

Cisco.200-201.vMay-2024.by.Utanomoto.139q

Number: 200-201
Passing Score: 800
Time Limit: 120
File Version: 15.5

Exam Code: 200-201

Exam Name: Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)



Exam A

QUESTION 1

An intruder attempted malicious activity and exchanged emails with a user and received corporate information, including email distribution lists. The intruder asked the user to engage with a link in an email. When the link launched, it infected machines and the intruder was able to access the corporate network.

Which testing method did the intruder use?

- A. social engineering
- B. eavesdropping
- C. piggybacking
- D. tailgating

Correct Answer: A

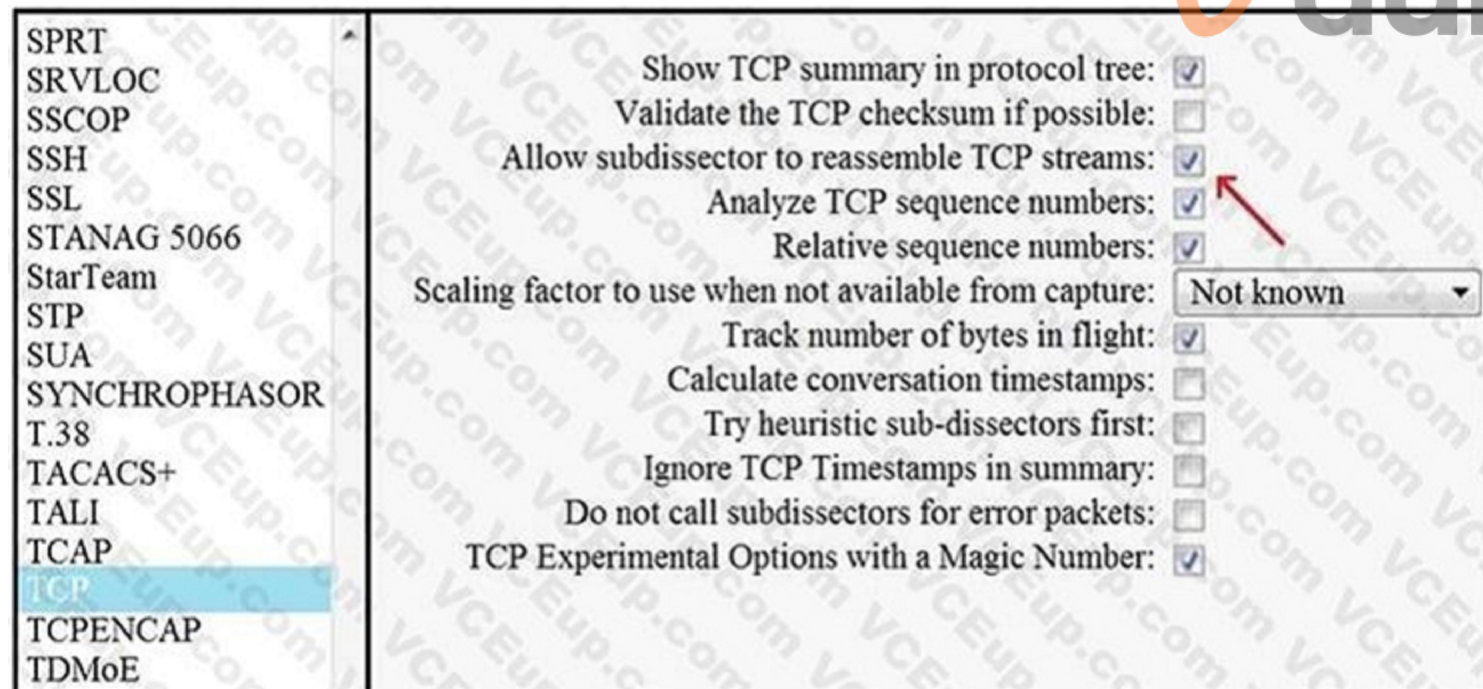
Section:

Explanation:

Social engineering is a type of testing method that involves manipulating or deceiving people into performing actions or divulging information that can compromise the security of the organization. Social engineering can take various forms, such as phishing, vishing, baiting, quid pro quo, or impersonation. The scenario in the question is an example of a phishing attack, where the intruder sent an email to the user that appeared to be legitimate and contained a malicious link that infected the user's machine and allowed the intruder to access the corporate network. Reference: [Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) - Module 6: Security Incident Investigations]

QUESTION 2

Refer to the exhibit.



