A security specialist notices 100 HTTP GET and POST requests for multiple pages on the web servers. The agent in the requests contains PHP code that, if executed, creates and writes to a new PHP file on the webserver. Which event category is described?

A.reconnaissance
B.action on objectives
C.installation
D.exploitation

Answer: D

Explanation:

The correct answer is **D. exploitation**. Here's why:

The scenario describes a malicious activity where HTTP requests containing PHP code are sent to a web server. This code, if executed, will create a new file, effectively altering the server's file system. This signifies an attacker actively trying to leverage a vulnerability on the web server. Exploitation, in the context of cybersecurity, refers to the stage where an attacker takes advantage of a system or application's weaknesses to gain unauthorized access, control, or cause harm. This action goes beyond reconnaissance, which would involve gathering information about the target; it's an active attempt to gain control over resources. It also precedes installation, which usually entails deploying additional malicious software, and occurs before any action on objectives, such as data exfiltration. The provided requests with embedded code are directly an attempt to exploit a vulnerability that allows the injection and execution of arbitrary code. Therefore, the creation and writing of a new file through malicious code execution perfectly demonstrates exploitation.

Further research can be conducted on the following topics:

OWASP Top Ten: A standard awareness document for developers on critical web application security risks, which can include the injection vulnerabilities described. https://owasp.org/www-project-top-ten/ **Exploitation in the Cyber Kill Chain:** Research on the stages of a cyber attack, further elaborating on what actions fall under the exploitation stage. https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
Web Shells: Understanding what a PHP web shell looks like and how it functions within a web server environment helps to better identify exploitation attempts.
https://www.cloudflare.com/learning/security/threats/web-shells/

Question: 32

What specific type of analysis is assigning values to the scenario to see expected outcomes?

A.deterministic
B.exploratory
C.probabilistic
D.descriptive

Answer: A

Explanation:

The correct answer is **A. deterministic**. Deterministic analysis involves assigning specific, fixed values to variables within a scenario to predict a definite outcome. In essence, it operates on the premise that given a particular set of inputs, the output will always be the same, eliminating uncertainty. This approach focuses on concrete relationships and cause-and-effect within a model. By assigning set values and running the analysis, a single expected outcome is produced. This contrasts with probabilistic analysis, which deals with uncertainty and a range of potential outcomes, not a fixed one. Exploratory analysis seeks patterns and insights without specific prior assumptions, and descriptive analysis summarizes existing data, neither actively predicting future events using fixed values. Therefore, the process of assigning values to predict singular outcomes aligns precisely with deterministic analysis. This type of analysis is crucial for understanding the behavior of systems under controlled parameters, a common practice in cybersecurity operations when evaluating the effects of specific actions or configurations.

Further Research:

Deterministic Systems: Wikipedia page on deterministic systems, explaining their properties and characteristics.

Deterministic vs. Probabilistic Models: Analytics Vidhya article explaining the key differences between deterministic and probabilistic models with use-cases.

Question: 33

When trying to evade IDS/IPS devices, which mechanism allows the user to make the data incomprehensible without a specific key, certificate, or password?

A. fragmentation
B. pivoting
C. encryption
D. stenography

Answer: C

Explanation:

The correct answer is **C. encryption**. Encryption is the process of converting data (plaintext) into an unreadable format (ciphertext) using an algorithm and a key. Without the specific key used for encryption, the data remains incomprehensible. This directly addresses the question's requirement of making data unintelligible without a specific key, certificate, or password.

Here's why the other options are incorrect:

A. fragmentation: Fragmentation breaks data into smaller packets for transmission. While this can complicate network analysis, it doesn't inherently make the data itself unreadable without a specific key. The original data can be reconstructed once all fragments are received.

B. pivoting: Pivoting is a technique used by attackers to move laterally within a network after gaining initial access. It does not involve making data incomprehensible.

D. steganography: Steganography hides data within other data, like an image or audio file. While it conceals the presence of data, it doesn't directly render it unintelligible without a key if the hidden data is discovered. The hidden data still could be read without a key.

In the context of evading IDS/IPS, attackers might use encryption to obfuscate malicious payloads or communication, preventing detection. The IDS/IPS would need the decryption key to understand the traffic, which they typically won't have in the case of attacker-controlled encryption. This makes encryption a common technique used by adversaries to avoid network security controls.

Authoritative Links for further research:

NIST (National Institute of Standards and Technology) - Cryptography:
https://www.nist.gov/itl/csd/cryptography (Comprehensive resource on cryptography concepts and standards)
OWASP (Open Web Application Security Project) - Cryptographic Storage Cheat Sheet:
https://cheatsheetseries.owasp.org/cheatsheets/Cryptographic_Storage_Cheat_Sheet.html (Information on

secure cryptographic practices)
SANS Institute - Information Security Training and Resources:https://www.sans.org/ (Offers training and materials on various security topics, including cryptography and network security)

Question: 34

Why is encryption challenging to security monitoring?

A.Encryption analysis is used by attackers to monitor VPN tunnels.
B.Encryption is used by threat actors as a method of evasion and obfuscation.
C.Encryption introduces additional processing requirements by the CPU.
D.Encryption introduces larger packet sizes to analyze and store.

Answer: B

Explanation:

The correct answer is **B. Encryption is used by threat actors as a method of evasion and obfuscation.**

Here's why:

Encryption, while crucial for protecting data confidentiality, poses significant challenges to security monitoring. Security monitoring systems rely on analyzing network traffic and system logs to detect malicious activities. When data is encrypted, this analysis becomes difficult because the content is obscured.

Attackers often leverage encryption to hide their malicious payloads, communication channels, and exfiltrated data. This obfuscation technique prevents security tools from identifying patterns, keywords, or anomalies that would otherwise indicate a compromise. For instance, malware communicating with its command-and-control (C2) server can mask the communication using encryption, making it harder to detect the malicious connection. The use of HTTPS can make it harder to inspect traffic, and the use of custom encryption methods can completely bypass analysis. While analysis may be possible, it requires specialized decryption knowledge and resources.

Option A is incorrect as encryption analysis is not typically used by attackers to monitor VPN tunnels; VPNs themselves leverage encryption for security. Option C, while true that encryption adds CPU overhead, is not the primary challenge to security monitoring. Option D's claim that increased packet sizes are the main issue with monitoring encrypted traffic is also inaccurate; while packet size increases with encryption, the content being obscured is the core obstacle.

In short, encryption provides a layer of secrecy that can be misused by threat actors to evade detection, hindering effective security monitoring. The inability to inspect encrypted data streams limits the effectiveness of traditional security monitoring tools, necessitating the adoption of more sophisticated techniques.

Further Research:

NIST Special Publication 800-53 Revision 5: See "Control AC-3 Information Access Enforcement"
https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
SANS Institute: Search for "Security Monitoring and Encryption" on their website. https://www.sans.org/
OWASP: Explore topics related to "Transport Layer Security (TLS) Best Practices" on their site.
https://owasp.org/

Question: 35

An employee reports that someone has logged into their system and made unapproved changes, files are out of order, and several documents have been placed in the recycle bin. The security specialist reviewed the system logs, found nothing suspicious, and was not able to determine what occurred. The software is up to date; there are no alerts from antivirus and no failed login attempts. What is causing the lack of data visibility needed to detect the attack?

A.The threat actor used a dictionary-based password attack to obtain credentials.

B.The threat actor gained access to the system by known credentials.

C.The threat actor used the teardrop technique to confuse and crash login services.

D.The threat actor used an unknown vulnerability of the operating system that went undetected.

Answer: B

Explanation:

Here's a detailed justification for why option B is the correct answer:

The scenario describes a situation where an attacker has successfully compromised a user's system without triggering typical security alerts. The fact that system logs show nothing suspicious, there are no antivirus alerts, and no failed login attempts suggests the attacker didn't use brute force or exploit a known vulnerability that would be easily detected. The system has been altered - files moved and deleted - indicative of an intruder's actions. This points to a compromise using legitimate credentials. Option B, "The threat actor gained access to the system by known credentials," directly addresses this. If the attacker uses legitimate credentials that belong to the user or a privileged account, the system would likely not flag the login as suspicious, as the authentication process is successful and deemed legitimate. They are behaving like an authorized user, bypassing any login-related alarms. Dictionary attacks (Option A) and teardrop attacks (Option C) would likely generate failed login attempts or system crashes, respectively, which were explicitly ruled out in the question statement. Finally, while an unknown vulnerability (Option D) could be a possibility, the context points more towards compromised credentials as the root cause, based on lack of any other alerts. This lack of detection indicates the attacker was authenticated.

Therefore, the lack of visibility stems from the fact that the attacker used known, valid credentials to access the system. This highlights a critical point in security: even with up-to-date software and active antivirus, compromised credentials can allow attackers to operate undetected. The focus for detection then shifts from access attempts to analyzing user behavior for deviations from the norm.

Relevant concepts:

Credential Compromise: One of the most common attack vectors; attackers steal or obtain valid user credentials for unauthorized access.

Authentication vs. Authorization: Authentication verifies identity, while authorization determines what the authenticated user can do. Successfully using stolen credentials would successfully authenticate the attacker.

Behavioral Anomaly Detection: The process of detecting unusual or suspicious actions performed by legitimate users or compromised accounts.

Further Research:

MITRE ATT&CK - Valid Accounts:https://attack.mitre.org/techniques/T1078/
NIST - Incident Handling:https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final
OWASP Top 10 - Broken Access Control: https://owasp.org/Top10/A01_2021-Broken_Access_Control/

Question: 36

A company receptionist received a threatening call referencing stealing assets and did not take any action

assuming it was a social engineering attempt. Within
48 hours, multiple assets were breached, affecting the confidentiality of sensitive information. What is the threat actor in this incident?

A.company assets that are threatened

B.customer assets that are threatened

C.perpetrators of the attack

D.victims of the attack

Answer: C

Explanation:

The correct answer is **C. perpetrators of the attack**. Here's a breakdown:

The scenario describes a security incident initiated by a threatening call, followed by a successful breach. The core question asks about the threat actor, which refers to the entity actively causing the harm. Options A, B, and D represent the targets or victims of the attack, not the initiators.

Perpetrators are those who commit the malicious actions, such as the individuals making the threatening call and executing the subsequent breach. Their goal is typically to gain unauthorized access, steal data, or cause disruption. In this instance, they are the ones who actively "stole assets" and "breached" systems.

Company assets (Option A) are the targets of the attack, not the actors. They are what the perpetrators aim to compromise.

Customer assets (Option B) may be indirectly affected if they depend on the company's services, but they aren't the direct threat actor. They become victims.

Victims of the attack (Option D) include the company and potentially its customers, but they are not the ones initiating the attack.

Therefore, the threat actor is definitively the group or person who made the threatening call and followed through with the breach. This aligns with common security definitions where a "threat actor" is the agent of malicious activity.

Supporting Concepts:

Threat Actor: In cybersecurity, a threat actor is an entity responsible for a malicious activity that targets digital assets, systems, or networks.

Incident Response: This scenario is an example of a security incident that requires an incident response plan. Identifying the threat actor is crucial in addressing and remediating the incident.

Authoritative Links:

NIST Cybersecurity Framework:https://www.nist.gov/cyberframework (Provides a comprehensive framework for managing cybersecurity risk and identifying threat actors).

MITRE ATT&CK Framework:https://attack.mitre.org/ (A knowledge base of adversary tactics and techniques, useful for understanding how threat actors operate.)

Question: 37

What is the relationship between a vulnerability and a threat?

A.A threat exploits a vulnerability

B.A vulnerability is a calculation of the potential loss caused by a threat

C.A vulnerability exploits a threat

D.A threat is a calculation of the potential loss caused by a vulnerability

Answer: A

Explanation:

The correct answer is A: "A threat exploits a vulnerability." This statement accurately reflects the fundamental relationship between these two crucial cybersecurity concepts. A vulnerability is a weakness or flaw in a system, network, or application that could be exploited. Think of it as an open door or an unlocked window in a building. A threat, on the other hand, is anything that has the potential to cause harm or damage by taking advantage of that vulnerability. The threat is the burglar who sees the open window and enters. The threat agent is the "who" or "what" that executes the threat. Threats can come in many forms: malicious software, human actors, natural disasters, etc. A vulnerability is a passive state; it's a potential weakness. It only becomes a problem when a threat is actively taking advantage of it. For example, a software bug (vulnerability) can be exploited by a hacker (threat) to gain unauthorized access. Without the vulnerability, the threat cannot be realized and, similarly, the vulnerability is not a risk until it can be exploited. The concept of risk ties these together as the calculated likelihood and impact of a threat exploiting a vulnerability.

Options B, C, and D are incorrect. Option B mistakenly defines a vulnerability as a calculation of loss, which is actually related to risk, not a vulnerability itself. Option C reverses the relationship, incorrectly stating that vulnerabilities exploit threats. Lastly, option D incorrectly states a threat is a calculation, whereas the threat is the actor or event, not a metric.

For further research, consider resources like:

NIST Special Publication 800-30 (Guide for Conducting Risk Assessments): This publication provides a detailed look into risk assessment, including the identification of threats and vulnerabilities.

https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final
OWASP (Open Web Application Security Project): OWASP provides resources on web application security, including vulnerability analysis and threat modeling. https://owasp.org/
SANS Institute: SANS provides a variety of cybersecurity courses and resources, often delving into threat and vulnerability management. https://www.sans.org/

Question: 38

What is the principle of defense-in-depth?

A.Agentless and agent-based protection for security are used.

B.Several distinct protective layers are involved.

C.Access control models are involved.

D.Authentication, authorization, and accounting mechanisms are used.