What is the expected result when the 'Allow subdissector to reassemble TCP streams' feature is enabled?

- A. insert TCP subdissectors
- B. extract a file from a packet capture
- C. disable TCP streams
- D. unfragment TCP

Correct Answer: B

Section:

Explanation:

Enabling the "Allow subdissector to reassemble TCP streams" feature in Wireshark allows the tool to reassemble TCP segments into a contiguous sequence, which can be used by higher-level protocols to reconstruct a full message, such as an HTTP request or response. This is particularly useful for extracting files or data transmitted over TCP that are spread across multiple packets.

QUESTION 3

Which two elements are assets in the role of attribution in an investigation? (Choose two.)

- A. context
- B. session
- C. laptop
- D. firewall logs
- E. threat actor

Correct Answer: C, E

Section:

Explanation:

In the context of cybersecurity, an asset is anything that has value to the organization, its business operations and their continuity, including data and physical devices. In the role of attribution in an investigation, which is the process of associating an action or event with a particular individual or entity, certain assets are particularly relevant. A laptop can be an asset because it may contain data or clues that can help trace the origin of a cyber attack. Similarly, identifying the threat actor (E) is crucial for attribution, as it involves understanding who is behind the attack and their motives, which can be essential for preventing future attacks and for legal proceedings.

QUESTION 4

What is personally identifiable information that must be safeguarded from unauthorized access?

- A. date of birth
- B. driver's license number
- C. gender
- D. zip code

Correct Answer: B

Section:

Explanation:

Personally Identifiable Information (PII) refers to any data that can be used to identify a specific individual. Safeguarding PII is critical to protect individuals' privacy and prevent identity theft. A driver's license number (B) is considered PII because it is unique to an individual and can be used to confirm their identity. Other examples of PII include social security numbers, passport numbers, and financial account numbers. It is important to protect such information from unauthorized access to maintain personal privacy and security.

QUESTION 5

In a SOC environment, what is a vulnerability management metric?

- A. code signing enforcement
- B. full assets scan
- C. internet exposed devices
- D. single factor authentication

Correct Answer: B

Section:

Explanation:

In a Security Operations Center (SOC) environment, a vulnerability management metric is a quantifiable measure used to assess the effectiveness of the vulnerability management program. A full assets scan is a metric that can be used to determine the coverage and frequency of vulnerability scans across all assets. This helps in identifying unscanned assets and ensuring that all parts of the network are regularly checked for vulnerabilities¹.

SOC Metrics: Security Metrics & KPIs for Measuring SOC Success

Vulnerability Management Metrics: 5 Metrics to Start Measuring in Your Vulnerability Management Program

Top 10 Vulnerability Management Metrics & KPIs To Measure Success

QUESTION 6

A security expert is working on a copy of the evidence, an ISO file that is saved in CDFS format. Which type of evidence is this file?

- A. CD data copy prepared in Windows
- B. CD data copy prepared in Mac-based system
- C. CD data copy prepared in Linux system
- D. CD data copy prepared in Android-based system

Correct Answer: A

Section:

Explanation:

The CDFS (Compact Disc File System) format is associated with the ISO 9660 standard, which is a file system for optical disc media. It is commonly used in Windows systems for CDs. When a security expert works on an ISO file saved in CDFS format, it typically indicates that the data was prepared or copied using a Windows-based system. This is because CDFS is the file system that Windows uses to read and write CDs, and the ISO file is an image of that CD data¹.

Understanding CDFS (Compact Disc File System): A Comprehensive Guide².

What type of evidence is this file? - VCEguide.com

QUESTION 7

Which two elements of the incident response process are stated in NIST Special Publication 800-61 r2? (Choose two.)

- A. detection and analysis
- B. post-incident activity
- C. vulnerability management
- D. risk assessment
- E. vulnerability scoring

Correct Answer: A, B

Section:

Explanation:

NIST Special Publication 800-61 r2 outlines the incident response process including detection and analysis, which involves identifying and validating the occurrence of incidents, and post-incident activity that focuses on lessons learned and improvements to be made after an incident has occurred. Reference: NIST Special Publication 800-61 r2

QUESTION 8

Which type of data collection requires the largest amount of storage space?

- A. alert data
- B. transaction data
- C. session data
- D. full packet capture

Correct Answer: D

Section:

Explanation:

Full packet capture requires the largest amount of storage space because it involves recording all packets that pass through a network, including all headers and payloads. This type of data collection is comprehensive and allows for detailed analysis, but due to the volume of data it encompasses, it demands significant storage capacity¹.

QUESTION 9

Which event is user interaction?

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

Correct Answer: D

Section:

Explanation:

User interaction is any event that requires the user to perform an action that enables or facilitates a cyberattack. Opening a malicious file is an example of user interaction, as it can trigger the execution of malicious code or malware that can compromise the system or network. Gaining root access, executing remote code, and reading and writing file permissions are not user interactions, but rather actions that can be performed by an attacker after exploiting a vulnerability or bypassing security controls. Reference: Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) - Cisco, More than 99% of cyberattacks rely on human interaction

QUESTION 10

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



Correct Answer: C

Section:

Explanation:

Separation of duties is a security principle that requires more than one person to perform a critical task, such as authorizing a transaction, approving a budget, or granting access to sensitive data. Separation of duties reduces the risk of fraud, error, abuse, or conflict of interest by preventing any single person from having too much power or privilege. Least privilege, need to know, and due diligence are other security principles, but they do not require more than one person to perform a critical task. Reference: Separation of Duty (SOD) - Glossary | CSRC - NIST Computer Security ..., Separation of Duties | Imperva

QUESTION 11

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

Correct Answer: A

Section:

Explanation:

A vulnerability management framework is a set of processes and tools that helps an organization identify, assess, prioritize, remediate, and mitigate system vulnerabilities. A vulnerability management framework aims to reduce the attack surface and the risk of compromise by applying security patches, hardening configurations, implementing security controls, and monitoring the system status. A vulnerability management framework is an essential component of a security operations center (SOC). Reference: Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) - Cisco, page 2-14; 200-201 CBROPS - Cisco, exam topic 1.2.b

QUESTION 12

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

Correct Answer: D

Section:

Explanation:

A threat agent is the entity that is responsible for initiating a threat action that exploits a vulnerability. A threat agent can be a person, a group, an organization, or a system. In this scenario, the threat agent is the foreign government that hacked the defense contractor and stole the intellectual property. The threat agent's motivation, capability, and resources determine the level of threat they pose to the target. Reference: Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) - Cisco, page 1-3;200-201 CBROPS - Cisco, exam topic 1.1.b

QUESTION 13

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

Correct Answer: A

Section:

Explanation:

The principle of least privilege is a security best practice that states that an employee should have access to only the minimum amount of resources and permissions needed to perform their job function. This principle reduces the attack surface and the potential damage that can be caused by a compromised account, a malicious insider, or human error. The principle of least privilege can be enforced by using role-based access control (RBAC) and regular audits. Reference: Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) - Cisco, page 1-10;200-201 CBROPS - Cisco, exam topic 1.2.a



QUESTION 14

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

Correct Answer: A

Section:

Explanation:

Privileges required is a metric in the Common Vulnerability Scoring System (CVSS) that measures the level of access needed to launch a successful attack. The higher the privileges required, the lower the severity of the vulnerability. The privileges required metric has three possible values: none, low, and high. None means that the attacker does not need any privileges to exploit the vulnerability. Low means that the attacker needs privileges that provide basic user capabilities. High means that the attacker needs privileges that provide significant or administrative control over the target. Reference: Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) - Cisco, page 2-17;200-201 CBROPS - Cisco, exam topic 1.3.c

QUESTION 15

What is the difference between an attack vector and 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.