Answer: B

Explanation:

The principle of defense-in-depth, also known as layered security, is fundamentally about implementing multiple security controls at various points in a system or network. This strategy acknowledges that no single security measure is foolproof and that a breach may occur despite initial safeguards. Therefore, by layering different security mechanisms, you create a more resilient posture. If one layer is compromised, other layers are still in place to mitigate the impact. This approach might include a combination of preventive, detective, and corrective controls. For example, a network might use firewalls, intrusion detection systems, and endpoint protection to form multiple barriers. This way, an attacker would need to bypass multiple security layers to reach their target, making it much harder and time-consuming. Options A, C, and D describe specific security techniques but do not capture the core concept of a layered, multi-pronged approach to security.
Defense-in-depth is a foundational principle in cybersecurity and a key concept for protecting systems

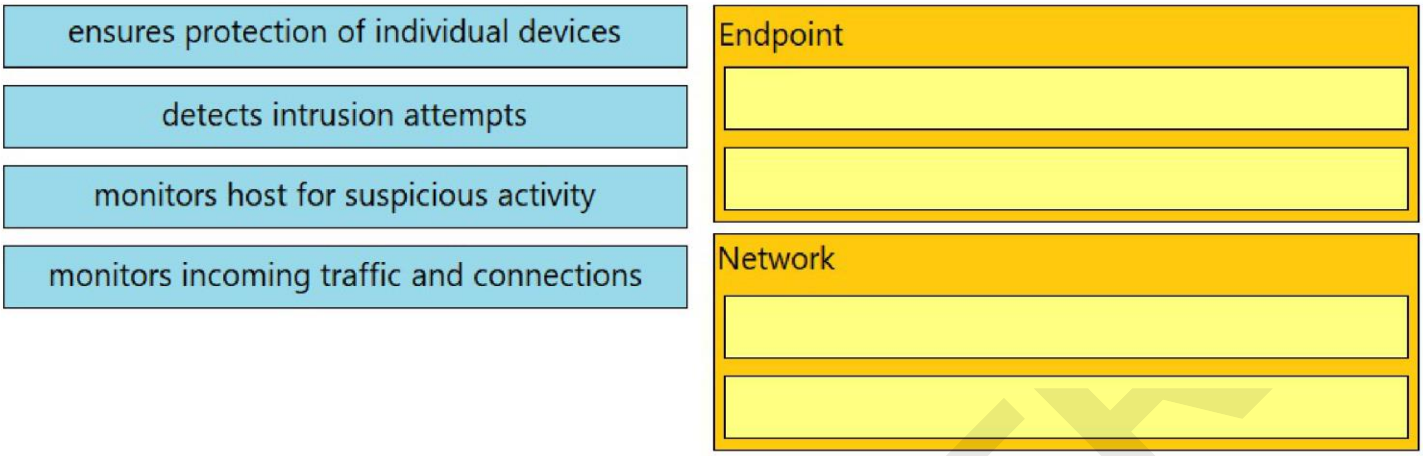
effectively.

Authoritative Links:

NIST SP 800-53: While not directly defining defense-in-depth, it provides a comprehensive framework for security controls that aligns with the concept of layered security: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
SANS Institute:https://www.sans.org/information-security/glossary/defense-in-depth (Provides a clear definition and explanation of defense-in-depth.)
OWASP:https://owasp.org/www-project-top-ten/ (While OWASP focuses on web application security, it emphasizes the need for layered security controls, which reflects defense-in-depth principles.)

Question: 39

DRAG DROP -
Drag and drop the uses on the left onto the type of security system on the right.
Select and Place:



ensures protection of individual devices

detects intrusion attempts

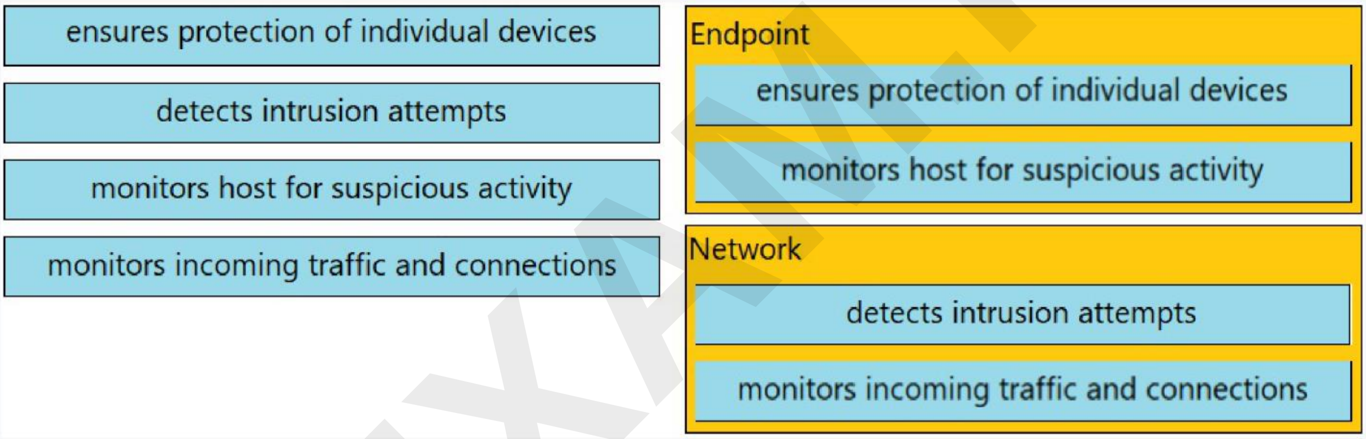
monitors host for suspicious activity

monitors incoming traffic and connections

Endpoint

Network

Answer:



ensures protection of individual devices

detects intrusion attempts

monitors host for suspicious activity

monitors incoming traffic and connections

Endpoint
- ensures protection of individual devices
- monitors host for suspicious activity

Network
- detects intrusion attempts
- monitors incoming traffic and connections

Question: 40

What is the difference between the rule-based detection when compared to behavioral detection?

A.Rule-Based detection is searching for patterns linked to specific types of attacks, while behavioral is identifying per signature.

B.Rule-Based systems have established patterns that do not change with new data, while behavioral changes.

C.Behavioral systems are predefined patterns from hundreds of users, while Rule-Based only flags potentially abnormal patterns using signatures.

D.Behavioral systems find sequences that match a particular attack signature, while Rule-Based identifies potential attacks.

Answer: C

Explanation:

Okay, let's break down why option C is the most accurate answer and why the others are incorrect regarding rule-based and behavioral detection in cybersecurity, particularly within the context of the Cisco CBROPS exam.

Justification for Answer C:

Option C accurately describes the core difference. **Behavioral detection** systems, at their foundation, establish a "baseline" of normal user or system activity by monitoring and learning from historical data. This baseline reflects patterns of typical behavior from a multitude of users. Deviations from this baseline, even if not matching a known attack signature, are flagged as potentially suspicious. This allows behavioral detection to identify novel attacks and insider threats. This is in contrast to **Rule-based detection,** which relies on predefined signatures or patterns. These patterns are directly associated with known attacks. When a match is identified the alert is triggered. So, Rule-Based focuses on matching known bad behavior, while behavioral is focused on identifying deviations from the known normal. The answer is thus C.

Why other options are incorrect:

Option A reverses the core concept. Rule-based detection searches for specific patterns or signatures of known attacks. Behavioral detection does not identify per signature; instead it identifies per deviation from a learned baseline.

Option B incorrectly states that rule-based patterns do not change. While the rules themselves may be static, the systems are updated frequently with new rules. This means they change to include new attack patterns. The most accurate statement would be that Behavioral is adaptive with new data, not Rule-based.

Option D reverses the actions of rule-based and behavioral detection. Behavioral does not find specific signatures; instead behavioral finds deviations from the norm. Rule-based detection does not identify "potential attacks" in the same way behavioral does. Instead Rule-based looks for a precise pattern in the data and flags that pattern.

In summary:

Behavioral detection excels at identifying novel attacks and internal threats by recognizing deviations from established patterns of normal behavior. Rule-based detection, on the other hand, is effective at spotting known threats via pre-defined signatures.

Authoritative Links for Further Research:

1. **Cisco's Cybersecurity Documentation:** Cisco provides in-depth documentation on their cybersecurity solutions and technologies, including explanations of detection methods: https://www.cisco.com/c/en/us/solutions/security.html
2. **National Institute of Standards and Technology (NIST):** NIST publications, such as their Cybersecurity Framework, address detection and response strategies: https://www.nist.gov/cyberframework
3. **SANS Institute:** SANS provides training and resources on cybersecurity topics, including detection techniques: https://www.sans.org/

By studying these resources, you can further solidify your understanding of these fundamental cybersecurity concepts.

Question: 41

A security incident occurred with the potential of impacting business services. Who performs the attack?

A. threat actor

B. malware author

C. direct competitor

D. bug bounty hunter

Answer: A

Explanation:

The correct answer is A, threat actor. A threat actor is the individual or group responsible for carrying out a malicious attack or security incident. They are the agents actively involved in exploiting vulnerabilities and initiating actions that lead to the compromise of systems or data. Options B, C, and D are not the correct actors in this scenario. A malware author (B) creates malicious software but is not necessarily the one deploying it in a specific attack. A direct competitor (C) might have a motive for an attack, but this doesn't define them as the attack perpetrator. Lastly, a bug bounty hunter (D) actively seeks and reports
vulnerabilities, not exploits them for malicious purposes. Security incidents impacting business services are typically caused by malicious activities initiated by a threat actor. These actors may range from amateur hackers to sophisticated cybercriminal organizations. Understanding the role of a threat actor is fundamental in incident response and cybersecurity operations. Threat actors' motivations vary but often include financial gain, espionage, or disruption of operations. Identifying and tracking threat actors helps security teams understand attack patterns and implement more effective preventative measures.

Further research:

MITRE ATT&CK Framework - This framework provides a comprehensive matrix of adversary tactics and techniques.

NIST Cybersecurity Framework - This framework helps organizations manage and reduce cybersecurity risks, including those posed by threat actors.

ENISA Threat Landscape - This resource from the European Union Agency for Cybersecurity provides insights into current threat actor trends.

Question: 42

How does a certificate authority impact security?

A.It authenticates domain identity when requesting an SSL certificate.

B.It validates client identity when communicating with the server.

C.It authenticates client identity when requesting an SSL certificate.

D.It validates the domain identity of the SSL certificate.

Answer: D

Explanation:

A Certificate Authority (CA) plays a crucial role in establishing trust within Public Key Infrastructure (PKI) and securing communication using protocols like SSL/TLS. The primary function of a CA is to validate the identity of entities requesting digital certificates. These certificates are used to verify that a website, service, or individual is who they claim to be. Option D, “It validates the domain identity of the SSL certificate,” is correct because the CA's primary responsibility when issuing an SSL/TLS certificate is to verify that the domain name specified in the certificate belongs to the entity requesting it. This verification process typically involves confirming domain ownership through DNS records or email verification. Once ownership is confirmed, the CA signs the certificate, thereby creating a trusted digital identity that browsers and other clients can verify.

Browsers rely on this signature to ensure that the connection to the website is secure and legitimate, preventing man-in-the-middle attacks. A CA does not directly authenticate the client or server identities in the manner that options A and B suggest; that authentication happens later using the already issued and trusted certificates. Option C is incorrect, as the CA verifies the domain's identity, not the client's identity during the certificate request. Therefore, the CA is essential for guaranteeing that a certificate corresponds to a specific domain and thus supports secure and trustworthy digital communication.

Authoritative Links:

What is a Certificate Authority - Sectigo
Public key infrastructure (PKI) - Cloudflare
Certificate Authority - SSL.com

Question: 43

Which data type is necessary to get information about source/destination ports?

A.statistical data
B.session data
C.alert data
D.connectivity data

Answer: B

Explanation:

Session data is the correct answer because it contains information about communication sessions, specifically including the source and destination ports used by network traffic. This data is crucial for understanding how applications communicate across networks. It provides a detailed record of the established connections, allowing security analysts to track which services are communicating with one another and on what specific ports. Statistical data, while useful for identifying trends, doesn't directly link to specific port numbers used by individual connections. Alert data focuses on detected security incidents rather than the underlying connection details. Connectivity data may describe overall network links but lacks the granular detail of specific sessions and their port usage. Session data, on the other hand, captures the complete flow of network communication, making it essential for investigating network events, troubleshooting connectivity issues, and detecting malicious activity that utilizes specific ports. Analyzing session data helps understand the "who, what, where, when, and how" of network communication, making it fundamental for cybersecurity operations.

For more information about session data and its role in network monitoring and security, refer to:

Cisco Cybersecurity Operations Fundamentals (CBROPS) documentation: Look for chapters on network analysis and session data within your specific course material.

Wireshark documentation: https://www.wireshark.org/docs/ - Wireshark is a widely used network protocol analyzer that captures and analyzes session data.

Network security books and articles: Search for materials covering network traffic analysis and the use of session data for security purposes.

RFC 793 (Transmission Control Protocol): https://datatracker.ietf.org/doc/html/rfc793 - Provides foundational details about the TCP protocol and its associated ports.

RFC 959 (File Transfer Protocol): https://datatracker.ietf.org/doc/html/rfc959 - Example of an application protocol utilizing specific ports.

Question: 44

Which event is a vishing attack?

A. obtaining disposed documents from an organization
B. using a vulnerability scanner on a corporate network
C. impersonating a tech support agent during a phone call
D. setting up a rogue access point near a public hotspot

Answer: C

Explanation:

The correct answer is **C. impersonating a tech support agent during a phone call.** This scenario aligns perfectly with the definition of a vishing attack. Vishing, short for "voice phishing," is a type of social engineering attack that uses phone calls to deceive victims into divulging sensitive information or performing actions that benefit the attacker. In this case, the attacker pretends to be a legitimate tech support agent, leveraging trust to manipulate the target. This often involves creating a sense of urgency or fear to bypass normal security protocols.

Options A, B, and D are not vishing attacks. Obtaining disposed documents (A) is often referred to as "dumpster diving" and is a form of physical reconnaissance, not a voice-based attack. Using a vulnerability scanner (B) is a legitimate security practice, though it can be used maliciously in some cases, it doesn't involve deception via voice communication. Setting up a rogue access point (D) is a man-in-the-middle attack affecting network traffic, not a social engineering attack executed via voice.

Vishing exploits the human element of security, making it crucial to educate individuals about these tactics.

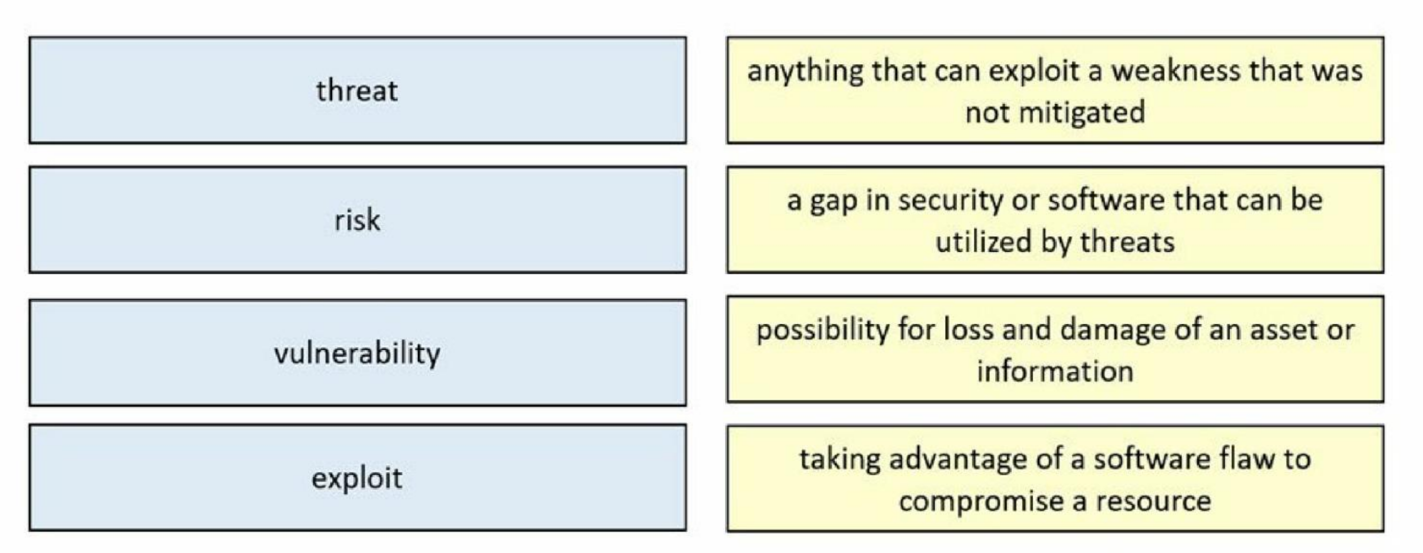
Cloud computing is not directly involved in this specific definition of vishing, though the victims may often utilize cloud-based services. Understanding the concept of social engineering is paramount to cybersecurity, since it's often the weakest link in the security chain.

Further research on this topic can be done at the following links:

NIST - Phishing (While this covers broader phishing, it explains the root social engineering concept) US-CERT - Understanding Social Engineering
IBM - What is Vishing?

Question: 45

DRAG DROP -
Drag and drop the security concept from the left onto the example of that concept on the right.
Select and Place:



threat

risk

vulnerability

exploit

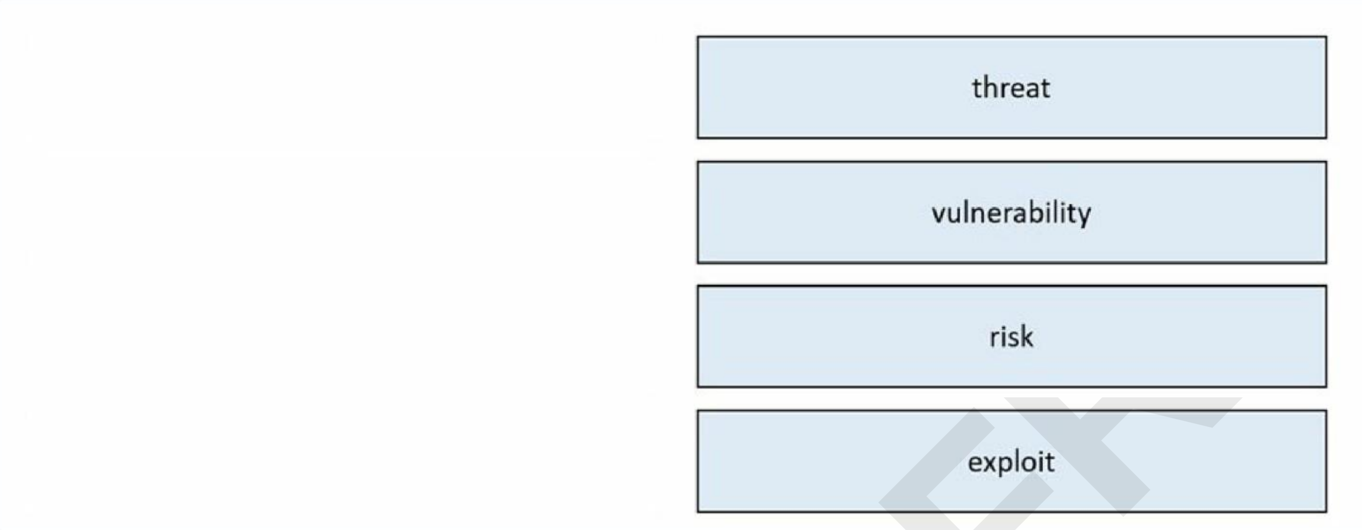
anything that can exploit a weakness that was not mitigated

a gap in security or software that can be utilized by threats

possibility for loss and damage of an asset or information

taking advantage of a software flaw to compromise a resource

Answer:



threat

vulnerability

risk

exploit

Explanation:

threat can exploit the weakness

gap is vulnerability

possibility is risk

compromise is exploit

Question: 46 What is a difference between SIEM and SOAR?

A.SIEM predicts and prevents security alerts, while SOAR checks attack patterns and applies the mitigation.

B.SIEM's primary function is to collect and detect anomalies, while SOAR is more focused on security operations automation and response.

C.SOAR's primary function is to collect and detect anomalies, while SIEM is more focused on security operations automation and response.

D.SOAR predicts and prevents security alerts, while SIEM checks attack patterns and applies the mitigation.

Answer: B

Explanation:

The correct answer is B because it accurately reflects the core functionalities of Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) tools. SIEM systems are primarily designed to gather logs and security events from various sources across an organization's infrastructure, including servers, applications, and network devices. This collected data is then analyzed for anomalies and potential security threats. SIEM's core strength lies in its ability to provide a centralized platform for detection and alerting. In contrast, SOAR platforms focus on automating security operations and incident response processes. SOAR integrates with various security tools and services, enabling security teams to define workflows and playbooks that automatically respond to security incidents.

This includes tasks like isolating infected machines, blocking malicious traffic, and escalating incidents to human analysts. SOAR's automation capabilities reduce manual intervention and improve incident response efficiency. Option A incorrectly describes the functions. Option C reverses the correct functionalities of SIEM and SOAR. Option D also incorrectly assigns the functions of prediction/prevention and pattern-checking/mitigation. Therefore, option B clearly distinguishes between SIEM's data collection, detection, and analysis role and SOAR's focus on automation and response.

Authoritative links for further research:

NIST Special Publication 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS): https://csrc.nist.gov/publications/detail/sp/800-94/final (While not directly about SIEM/SOAR, it explains core IDPS concepts which SIEM builds upon)
Gartner's Market Guide for Security Orchestration, Automation and Response: https://www.gartner.com/en/documents/3887324 (Requires Gartner subscription but a good starting point) **SANS Institute resources on SIEM and SOAR:**https://www.sans.org/ (Search for specific SIEM and SOAR related content)

Question: 47

What is vulnerability management?

A.A process to identify and remediate existing weaknesses.

B.A process to recover from service interruptions and restore business-critical applications.

C.A security practice of performing actions rather than acknowledging the threats.

D.A security practice focused on clarifying and narrowing intrusion points.

Answer: A

Explanation:

The correct answer, "A. A process to identify and remediate existing weaknesses," accurately defines vulnerability management. Vulnerability management is a cyclical security process focused on proactively discovering, assessing, and resolving security flaws within a system or network. This includes identifying potential vulnerabilities through automated scanning tools and manual assessments, prioritizing them based on severity and risk, and implementing appropriate mitigation strategies like patching, configuration changes, or implementing compensating controls. Option B describes Disaster Recovery, while option C is vague and doesn't accurately depict any specific security process. Option D touches on a principle related to security hardening but doesn't define vulnerability management. Vulnerability management is a critical component of a robust cybersecurity posture and is typically included in risk management framework. Failure to perform adequate vulnerability management can expose organizations to successful cyberattacks.

To better understand the concept, you may refer to authoritative sources:

NIST (National Institute of Standards and Technology) - Special Publication 800-40:

https://csrc.nist.gov/publications/detail/sp/800-40/rev-3/final. This document provides guidance on patch management, a component of vulnerability management.

SANS Institute - Vulnerability Management: https://www.sans.org/information-security/topic/vulnerability-management. This resource provides a detailed overview of vulnerability management concepts.

OWASP (Open Web Application Security Project) - Vulnerability Management: https://owasp.org/www-project-vulnerability-management-guide/. This site focuses on web application security vulnerability management.

Question: 48

What is a difference between signature-based and behavior-based detection?

A.Signature-based identifies behaviors that may be linked to attacks, while behavior-based has a predefined set of rules to match before an alert.

B.Behavior-based identifies behaviors that may be linked to attacks, while signature-based has a predefined set of rules to match before an alert.

C.Behavior-based uses a known vulnerability database, while signature-based intelligently summarizes existing data.

D.Signature-based uses a known vulnerability database, while behavior-based intelligently summarizes existing data.

Answer: B

Explanation:

Okay, let's break down why option B is the correct answer.

Signature-based detection operates by comparing network traffic or system activity against a database of known attack patterns, or "signatures." Think of it like a fingerprint; if the traffic matches a known malicious fingerprint, an alert is triggered. These signatures are often created from previously identified malware or exploits. This method is highly effective at detecting known threats but struggles with zero-day exploits or attacks that use variations of known malicious code.

Behavior-based detection, on the other hand, focuses on establishing a baseline of "normal" system or network activity. It then looks for deviations from this baseline. For instance, if a user suddenly logs in from a new location or attempts to access a restricted resource, behavior-based detection might flag it as suspicious, even if no known malware is involved. This method is more effective at catching new or customized attacks but can also generate false positives if there's a significant shift in legitimate user behavior.

Therefore, option B correctly states that behavior-based detection identifies behaviors that may be linked to attacks while signature-based detection relies on a predefined set of rules to match before an alert. Option A reverses these definitions, while options C and D incorrectly associate vulnerability databases and data summarization with the respective detection methods.

In summary, signature-based detection is reactive, focusing on known threats, while behavior-based detection is proactive, focusing on anomalies. Both methods have their strengths and weaknesses, and are often used in combination within a comprehensive security system.

Authoritative Links for further research:

1. **NIST Special Publication 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS):** https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf - This document provides a broad overview of intrusion detection systems and includes explanations of signature-based and anomaly-based (behavior-based) detection.
2. **SANS Institute:**https://www.sans.org/ - SANS offers numerous resources, including courses and

white papers, covering different aspects of cybersecurity including intrusion detection and prevention methods. Search their resources for articles related to "signature based detection" or "behavior based detection".

3. **Cisco Security Documentation**https://www.cisco.com/c/en/us/products/security/index.html -Although specific documentation for CBROPS may require a login, exploring Cisco's general security pages provides valuable insights into their approach to threat detection.

These links provide deeper context on the concepts discussed and will help you understand the nuances of these detection methods.

Question: 49

When communicating via TLS, the client initiates the handshake to the server and the server responds back with its certificate for identification.
Which information is available on the server certificate?

A.server name, trusted subordinate CA, and private key

B.trusted subordinate CA, public key, and cipher suites

C.trusted CA name, cipher suites, and private key

D.server name, trusted CA, and public key

Answer: D

Explanation:

The correct answer is **D. server name, trusted CA, and public key**. Let's break down why. During a TLS handshake, the server's certificate is crucial for the client to verify the server's identity and establish a secure connection. This certificate is like a digital passport.

Firstly, the **server name**, typically the Fully Qualified Domain Name (FQDN) is present. This enables the client to confirm that the certificate is indeed issued to the server it intended to connect with. This prevents man-in-the-middle attacks where an attacker could impersonate the server.

Secondly, the certificate contains the **trusted CA (Certificate Authority)**. The CA is an entity that verifies the server's identity and signs the certificate. The client checks if the CA is in its trusted list. If it is, the client can be confident about the authenticity of the server certificate and that the server is who it claims to be. This builds trust in the process.