Correct Answer: B

Section:

Explanation:

An attack vector is the method or technique that an attacker uses to exploit a vulnerability in a system or network. An attack vector can be a software, hardware, or human component that can be manipulated to gain unauthorized access, execute malicious code, or cause damage. An attack surface is the sum of all the possible attack vectors that are exposed by a system or network. An attack surface can be reduced by applying security measures such as patching, hardening, firewalling, and encrypting. Reference: Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) - Cisco, page 1-4; 200-201 CBROPS - Cisco, exam topic 1.1.c

QUESTION 16

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.

Correct Answer: B

Section:

Explanation:

Defense-in-depth is a security strategy where multiple layers of defense are placed throughout an information technology (IT) system. It addresses physical, technical, and administrative controls to provide redundancy and ensure that if one layer fails, others will be in place to thwart an attack. Reference: Cisco Tech Roles - CyberOps Engineer

QUESTION 17

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.

Correct Answer: B

Section:

Explanation:

Rule-based detection involves identifying malicious activities based on predefined rules or patterns of known attacks; it does not adapt or change with new data. In contrast, behavioral detection adapts over time by learning from new data; it identifies malicious activities based on deviations from established norms or behaviors. Reference: Cisco Certified CyberOps Associate Overview, Section 1.0: Security Concepts, Subsection 1.1: Compare and contrast the characteristics of data obtained from taps, NetFlow, and packet capture)

QUESTION 18

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

- A. NetScout
- B. tcpdump

- C. SolarWinds
- D. netsh

Correct Answer: B

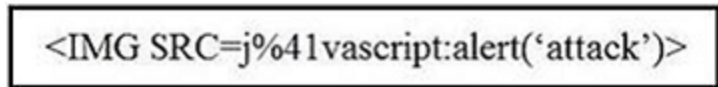
Section:

Explanation:

tcpdump is an open-source packet capture tool that uses the libpcap library to capture network traffic on Linux and Mac OS X operating systems. It can display the contents of packets in various formats, filter packets based on criteria, and save packets to a file. tcpdump is a command-line tool that can be run on a terminal or a remote shell. Reference: Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) - Module 2: Security Monitoring

QUESTION 19

Refer to the exhibit.



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

Which kind of attack method is depicted in this string?

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

Correct Answer: A

Section:

Explanation:

The image shows a piece of code within a bordered rectangular area.

It is a string of HTML code that appears to be an example of an attack, specifically "".

The code suggests an attempt to execute JavaScript within an image source attribute, indicative of a cross-site scripting attack.

QUESTION 20

Which two components reduce the attack surface on an endpoint? (Choose two.)

- A. secure boot
- B. load balancing
- C. increased audit log levels
- D. restricting USB ports
- E. full packet captures at the endpoint

Correct Answer: A, D

Section:

Explanation:

Secure boot and restricting USB ports are two components that can reduce the attack surface on an endpoint. The attack surface is the sum of all paths for data into and out of the environment. Reducing the attack surface means minimizing the number and complexity of these paths, and thus reducing the opportunities for attackers to exploit vulnerabilities or gain unauthorized access. Secure boot is a feature that ensures that only trusted and verified code can run during the boot process, preventing malware or unauthorized software from compromising the system. Restricting USB ports is a policy that limits the use of USB devices, such as flash drives or external hard drives, that can introduce malware or exfiltrate data from the endpoint.

Reference: [Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) - Module 4: Network Intrusion Analysis], [Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) - Module 5: Security Policies and Procedures]

QUESTION 21

What is an attack surface as compared to a vulnerability?

- A. any potential danger to an asset
- B. the sum of all paths for data into and out of the environment
- C. an exploitable weakness in a system or its design
- D. the individuals who perform an attack

Correct Answer: B

Section:

Explanation:

The attack surface is the sum of all paths for data into and out of the environment, such as network interfaces, applications, services, protocols, ports, and user accounts. The attack surface represents the exposure of the environment to potential threats and attacks. A vulnerability is an exploitable weakness in a system or its design that can allow an attacker to compromise the system or its data. A vulnerability is a subset of the attack surface, as not all paths for data are vulnerable. Reference: [Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) - Module 1: Security Concepts]

QUESTION 22

How is attacking a vulnerability categorized?