Thirdly, the certificate includes the server's **public key**. This is used to encrypt data that only the server, with its corresponding private key, can decrypt. The client uses this public key to encrypt a secret key which is used for the rest of the secure communication, establishing the encrypted channel between client and server. This demonstrates the fundamental principle of asymmetric cryptography.

Option A is incorrect because the server's private key is never included in the certificate. This key remains secret and solely resides on the server. Option B is wrong because while it contains the public key, it misses the server name and mentions cipher suites, which is negotiated separately. Option C is also incorrect because it mentions cipher suites and also the server's private key, which never leaves the server.

Further reading:

SSL/TLS Handshake:https://www.cloudflare.com/learning/ssl/what-happens-in-a-tls-handshake/ **Digital Certificates:**https://www.globalsign.com/en/blog/digital-certificates-what-are-they
Public Key Cryptography:https://www.cloudflare.com/learning/ssl/what-is-public-key-cryptography/

Question: 50

How does an SSL certificate impact security between the client and the server?

A.by enabling an authenticated channel between the client and the server
B.by creating an integrated channel between the client and the server
C.by enabling an authorized channel between the client and the server
D.by creating an encrypted channel between the client and the server

Answer: D

Explanation:

The correct answer, **D. by creating an encrypted channel between the client and the server**, accurately reflects the primary security impact of an SSL certificate. SSL (Secure Sockets Layer) or its successor TLS (Transport Layer Security) certificates are fundamental to establishing secure communication over the internet. These certificates utilize public key infrastructure (PKI) to enable encryption of data transmitted between a client (like a web browser) and a server (like a website's server). This encryption process scrambles the data, rendering it unreadable to unauthorized parties who might intercept it. Without encryption, data such as passwords, personal information, and financial details would be vulnerable to eavesdropping.

The encryption is achieved through a handshake process where the server presents its SSL certificate to the client. The client then verifies the certificate's validity using a trusted Certificate Authority (CA). Once validated, a secure, encrypted channel is established, ensuring that only the intended client and server can decipher the transmitted data. Therefore, the SSL certificate plays a crucial role in maintaining the
confidentiality of communications, a core tenet of information security. Options A and C, while related to security, are not the direct impact of an SSL certificate. Authentication (Option A) and authorization (Option C) may be subsequent steps facilitated by the secure channel, but the certificate’s primary function is enabling encryption. Option B, integrated channel, is not an accurate term in this context.

Authoritative links for further reading:

Cloudflare: What is an SSL Certificate?https://www.cloudflare.com/learning/ssl/what-is-an-ssl-certificate/
DigiCert: What is an SSL Certificate?https://www.digicert.com/resources/what-is-ssl-certificate
Wikipedia: Transport Layer Securityhttps://en.wikipedia.org/wiki/Transport_Layer_Security

Question: 51

Which attack is the network vulnerable to when a stream cipher like RC4 is used twice with the same key?

A.forgery attack
B.plaintext-only attack
C.ciphertext-only attack
D.meet-in-the-middle attack

Answer: C

Explanation:

Here's a detailed justification for why the correct answer is **C. ciphertext-only attack** when a stream cipher like RC4 is used twice with the same key.

Stream ciphers, such as RC4, work by generating a pseudorandom keystream. This keystream is then XORed with the plaintext to produce the ciphertext. Ideally, this keystream should be unique for each encryption operation. However, if the same key is used to initialize the keystream generator twice, the exact same keystream will be produced both times.

If an attacker intercepts two different ciphertexts that were encrypted with the same key and thus the same keystream, a ciphertext-only attack becomes possible. Specifically, because both ciphertexts (C1 and C2) are derived from the XOR of their respective plaintexts (P1 and P2) with the same keystream (K), i.e., C1=P1 XOR K and C2=P2 XOR K, the attacker can XOR the two ciphertexts together (C1 XOR C2). This operation effectively cancels out the shared keystream: (P1 XOR K) XOR (P2 XOR K) simplifies to P1 XOR P2. Knowing P1 XOR P2, an attacker might be able to gain information about the plaintexts themselves, especially if they have partial knowledge of one of them or if certain patterns are present in the data. This is a core principle of a ciphertext-only attack exploiting a key reuse vulnerability. Essentially, by reusing the same key, the ciphertexts are no longer protected by the security that comes from unique keystreams. The vulnerability arises from the predictability of the repeated keystream, which leaks information when combining the ciphertexts, allowing for possible plaintext recovery. This is a classic flaw of misusing stream ciphers, highlighting the importance of using unique keys and initialization vectors (IVs) for each encryption.

Here are some resources for further research:

NIST Special Publication 800-38A:https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.pdf (While not focused on RC4 specifically, it covers modes of operation for block ciphers and related security implications, which are relevant in understanding key reuse dangers)
Wikipedia on RC4:https://en.wikipedia.org/wiki/RC4 (Details its weaknesses, including key reuse vulnerabilities)
Cryptography Engineering (by Ferguson, Schneier, and Kohno): This book discusses real-world security problems, including issues with stream ciphers, in detail.

Therefore, given the context, the correct answer is definitively **C. ciphertext-only attack.**

Question: 52

Which list identifies the information that the client sends to the server in the negotiation phase of the TLS handshake?

A. ClientStart, ClientKeyExchange, cipher-suites it supports, and suggested compression methods
B. ClientStart, TLS versions it supports, cipher-suites it supports, and suggested compression methods
C. ClientHello, TLS versions it supports, cipher-suites it supports, and suggested compression methods
D. ClientHello, ClientKeyExchange, cipher-suites it supports, and suggested compression methods

Answer: C

Explanation:

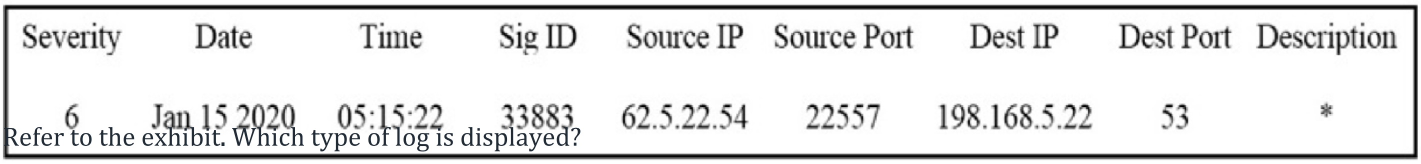
The correct answer is C: ClientHello, TLS versions it supports, cipher-suites it supports, and suggested compression methods. The TLS handshake's negotiation phase begins with the client initiating communication using a "ClientHello" message. This message is crucial as it sets the stage for secure communication. It does not include the "ClientKeyExchange" message; that comes later. Crucially, the ClientHello lists the TLS versions the client is capable of supporting, allowing the server to select a mutually compatible version. It also provides a list of cipher suites, combinations of encryption algorithms, hash functions, and key exchange methods, that the client is willing to use for the secure connection. Furthermore, if supported, the client may suggest compression methods to reduce the data transfer size. This exchange allows both parties to agree on the highest level of security and performance they can achieve together. Options A and D are incorrect because "ClientStart" is not a valid message in the TLS handshake, and D also incorrectly includes
"ClientKeyExchange" in this initial message. Option B is incorrect because the name of the message is

"ClientHello" not "ClientStart". The negotiation phase is about establishing common grounds, not about already exchanging keys, therefore "ClientKeyExchange" is a later step.

Further Research:

Cloudflare Learning Center - What is a TLS handshake?: https://www.cloudflare.com/learning/ssl/what-is-a-tls-handshake/
Wikipedia - Transport Layer Security: https://en.wikipedia.org/wiki/Transport_Layer_Security
IBM - TLS handshake: https://www.ibm.com/docs/en/zvm/7.3?topic=security-tls-handshake

Question: 53



Severity	Date	Time	Sig ID	Source IP	Source Port	Dest IP	Dest Port	Description
6	Jan 15 2020	05:15:22	33883	62.5.22.54	22557	198.168.5.22	53	*

Refer to the exhibit. Which type of log is displayed?

A.IDS
B.proxy
C.NetFlow
D.sys

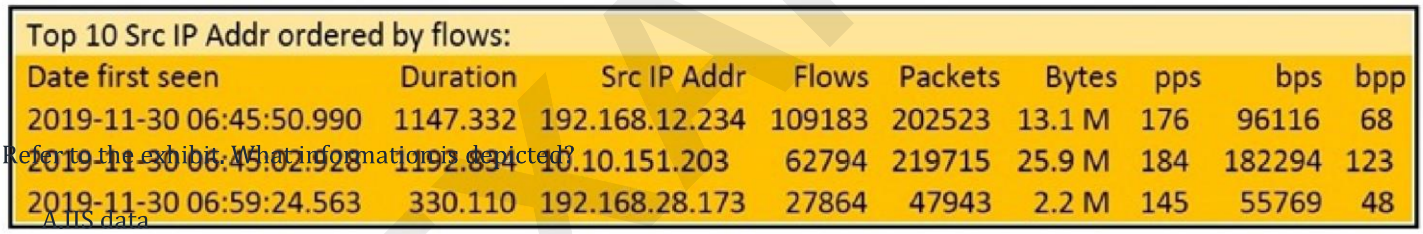
Answer: A

Explanation:

"Sig ID" typically refers to a Signature ID, which is a unique identifier assigned to a particular security threat or event by an intrusion detection or prevention system (IDS/IPS). A log message that includes a Sig ID would suggest that the message is related to an alert triggered by the IDS/IPS in response to a security event.

IDS and firewalls uses signatures.

Question: 54



Top 10 Src IP Addr ordered by flows:

Date first seen	Duration	Src IP Addr	Flows	Packets	Bytes	pps	bps	bpp
2019-11-30 06:45:50.990	1147.332	192.168.12.234	109183	202523	13.1 M	176	96116	68
2019-11-30 06:45:02.928	1192.834	10.10.151.203	62794	219715	25.9 M	184	182294	123
2019-11-30 06:59:24.563	330.110	192.168.28.173	27864	47943	2.2 M	145	55769	48

Refer to the exhibit. What information is depicted?

A.IIS data
B.NetFlow data
C.network discovery event
D.IPS event data

Answer: B

Explanation:

Correct answer is B:.NetFlow data.

Question: 55

What is the difference between the ACK flag and the RST flag in the NetFlow log session?

A. The RST flag confirms the beginning of the TCP connection, and the ACK flag responds when the data for the payload is complete

B. The ACK flag confirms the beginning of the TCP connection, and the RST flag responds when the data for the payload is complete

C. The RST flag confirms the receipt of the prior segment, and the ACK flag allows for the spontaneous termination of a connection

D. The ACK flag confirms the receipt of the prior segment, and the RST flag allows for the spontaneous termination of a connection

Answer: D

Explanation:

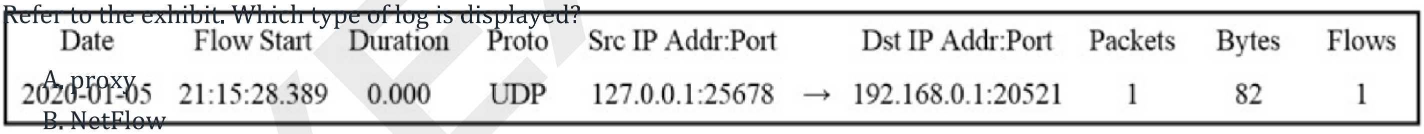
Let's break down the TCP flags ACK and RST within the context of NetFlow logs and their significance in network communication. The TCP (Transmission Control Protocol) header includes control flags that manage the state and flow of a connection. The ACK (Acknowledgment) flag, when set, indicates that the sending device has successfully received the previous TCP segment. It signifies that the receiver has got the data and is acknowledging it, progressing the conversation forward. On the other hand, the RST (Reset) flag signals an abrupt termination of a TCP connection. This forceful termination usually occurs due to a problem, such as a connection timeout or invalid data. Within a NetFlow session log, these flags play a crucial role in
understanding the nature of TCP traffic. The ACK flag would appear in segments involved in the typical three-way handshake and subsequent data exchange. The RST flag, conversely, would indicate a connection was forcibly closed rather than closed gracefully. Therefore, option D correctly states that the ACK flag confirms the receipt of the prior segment and the RST flag allows for the spontaneous termination of a connection. The other options invert the meanings or apply the flags incorrectly to connection initiation and data completion, which is inaccurate. Option A, B and C are not aligned with the specific function of the ACK and RST flag.

Further resources can be found at:

Cisco Documentation on TCP Flags:https://www.cisco.com/c/en/us/support/docs/ip/transmission-control-protocol-tcp/13803-tcpflags.html
Wikipedia on TCP flags:
https://en.wikipedia.org/wiki/Transmission_Control_Protocol#TCP_segment_structure

Question: 56

Refer to the exhibit. Which type of log is displayed?



Date	Flow Start	Duration	Proto	Src IP Addr:Port		Dst IP Addr:Port	Packets	Bytes	Flows
2020-01-05	21:15:28.389	0.000	UDP	127.0.0.1:25678	→	192.168.0.1:20521	1	82	1

A. proxy

B. NetFlow

C. IDS

D. sys

Answer: B

Explanation:

Duration ==> Netflow

Question: 57

How is NetFlow different from traffic mirroring?

A. NetFlow collects metadata and traffic mirroring clones data.
B. Traffic mirroring impacts switch performance and NetFlow does not.
C. Traffic mirroring costs less to operate than NetFlow.
D. NetFlow generates more data than traffic mirroring.

Answer: A

Explanation:

The correct answer is **A. NetFlow collects metadata and traffic mirroring clones data.** This accurately distinguishes the core functional difference between the two technologies. NetFlow, a network protocol developed by Cisco, operates by collecting and exporting summaries or metadata about network traffic flows.

It doesn't capture the entire packet content; rather, it aggregates information like source/destination IP addresses, ports, protocol, and bytes/packets transferred within a specific flow. This summary data is then sent to a NetFlow collector for analysis, allowing for traffic monitoring, anomaly detection, and capacity planning.

Traffic mirroring, often implemented through SPAN (Switched Port Analyzer) or port mirroring, on the other hand, creates a complete copy (clone) of network traffic passing through a specific port or VLAN. This mirrored traffic is then sent to a monitoring device for in-depth analysis, often used for security analysis, intrusion detection, and debugging. The mirrored data contains the full packet payload, allowing for granular inspection.

Option B is partially correct, as traffic mirroring can impact switch performance due to the added overhead of copying packets. However, NetFlow can also cause resource usage on routers generating the metadata.

Option C is incorrect; generally, NetFlow infrastructure might be lower in operation cost than dedicated mirroring infrastructure due to its less bandwidth-intensive nature. Finally, Option D is also incorrect, because traffic mirroring generates significantly more data due to copying the entire packet content compared to the summaries provided by NetFlow.

In summary, NetFlow provides flow-based statistics while traffic mirroring provides full copies, each serving different monitoring purposes with different resource implications.

Authoritative Links for Further Research:

Cisco NetFlow:https://www.cisco.com/c/en/us/products/ios-nx-os-software/ios-netflow/index.html
Traffic Mirroring/SPAN:
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2_55_se/configuration/guide/scg2960/swspan.html

Question: 58

What makes HTTPS traffic difficult to monitor?

A. SSL interception

B. packet header size

C. signature detection time

D. encryption

Answer: D

Explanation:

The correct answer is **D. encryption**. HTTPS traffic is inherently difficult to monitor primarily due to its use of encryption protocols, such as TLS (Transport Layer Security). Encryption transforms data into an unreadable format, preventing direct inspection of the content by network monitoring devices. While techniques like SSL/TLS interception (option A) exist, they add complexity and can introduce security risks themselves. The packet header size (option B) doesn't impede monitoring; headers are typically unencrypted and provide routing information. Signature detection time (option C) is relevant to identifying known malicious patterns but is not the primary challenge with HTTPS. Encryption conceals the actual data exchanged within the HTTPS connection. Network monitoring tools, without decryption, can only observe encrypted packets, making it hard to understand the application-level details or detect any malicious content that may be present. This lack of visibility into encrypted payloads poses a significant hurdle for traditional security monitoring systems. Interception methods, if applied improperly, can lead to man-in-the-middle attacks, underscoring the inherent difficulties in dealing with encrypted traffic.

Authoritative links:

1. **Cloudflare: What is HTTPS? -** https://www.cloudflare.com/learning/ssl/what-is-https/
2. **OWASP: Transport Layer Protection Cheat Sheet -** https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Protection_Cheat_Sheet.html 3. **Akamai: Encrypted Traffic Management -** https://www.akamai.com/solutions/security/encrypted-traffic-management

Question: 59

How does an attacker observe network traffic exchanged between two users?

A. port scanning

B. man-in-the-middle

C. command injection

D. denial of service

Answer: B

Explanation:

The correct answer is **B. man-in-the-middle (MitM)**. A man-in-the-middle attack allows an attacker to intercept and potentially alter communication between two parties without either party knowing. This is achieved by positioning the attacker between the two users' network connections. The attacker essentially acts as a relay, forwarding data packets but also observing and possibly modifying them. Port scanning (A) is used to identify open ports on a system but doesn't directly enable real-time traffic observation. Command injection (C) exploits vulnerabilities to execute commands on a system and wouldn't allow for passive traffic observation of two users. Denial of Service (D) aims to disrupt service availability, not to eavesdrop on communications. In a MitM attack, the attacker might use techniques like ARP poisoning to redirect traffic through their device. They could use tools like Wireshark to passively observe the network traffic passing through. This allows the attacker to analyze the content of the communication and potentially steal sensitive information. This interception and observation of ongoing traffic is the core principle of a MitM attack making it the correct answer.

Authoritative Links for further research:

OWASP - Man-in-the-Middle Attack: https://owasp.org/www-community/attacks/Man-in-the-middle NIST - Man-in-the-Middle Attacks: https://csrc.nist.gov/glossary/term/man_in_the_middle_attack
Cisco - MitM Attack Prevention: https://www.cisco.com/c/en/us/products/security/what-is-man-in-the-middle-attack.html

Question: 60

Which type of data consists of connection level, application-specific records generated from network traffic?

A. transaction data
B. location data
C. statistical data
D. alert data

Answer: A

Explanation:

The correct answer is A. Transaction data encompasses detailed records of specific actions or interactions within a system. In the context of network security, transaction data often refers to logs generated by network devices or security tools that capture the specifics of a connection. These records can include source and destination IP addresses, ports used, protocols involved, and timestamps of the connection's initiation and termination. This level of granularity allows for a deep dive into network activity, aiding in the identification of anomalies or malicious behavior. For instance, a web server log detailing each HTTP request is a form of transaction data. Similarly, a firewall log capturing every accepted or blocked connection is another example.

This data is crucial for incident response and forensic analysis because it provides a chronological record of events. Option B, location data, refers to geographic coordinates. Option C, statistical data, summarizes aggregated information, not individual events. Option D, alert data, indicates triggers for potential issues but doesn't inherently provide the detailed context of each connection. Transaction data, therefore, best fits the description of connection-level, application-specific records.

Further research can be done here:

Understanding Network Logs:https://www.cloudflare.com/learning/security/glossary/network-log/
Transaction Logging:https://www.ibm.com/docs/en/cloud-paks/cp-management/22.3?topic=logging-transaction

Question: 61

An engineer receives a security alert that traffic with a known TOR exit node has occurred on the network. What is the impact of this traffic?

A.ransomware communicating after infection
B.users downloading copyrighted content
C.data exfiltration
D.user circumvention of the firewall

Answer: D

Explanation:

The correct answer is **D. user circumvention of the firewall**.

Here's why:

TOR (The Onion Router) is a network designed to anonymize internet traffic. Its exit nodes are the last points of connection before traffic reaches its destination on the public internet. When traffic is detected originating from a known TOR exit node, it signifies that a user within the network is likely attempting to bypass network restrictions or monitoring.

While TOR can be used for legitimate purposes, such as protecting user privacy, its ability to anonymize traffic makes it a common tool for circumventing security controls. For example, a user might utilize TOR to access websites blocked by the company firewall, or to bypass web content filtering.

The other options are less directly linked to TOR exit node traffic:

A. ransomware communicating after infection: While ransomware could use TOR to communicate with command-and-control servers, the detection of a TOR exit node alone doesn't specifically indicate ransomware activity. Other signs of compromise are usually required.

B. users downloading copyrighted content: While TOR can mask activities, simply using a TOR exit node doesn't confirm copyright infringement. Users use TOR for various purposes.

C. data exfiltration: While TOR can be used for data exfiltration, the detection of a TOR exit node doesn't necessarily mean that exfiltration is happening. TOR simply provides an anonymous pathway.

In summary, the most direct impact of traffic originating from a TOR exit node is that it bypasses the network's firewall and visibility, which is the essence of **user circumvention of the firewall**. It represents a security risk because the firewall is a critical component of network security. This circumvention is a violation of the intended security posture.

Authoritative Links:

The Tor Project:https://www.torproject.org/ (Official site for information on TOR)
SANS Institute on TOR:https://www.sans.org/blog/tor-anonymity-network-detection-techniques/ **NIST Special Publication 800-47 - Security Guide for Outsourcing Information Technology Services:** https://csrc.nist.gov/publications/detail/sp/800-47/final (Though not TOR specific, this highlights the importance of managing user circumvention of controls in cloud environments)

Question: 62

What is an example of social engineering attacks?

A.receiving an unexpected email from an unknown person with an attachment from someone in the same company

B.receiving an email from human resources requesting a visit to their secure website to update contact information

C.sending a verbal request to an administrator who knows how to change an account password

D.receiving an invitation to the department's weekly WebEx meeting

Answer: A

Explanation:

The correct answer is **A.** Here's why:

Social engineering attacks exploit human psychology to manipulate individuals into divulging confidential information or performing actions that benefit the attacker. Option A, "receiving an unexpected email from an unknown person with an attachment from someone in the same company," perfectly exemplifies this. The attacker uses a tactic called "spoofing" to make the email appear legitimate, often by mimicking internal communication styles and exploiting existing trust within an organization. The attachment likely contains malicious software designed to compromise the victim's system or steal sensitive data. This leverages the victim's tendency to trust communications from colleagues, even if slightly out of the ordinary.

Option B, while seemingly innocuous, could also be a form of phishing, a type of social engineering attack. However, without more context, it's not as clear cut as Option A. It's very likely a phishing attack if the link is not directly to the genuine human resources website.

Option C involves a direct verbal request, which isn't typically classified as social engineering, but it is an example of trickery that relies on personal interactions. While manipulation is involved, it’s not typically the focus of most social engineering discussions.

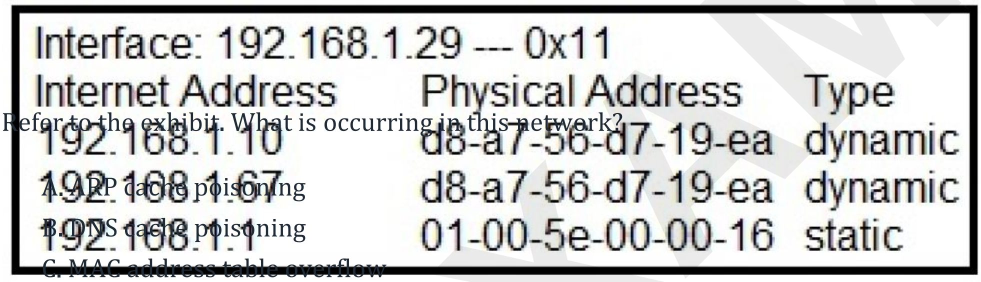
Option D, receiving an invitation to a scheduled WebEx meeting, is a routine communication and does not exhibit traits of a social engineering attack unless malicious intent can be shown, such as a hijacked meeting link.

Therefore, the clearest and most direct example of social engineering among the options is receiving a seemingly legitimate, but ultimately malicious, email with an attachment from an unknown person within the same company (Option A). This scenario preys on the victim's trust and lack of suspicion, aligning directly with common social engineering tactics.

For further research, consider these resources:

NIST (National Institute of Standards and Technology) Special Publication 800-53: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
SANS Institute: https://www.sans.org/ (search for social engineering resources)
OWASP (Open Web Application Security Project): https://owasp.org/ (search for social engineering and phishing)

Question: 63



```
Interface: 192.168.1.29 --- 0x11
Internet Address      Physical Address     Type
192.168.1.10          d8-a7-56-d7-19-ea    dynamic
192.168.1.67          d8-a7-56-d7-19-ea    dynamic
192.168.1.1           01-00-5e-00-00-16    static
```

Refer to the exhibit. What is occurring in this network?

A. ARP cache poisoning
B. DNS cache poisoning
C. MAC address table overflow
D. MAC flooding attack

Answer: A

Explanation:

ARP Spoofing

Also known as ARP poisoning, is a Man in the Middle (MitM) attack that allows attackers to intercept communication between network devices.

The attack works as follows:

The attacker must have access to the network. They scan the network to determine the IP addresses of at least two devices.

The attacker uses a spoofing tool such as Arpspoof or Driftnet, to send out forged ARP responses.

The forged responses advertise that the correct MAC address for both IP addresses, belonging to the router and workstation, is the attacker's MAC address. This fools both router and workstation to connect to the attacker's machine, instead of to each other.

The two devices update their ARP cache entries and from that point onwards, communicate with the attacker instead of directly with each other.

The attacker is now secretly in the middle of all communications.

https://www.imperva.com/learn/application-security/arp-spoofing/

Question: 64

Which data format is the most efficient to build a baseline of traffic seen over an extended period of time?

A.syslog messages
B.full packet capture
C.NetFlow
D.firewall event logs

Answer: C

Explanation:

The most efficient data format for establishing a long-term traffic baseline is NetFlow (C). Here's why: NetFlow provides summarized flow data, capturing key details like source and destination IP addresses, ports, protocols, and packet counts. This aggregation drastically reduces the volume of data compared to full packet captures. Full packet captures (B), while offering rich detail, generate massive storage and processing overhead, making them impractical for long-term baseline creation. Syslog messages (A) and firewall event logs (D) primarily focus on system events and security incidents, not comprehensive network traffic characteristics needed for baseline establishment. NetFlow's compact format enables efficient storage and analysis over extended periods, facilitating anomaly detection and identification of deviations from normal traffic patterns. By focusing on flow summaries rather than every packet, NetFlow provides a practical balance between detail and manageability for long-term traffic baselining. It allows network administrators and security analysts to easily recognize abnormal traffic spikes or shifts in communication patterns over time, a crucial aspect of cybersecurity operations. Furthermore, NetFlow is supported by a broad range of networking devices, making it readily available.

Authoritative Links:

1. Cisco on Netflow: https://www.cisco.com/c/en/us/solutions/enterprise-networks/netflow/index.html 2. Network World article on Netflow: https://www.networkworld.com/article/2224335/lan-wan/what-is-netflow--how-does-it-work-and-what-can-it-do.html

Question: 65

Which action prevents buffer overflow attacks?

A.variable randomization

B.using web based applications

C.input validation

D.using a Linux operating system

Answer: C

Explanation:

The correct answer is **C. input validation.** Buffer overflow attacks occur when a program attempts to write data beyond the allocated buffer's memory boundaries, potentially overwriting adjacent memory locations and causing crashes or allowing malicious code execution. Input validation directly addresses this vulnerability by checking the size and format of user-supplied data before it's written into a buffer. By verifying that input does not exceed the buffer's capacity, input validation prevents the overflow from happening. Variable randomization (A) might add some obfuscation, but doesn't inherently prevent overflows; it primarily hinders exploit predictability. Using web-based applications (B) is not a direct countermeasure against overflows and, in fact, web applications are often vulnerable to this type of attack if not properly coded. Using a Linux operating system (D) doesn't eliminate the risk of buffer overflows; they can exist in code running on any OS. Input validation at the application layer is crucial, regardless of the underlying system. Therefore, input validation is the most effective strategy directly targeting the root cause of buffer overflow vulnerabilities. Effective input validation should cover checks on data length, type, and valid ranges.

Further Research:

1. **OWASP Input Validation Cheat Sheet:** https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html - Provides a comprehensive guide on implementing input validation.
2. **CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer:** https://cwe.mitre.org/data/definitions/119.html - MITRE's definition of buffer overflows, including vulnerabilities and mitigations.
3. **Wikipedia - Buffer overflow:**https://en.wikipedia.org/wiki/Buffer_overflow - Detailed explanation of buffer overflow attacks and their mechanisms.

Question: 66

Which type of attack occurs when an attacker is successful in eavesdropping on a conversation between two IP phones?

A.known-plaintext

B.replay

C.dictionary

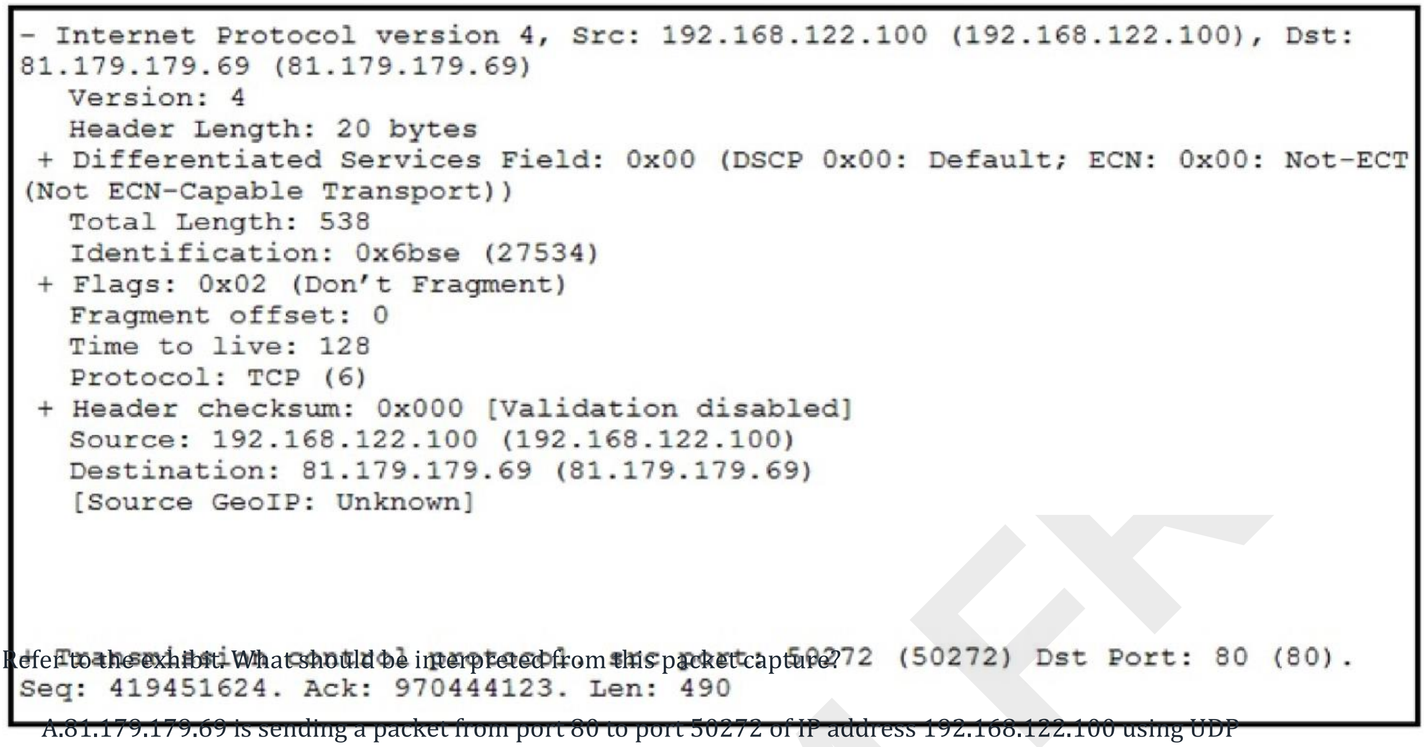
D.man-in-the-middle

Answer: D

Explanation:

The correct answer is D, man-in-the-middle (MitM) attack. A man-in-the-middle attack involves an attacker intercepting and potentially altering communications between two parties without their knowledge. In this specific scenario, the attacker positions themselves between the two IP phones, listening to the conversation, effectively acting as an intermediary. This direct interception of real-time communication is a hallmark of MitM attacks. The other options are less applicable: known-plaintext attacks are used in cryptography when the attacker has both the plaintext and the ciphertext of a message; replay attacks involve re-transmitting captured network traffic; and dictionary attacks are a form of password cracking using a list of common words. The key element of this question is the real-time eavesdropping, which aligns perfectly with the MitM attack concept. This attack can compromise the confidentiality of the conversation. For further research, consider these resources: OWASP Man in the Middle, Cisco's explanation of MitM attacks, and SANS Institute on MitM attacks.

Question: 67



```
- Internet Protocol version 4, Src: 192.168.122.100 (192.168.122.100), Dst:
81.179.179.69 (81.179.179.69)
   Version: 4
   Header Length: 20 bytes
 + Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT
(Not ECN-Capable Transport))
   Total Length: 538
   Identification: 0x6bse (27534)
 + Flags: 0x02 (Don't Fragment)
   Fragment offset: 0
   Time to live: 128
   Protocol: TCP (6)
 + Header checksum: 0x000 [Validation disabled]
   Source: 192.168.122.100 (192.168.122.100)
   Destination: 81.179.179.69 (81.179.179.69)
   [Source GeoIP: Unknown]



+ Transmission control protocol, src port: 50272 (50272) Dst Port: 80 (80).
Seq: 419451624. Ack: 970444123. Len: 490
```

Refer to the exhibit. What should be interpreted from this packet capture?

A.81.179.179.69 is sending a packet from port 80 to port 50272 of IP address 192.168.122.100 using UDP protocol.

B.192.168.122.100 is sending a packet from port 50272 to port 80 of IP address 81.179.179.69 using TCP protocol.

C.192.168.122.100 is sending a packet from port 80 to port 50272 of IP address 81.179.179.69 using UDP protocol.

D.81.179.179.69 is sending a packet from port 50272 to port 80 of IP address 192.168.122.100 using TCP protocol.

Answer: B

Explanation:

b is correct tcp protoco; has flag and segment offset

Question: 68

What are the two characteristics of the full packet captures? (Choose two.)

A.Identifying network loops and collision domains.
B.Troubleshooting the cause of security and performance issues.
C.Reassembling fragmented traffic from raw data.
D.Detecting common hardware faults and identify faulty assets.
E.Providing a historical record of a network transaction.

Answer: BE

Explanation:

Okay, let's break down why options B and E are the correct characteristics of full packet captures and why the others are not.

Full packet captures, also known as PCAPs, are essentially recordings of all network traffic traversing a specific point on a network. They capture the entire data payload of each packet, not just header information. This rich data provides vital capabilities for network analysis and security investigations.

Option B is correct: Troubleshooting security and performance issues is a primary use case for full packet captures. By examining the contents of packets, analysts can identify anomalies, diagnose latency problems, and pinpoint the root cause of network slowdowns or security incidents. They can trace the path of packets, identify communication failures, and reconstruct events. For example, if a web application is slow, a PCAP can reveal if the delay is due to the network or the application itself.

Option E is correct: Full packet captures create a detailed historical record of network transactions. This is crucial for forensic analysis after a security breach. Investigators can replay past communications, analyze the sequence of events, and determine how attackers penetrated a system or compromised data. This history also helps understand normal network behavior, making it easier to identify deviations that might indicate malicious activity.

Option A is incorrect: Identifying network loops and collision domains are typically handled by network discovery tools and protocols like Spanning Tree Protocol (STP) and are not the focus of PCAPs. PCAPs capture traffic, not network topology information directly.

Option C is incorrect: While full packet captures contain the raw data, the capture itself doesn't perform the reassembly of fragmented packets. Reassembly happens at the receiving device's network stack. Packet capture software presents the raw data and subsequent analysis tools can reassemble fragments, but the capture itself is focused on recording all traffic as it occurs.

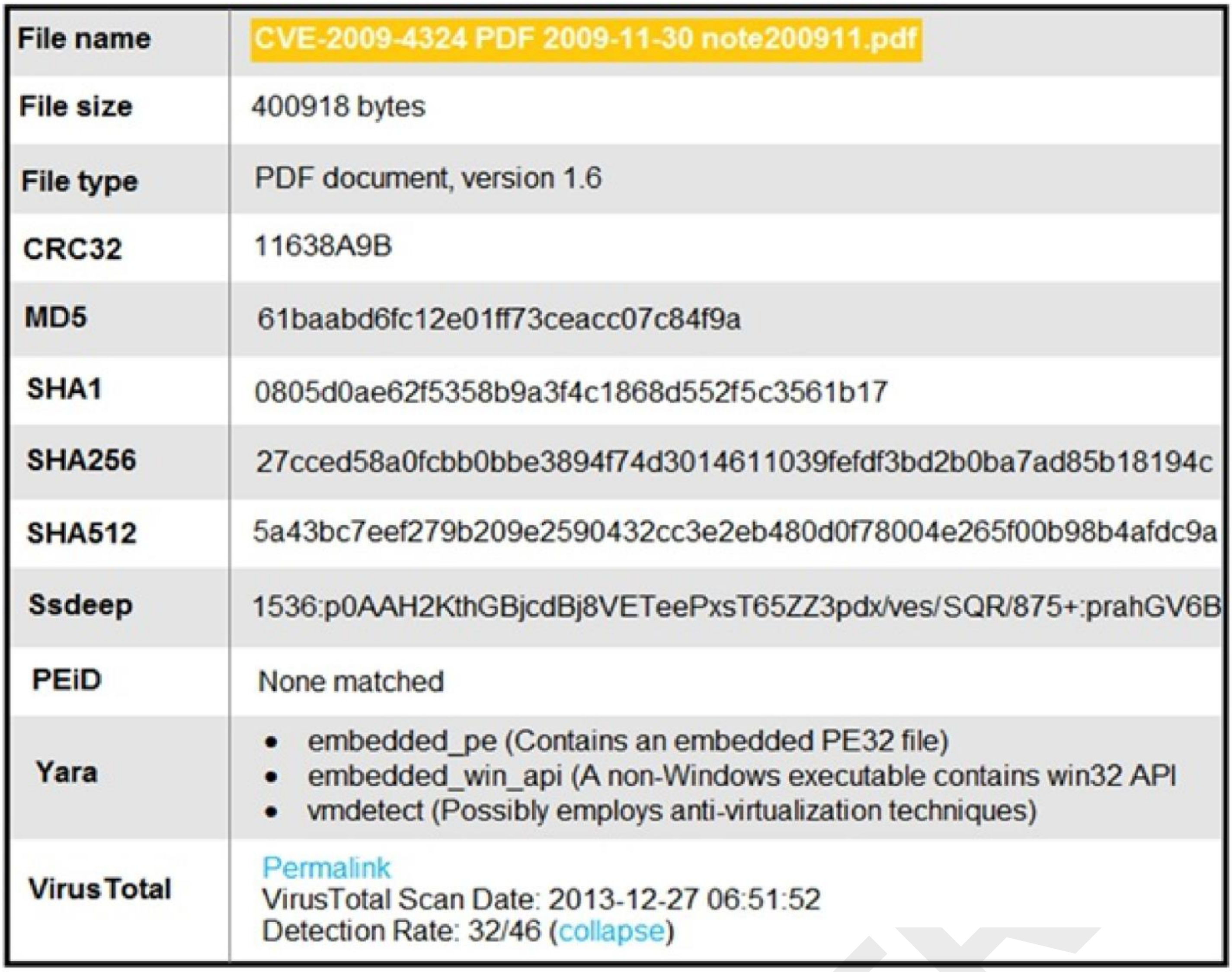
Option D is incorrect: PCAPs focus on network traffic and are not designed to detect hardware faults. Hardware monitoring tools are used to find faulty assets, not packet captures.

In summary, the core value of full packet captures lies in their ability to provide a granular, historical record of network traffic. This enables deep-dive troubleshooting of security incidents and performance issues.

Authoritative links for further research:

Wireshark: The de facto standard for network packet analysis: https://www.wireshark.org/
SANS Institute: Offers courses on network forensics and packet analysis, check: https://www.sans.org/ **Cisco's official documentation** on network security and packet capture: https://www.cisco.com/c/en/us/support/index.html

Question: 69



File name	CVE-2009-4324 PDF 2009-11-30 note200911.pdf
File size	400918 bytes
File type	PDF document, version 1.6
CRC32	11638A9B
MD5	61baabd6fc12e01ff73ceacc07c84f9a
SHA1	0805d0ae62f5358b9a3f4c1868d552f5c3561b17
SHA256	27cced58a0fcbb0bbe3894f74d3014611039fefdf3bd2b0ba7ad85b18194c
SHA512	5a43bc7eef279b209e2590432cc3e2eb480d0f78004e265f00b98b4afdc9a
Ssdeep	1536:p0AAH2KthGBjcdBj8VETeePxsT65ZZ3pdx/ves/SQR/875+:prahGV6B
PEiD	None matched
Yara	• embedded_pe (Contains an embedded PE32 file) • embedded_win_api (A non-Windows executable contains win32 API • vmdetect (Possibly employs anti-virtualization techniques)
VirusTotal	Permalink VirusTotal Scan Date: 2013-12-27 06:51:52 Detection Rate: 32/46 (collapse)

Refer to the exhibit. An engineer is analyzing this Cuckoo Sandbox report for a PDF file that has been downloaded from an email. What is the state of this file?

A.The file has an embedded executable and was matched by PEiD threat signatures for further analysis.

B.The file has an embedded non-Windows executable but no suspicious features are identified.

C.The file has an embedded Windows 32 executable and the Yara field lists suspicious features for further analysis.

D.The file was matched by PEiD threat signatures but no suspicious features are identified since the signature list is up to date.

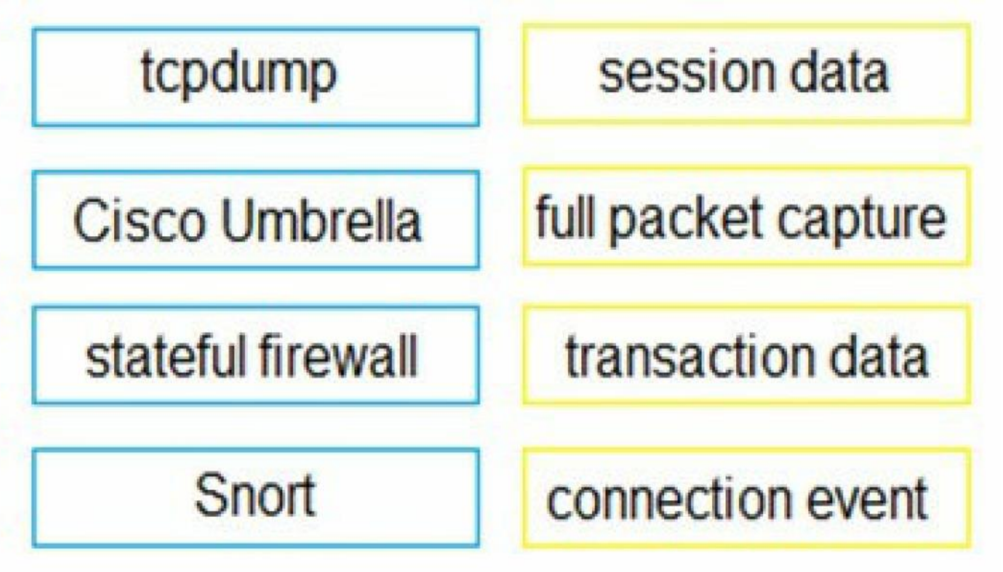
Answer: C

Explanation:

The file has an embedded Windows 32 executable and the Yara field lists suspicious features for further analysis.

Question: 70

DRAG DROP -
Drag and drop the technology on the left onto the data type the technology provides on the right.
Select and Place:



tcpdump

session data

Cisco Umbrella

full packet capture

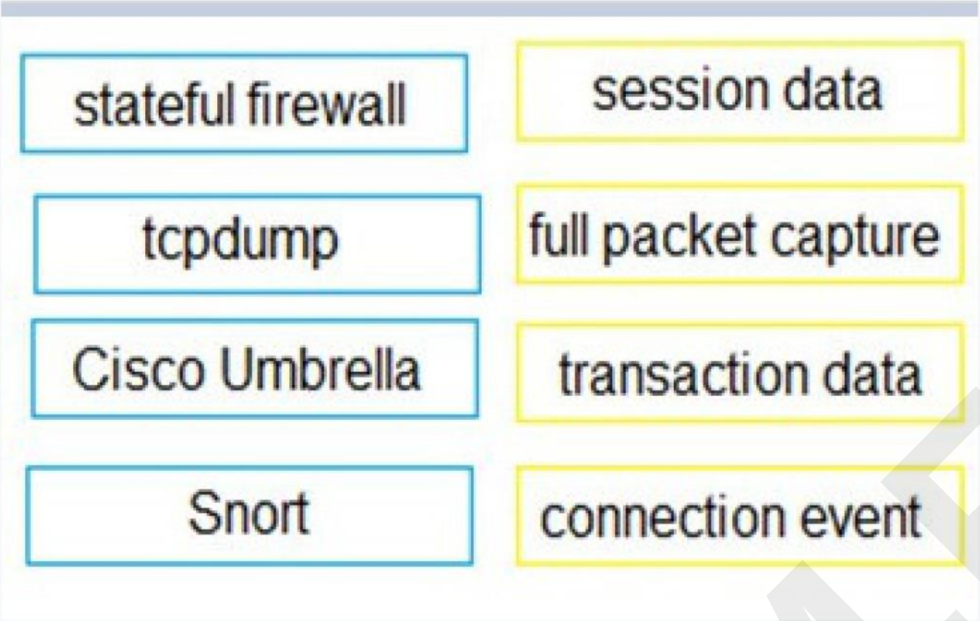
stateful firewall

transaction data

Snort

connection event

Answer:



stateful firewall

session data

tcpdump

full packet capture

Cisco Umbrella

transaction data

Snort

connection event

Explanation:

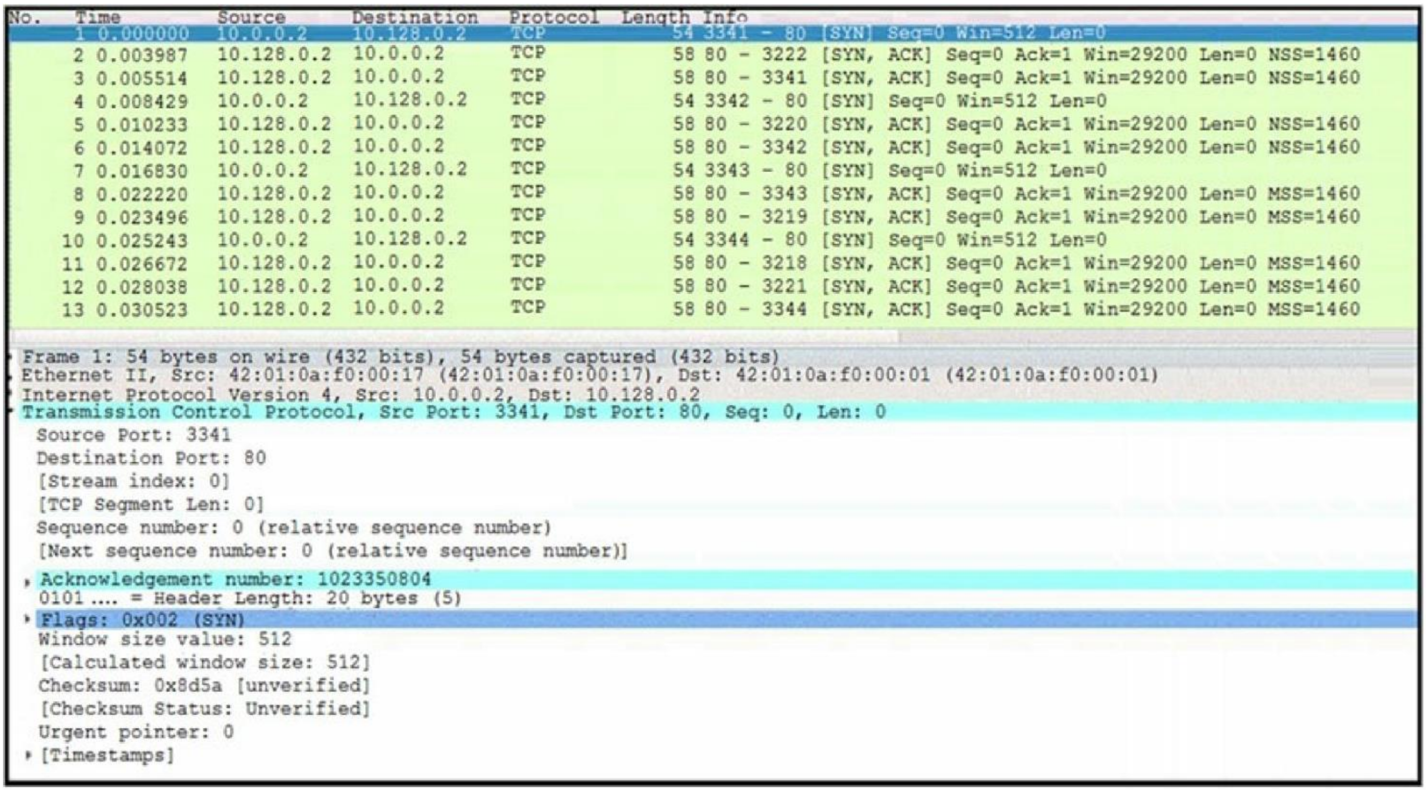
session data --> Statefull Firewall

full packet capt --> tcpdump

transaction data --> Cisco Umbrellac

onnection event --> Snort.

Question: 71



```
No.   Time       Source      Destination  Protocol  Length Info
    1 0.000000   10.0.0.2    10.128.0.2   TCP          54 3341 - 80 [SYN] Seq=0 Win=512 Len=0
    2 0.003987   10.128.0.2  10.0.0.2     TCP          58 80 - 3222 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 NSS=1460
    3 0.005514   10.128.0.2  10.0.0.2     TCP          58 80 - 3341 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 NSS=1460
    4 0.008429   10.0.0.2    10.128.0.2   TCP          54 3342 - 80 [SYN] Seq=0 Win=512 Len=0
    5 0.010233   10.128.0.2  10.0.0.2     TCP          58 80 - 3220 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 NSS=1460
    6 0.014072   10.128.0.2  10.0.0.2     TCP          58 80 - 3342 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 NSS=1460
    7 0.016830   10.0.0.2    10.128.0.2   TCP          54 3343 - 80 [SYN] Seq=0 Win=512 Len=0
    8 0.022220   10.128.0.2  10.0.0.2     TCP          58 80 - 3343 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
    9 0.023496   10.128.0.2  10.0.0.2     TCP          58 80 - 3219 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
   10 0.025243   10.0.0.2    10.128.0.2   TCP          54 3344 - 80 [SYN] Seq=0 Win=512 Len=0
   11 0.026672   10.128.0.2  10.0.0.2     TCP          58 80 - 3218 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
   12 0.028038   10.128.0.2  10.0.0.2     TCP          58 80 - 3221 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
   13 0.030523   10.128.0.2  10.0.0.2     TCP          58 80 - 3344 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460

Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
Ethernet II, Src: 42:01:0a:f0:00:17 (42:01:0a:f0:00:17), Dst: 42:01:0a:f0:00:01 (42:01:0a:f0:00:01)
Internet Protocol Version 4, Src: 10.0.0.2, Dst: 10.128.0.2
Transmission Control Protocol, Src Port: 3341, Dst Port: 80, Seq: 0, Len: 0
  Source Port: 3341
  Destination Port: 80
  [Stream index: 0]
  [TCP Segment Len: 0]
  Sequence number: 0 (relative sequence number)
  [Next sequence number: 0 (relative sequence number)]
 ▸ Acknowledgement number: 1023350804
  0101 .... = Header Length: 20 bytes (5)
 ▸ Flags: 0x002 (SYN)
  Window size value: 512
  [Calculated window size: 512]
  Checksum: 0x8d5a [unverified]
  [Checksum Status: Unverified]
  Urgent pointer: 0
 ▸ [Timestamps]
```

Refer to the exhibit. What is occurring in this network traffic?

A. High rate of SYN packets being sent from a multiple source towards a single destination IP. B. High rate of ACK packets being sent from a single source IP towards multiple destination IPs. C. Flood of ACK packets coming from a single source IP to multiple destination IPs.

D. Flood of SYN packets coming from a single source IP to a single destination IP.

Answer: D

Explanation:

The correct answer:D. Flood of SYN packets coming from a single source IP to a single destination IP.

Question: 72

An engineer needs to have visibility on TCP bandwidth usage, response time, and latency, combined with deep packet inspection to identify unknown software by its network traffic flow. Which two features of Cisco Application Visibility and Control should the engineer use to accomplish this goal? (Choose two.)

A.management and reporting
B.traffic filtering
C.adaptive AVC
D.metrics collection and exporting
E.application recognition

Answer: DE

Explanation:

The correct answer is **D. metrics collection and exporting** and **E. application recognition**. Here's why:

Application Recognition (E): Deep packet inspection (DPI) is crucial for identifying unknown software. Application recognition, a core feature of Cisco AVC, uses DPI to examine the packet payload, not just headers. By analyzing traffic patterns and signatures within the packets, AVC can identify applications, including those not easily recognized by port numbers or protocols. This allows identification of unknown software based on their specific network traffic characteristics.

Metrics Collection and Exporting (D): The engineer needs visibility on TCP bandwidth usage, response time, and latency. AVC's metrics collection feature gathers precisely this data. It tracks application performance metrics, including throughput, delay, and packet loss, which directly correspond to bandwidth usage, response time, and latency. Furthermore, the exporting function of AVC lets this collected data be shared with other monitoring tools or dashboards for visualization and further analysis. It enables the engineer to monitor performance and make informed decisions based on TCP bandwidth usage, response time, and latency, as requested in the scenario.

Why other options are incorrect:

A. management and reporting: While important for the overall operation of AVC, this feature doesn't directly address the core requirements of DPI for unknown software detection or collecting TCP metrics.

B. traffic filtering: This is used to manipulate or control what traffic is subject to inspection, but doesn't itself provide the deep inspection or collection of TCP metrics the question requires.

C. adaptive AVC: While offering automated adaptation, this option doesn't on its own provide visibility on TCP metrics or handle deep inspection to identify unknown software.

In summary, **application recognition** provides the DPI capability to identify unknown software, while **metrics collection and exporting** provides the necessary visibility on TCP performance parameters. Both are essential to fulfill the requirements outlined in the scenario.

Authoritative Links:

Cisco Application Visibility and Control:https://www.cisco.com/c/en/us/solutions/enterprise-networks/application-visibility-control/index.html
Deep Packet Inspection:https://www.fortinet.com/resources/cyberglossary/deep-packet-inspection

Question: 73

Which security technology guarantees the integrity and authenticity of all messages transferred to and from a web application?

A.Hypertext Transfer Protocol
B.SSL Certificate
C.Tunneling
D.VPN

Answer: B

Explanation:

The correct answer is B, SSL Certificate. Here's why:

SSL (Secure Sockets Layer) certificates, and their modern successor TLS (Transport Layer Security), are fundamental to securing web communications. They operate by encrypting the data exchanged between a web server and a client's browser. This encryption ensures the confidentiality of the messages, meaning that even if intercepted, the data is unreadable without the correct decryption key. More importantly for this question, SSL/TLS also provide mechanisms for message integrity and authenticity.

Integrity is guaranteed through cryptographic hash functions. When a message is transmitted, a hash is computed, and this hash is transmitted along with the encrypted message. The receiving end then computes the same hash from the received data. If the two hashes match, it proves that the message wasn't altered during transit, hence maintaining integrity. Authenticity is achieved by using public-key cryptography and the fact that a certificate is issued by a trusted certificate authority (CA). When a client connects to a web server, it receives a copy of the server's SSL/TLS certificate. This certificate contains the server's public key, and crucially, a signature from the trusted CA, which acts as a validation of the server's identity. This ensures the client is truly talking to the intended server and not a malicious impostor, thereby ensuring authenticity.

HTTP (Hypertext Transfer Protocol) by itself is an insecure protocol (Option A). Tunneling (Option C) is a technique to encapsulate a data packet within another protocol, and a VPN (Virtual Private Network) (Option D) creates a secure connection between two networks, but neither directly provides the integrity and authenticity guarantees that an SSL/TLS certificate does for web application communications.

Therefore, SSL/TLS certificates are the technology that effectively guarantees both the integrity and authenticity of messages transferred to and from web applications.

Further Research:

SSL/TLS:https://www.cloudflare.com/learning/ssl/what-is-ssl/
Public Key Cryptography:https://www.cloudflare.com/learning/encryption/what-is-public-key-cryptography/
Certificate Authority:https://www.digicert.com/blog/what-is-a-certificate-authority-ca

Question: 74

An engineer is investigating a case of the unauthorized usage of the `Tcpdump` tool. The analysis revealed that a malicious insider attempted to sniff traffic on a specific interface. What type of information did the malicious insider attempt to obtain?

A. tagged protocols being used on the network
B. all firewall alerts and resulting mitigations
C. tagged ports being used on the network
D. all information and data within the datagram

Answer: D

Explanation:

The correct answer is **D. all information and data within the datagram**.

Here's why: Tcpdump is a powerful command-line packet analyzer (also known as a network sniffer) that captures network traffic as it passes through a network interface. It operates by capturing and decoding the raw data packets transmitted over the network. When a user runs tcpdump on an interface, they can potentially see all the data within those packets, provided they have the necessary privileges. This includes the headers (source and destination IP addresses, port numbers, protocol information, etc.) as well as the payload – the actual data being transmitted. Therefore, a malicious insider attempting to sniff traffic using tcpdump would be trying to obtain all the information and data contained within the datagrams.

Option A is incorrect because while tcpdump can identify protocols in use, the goal is not to merely identify tagged protocols, rather access the contents of the communication. Similarly, option C is wrong; while tcpdump will show tagged ports being used, the aim is to acquire complete data, not solely identify port usage.
Option B is incorrect as tcpdump does not specifically deal with firewall alerts or mitigations; it operates at a lower network level capturing raw data traffic.

In summary, tcpdump's capability to intercept and display complete packet data makes it a potent tool for malicious activities like information theft, which aligns most closely with option D.

Authoritative Links:

1. **Tcpdump Official Documentation:**https://www.tcpdump.org/ - The official documentation provides detailed information on tcpdump's capabilities and usage.
2. **Wireshark Documentation (Similar Tool):**https://www.wireshark.org/docs/ - While Wireshark is a GUI tool, its underlying packet capture functionality is similar to tcpdump. The documentation is helpful in understanding packet capture concepts.
3. **Cisco Security Documentation:**https://www.cisco.com/c/en/us/solutions/security.html - Cisco's security documentation can provide broader context on network security concepts.

Question: 75

At a company party a guest asks questions about the company's user account format and password complexity. How is this type of conversation classified?

A.Phishing attack

B.Password Revelation Strategy

C.Piggybacking

D.Social Engineering

Answer: D

Explanation:

The correct answer is D, Social Engineering. Social engineering is a manipulation technique that exploits human trust and behavior to gain access to sensitive information or systems. In this scenario, the guest is using casual conversation to subtly extract information about the company's user account format and password complexity policies. This information, if obtained, could be used in a later attack. The guest is not trying to gain physical access (piggybacking), nor are they using digital communications to trick users (phishing). A password revelation strategy wouldn't be a type of conversation, it would be a process a company might use. Therefore, the most apt classification for this type of conversation is social engineering, which aligns perfectly with the manipulative nature of the interaction. The guest is leveraging trust and curiosity to gather valuable security-related data.

For further reading, explore resources on social engineering:

National Institute of Standards and Technology (NIST) Special Publication 800-53:
https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final (Search for "Social Engineering" within the document)
SANS Institute:https://www.sans.org/information-security-training/social-engineering-security-awareness-s440/
OWASP:https://owasp.org/www-project-top-ten/ (Often mentions social engineering in the context of application security vulnerabilities)

Question: 76

Which security monitoring data type requires the largest storage space?

A.transaction data

B.statistical data

C.session data

D.full packet capture

Answer: D

Explanation:

Full packet capture (FPC), also known as PCAP, requires the largest storage space compared to other security monitoring data types like transaction, statistical, and session data. FPC involves capturing and storing every single packet traversing a network. This includes all headers, payload, and metadata, providing a complete record of network activity. The sheer volume of data generated by FPC is significantly higher than other data types, as every communication, regardless of size, is preserved in its raw form. Transaction data, on the other hand, focuses on high-level details of actions, such as successful logins or financial transfers, rather than individual network packets. Statistical data aggregates information over time, reducing granularity and storage requirements further. Session data, while more detailed than transaction or statistical data, still only captures the communication parameters and states between two endpoints during a specific connection. The granularity and completeness of FPC directly translate to massive storage needs, often necessitating dedicated storage infrastructure and data retention policies. Cloud platforms offer solutions for storing FPC data using object storage or dedicated storage services. Proper management, indexing and retention is critical in order to control the costs associated with FPC. While FPC's size can be a challenge, the ability to analyze the minutia of network traffic is vital in advanced threat hunting, incident response and security investigations.

Here are some authoritative links for further research:

Cisco's CBROPS Overview:https://www.cisco.com/c/en/us/training-events/training-certifications/exams/current-list/cbrops.html
SANS Institute: Packet Analysis:https://www.sans.org/cyber-security-courses/network-packet-analysis/ **Cloud Storage Options for Packet Capture:** (search cloud provider sites, such as AWS, Azure or GCP for object storage and cold storage options)

Question: 77

What are two denial of service attacks? (Choose two.)

A.MITM
B.TCP connections
C.ping of death
D.UDP flooding
E.code red

Answer: CD

Explanation:

The correct answers are C and D: Ping of Death and UDP Flooding are both well-known denial-of-service (DoS) attacks. A Ping of Death attack exploits the Internet Control Message Protocol (ICMP) by sending oversized ping packets. When a target system receives such a large packet, it can crash or become unstable due to buffer overflow issues, rendering it unavailable to legitimate users. UDP flooding, on the other hand, overwhelms the victim server with a large volume of User Datagram Protocol (UDP) packets. The server attempts to process these packets, rapidly exhausting its resources (CPU, memory, bandwidth), thereby making the server unresponsive.

Option A, MITM (Man-in-the-Middle), is a type of attack where an attacker intercepts communication between two parties. While it compromises security, it is not a DoS attack. Option B, TCP connections, while fundamental to networking, aren't themselves a DoS attack but rather a mechanism often used in other DoS attacks (e.g. SYN flood). Option E, Code Red, refers to a specific computer worm, not a general category of DoS attack. Therefore, only options C (Ping of Death) and D (UDP flooding) accurately represent denial of service attacks. These DoS attacks aim to disrupt services and deny legitimate users access by exhausting system resources.

Supporting links:

Ping of Death: Cloudflare explanation of Ping of Death attacks.
UDP Flooding: Imperva details on UDP flood attacks.
Denial-of-Service Attack: OWASP page on DoS attacks.

Question: 78

An engineer needs to discover alive hosts within the 192.168.1.0/24 range without triggering intrusive portscan alerts on the IDS device using Nmap. Which command will accomplish this goal?

A.nmap --top-ports 192.168.1.0/24
B.nmap "sP 192.168.1.0/24
C.nmap -sL 192.168.1.0/24
D.nmap -sV 192.168.1.0/24

Answer: B

Explanation:

The correct answer is **B. nmap -sP 192.168.1.0/24**.

Here's a detailed justification:

The goal is to identify active hosts within the 192.168.1.0/24 network without triggering intrusion detection system (IDS) alerts associated with port scanning. This requires a less aggressive host discovery method.

nmap -sP (or nmap -sn): This command option instructs Nmap to perform a "ping scan" (also called a host discovery scan). It sends ICMP echo requests (pings) to each IP address within the target range. If a host responds to the ping, Nmap considers it to be "up" and reports it. Importantly, this scan type doesn't probe ports, which significantly reduces the likelihood of triggering IDS alarms that are designed to detect port scanning activity.

Option A (nmap --top-ports 192.168.1.0/24): This option performs a port scan on the most common ports of each discovered host within the range. This will trigger IDS alerts.

Option C (nmap -sL 192.168.1.0/24): The -sL option is for list scan; it only lists the IP addresses within the range and does not send any packets to verify the live status of hosts. It doesn't discover alive hosts.

Option D (nmap -sV 192.168.1.0/24): This performs version detection, which requires connecting to open ports and interacting with the services. This also will trigger IDS alerts.

Therefore, -sP is the most suitable option to achieve the requirement of identifying live hosts passively and without triggering IDS alerts. It only uses ICMP pings for host detection, making it stealthier than other scanning techniques.

Authoritative links for further research:

Nmap Official Documentation:https://nmap.org/docs/
Nmap man page:man nmap (on a Linux terminal)

Question: 79

Which open-sourced packet capture tool uses Linux and Mac OS X operating systems?

A.NetScout
B.tcpdump
C.SolarWinds
D.netsh

Answer: B

Explanation:

The correct answer is **B. tcpdump**. Tcpdump is a command-line packet analyzer, widely recognized and utilized for network traffic capture and analysis. Its primary strength lies in being open-source and readily available on Linux and Mac OS X systems, often pre-installed or easily installed via package managers.

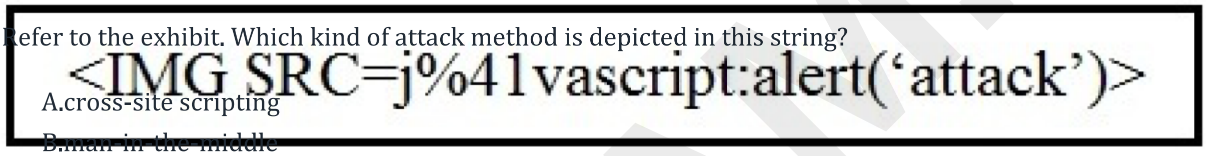
Tcpdump operates directly at the network interface level, allowing users to capture raw packet data. This feature is crucial for detailed network troubleshooting and security analysis. Unlike GUI-based tools, tcpdump provides low-level control and efficiency, making it a preferred choice for system administrators and cybersecurity professionals. It supports various filtering options, allowing users to target specific traffic for analysis, enhancing its utility in complex network environments. Other options are either commercial or Windows-based; NetScout and Solarwinds are primarily commercial network monitoring solutions, while netsh is a command-line tool specific to Windows. Tcpdump's open-source nature and availability across Linux and macOS make it the obvious answer in the context of the question.

Further research:

tcpdump Official Website:https://www.tcpdump.org/
tcpdump Wikipedia:https://en.wikipedia.org/wiki/Tcpdump

Question: 80

Refer to the exhibit. Which kind of attack method is depicted in this string?



```
<IMG SRC=j%41vascript:alert('attack')>
```

A.cross-site scripting
B.man-in-the-middle
C.SQL injection
D.denial of service

Answer: A

Explanation:

Cross-site scripting works by manipulating a vulnerable web site so that it returns malicious JavaScript to users.Key word: Java