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

Correct Answer: C

Section:

Explanation:

Attacking a vulnerability is categorized as exploitation, which is the third phase of the cyberattack lifecycle. Exploitation is the process of taking advantage of a vulnerability in a system, application, or network to gain access, escalate privileges, or execute commands. Action on objectives, delivery, and installation are other phases of the cyberattack lifecycle, but they do not involve attacking a vulnerability. Action on objectives is the final phase, where the attacker achieves their goal, such as stealing data, disrupting services, or destroying assets. Delivery is the second phase, where the attacker delivers the malicious payload, such as malware, phishing email, or malicious link, to the target. Installation is the fourth phase, where the attacker installs the malicious payload on the compromised system or network to maintain persistence or spread laterally. Reference: What is a Cyberattack? | IBM, Recognizing the seven stages of a cyber-attack - DNV

QUESTION 23

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

Correct Answer: C

Section:

Explanation:

Agent-based protection is a type of endpoint security that uses software agents installed on the devices to monitor and protect them. Agent-based protection can collect and detect all traffic locally, which means it can operate without relying on a network connection or a centralized server. Agent-based protection can also provide more granular and comprehensive visibility and control over the devices. Reference: <https://learningnetworkstore.cisco.com/on-demand-e-learning/understanding-cisco-cybersecurity-operations-fundamentals-cbrops-v1.0/CSCU-LP-CBROPS-V1-028093.html> (Module 2: Security Concepts, Lesson 2.3: Endpoint Security)

QUESTION 24

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

Correct Answer: A

Section:

Explanation:

Decision making is a principle that guides an analyst to gather information relevant to a security incident to determine the appropriate course of action. Decision making involves identifying the problem, defining the criteria, analyzing the alternatives, and choosing the best solution. Decision making helps an analyst to respond to an incident effectively and efficiently, while minimizing the impact and risk to the organization. Reference:

<https://learningnetworkstore.cisco.com/on-demand-e-learning/understanding-cisco-cybersecurity-operations-fundamentals-cbrops-v1.0/CSCU-LP-CBROPS-V1-028093.html> (Module 3: Security Monitoring, Lesson 3.1: Security Operations Center)

QUESTION 25

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

Correct Answer: D

Section:

Explanation:

CIA stands for confidentiality, integrity, and availability, which are the three main objectives of information security. Confidentiality means protecting the information from unauthorized access or disclosure. Integrity means ensuring the information is accurate and consistent, and preventing unauthorized modification or deletion. Availability means ensuring the information and systems are accessible and usable by authorized users when needed. Reference: <https://learningnetworkstore.cisco.com/on-demand-e-learning/understanding-cisco-cybersecurity-operations-fundamentals-cbrops-v1.0/CSCU-LP-CBROPS-V1-028093.html> (Module 2: Security Concepts, Lesson 2.1: Security Principles)

QUESTION 26

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

Correct Answer: B

Section:

Explanation:

Rule-based detection is a type of intrusion detection system (IDS) that uses predefined rules or signatures to identify malicious or suspicious activity. Rule-based detection can provide proof of a user's action, such as an attempt to exploit a known vulnerability or execute a malicious command. Rule-based detection can also provide a high level of accuracy and specificity, but it requires constant updates and maintenance of the rules or signatures. Reference: <https://learningnetworkstore.cisco.com/on-demand-e-learning/understanding-cisco-cybersecurity-operations-fundamentals-cbrops-v1.0/CSCU-LP-CBROPS-V1-028093.html> (Module 4: Attack Methods, Lesson 4.2: Attack Techniques)

QUESTION 27



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

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

Correct Answer: D

Section:

QUESTION 28

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

Correct Answer: B

Section:

QUESTION 29

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

Correct Answer: C

Section:

QUESTION 30

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

Correct Answer: A

Section:

QUESTION 31

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

Correct Answer: B

Section:

QUESTION 32

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

Correct Answer: C

Section:

Explanation:

NetFlow provides a more efficient way of recording and analyzing network traffic patterns over an extended period of time compared to syslog messages, full packet capture, or firewall event logs. It collects metadata about traffic flows traversing the network devices which can be used for understanding normal baseline behavior as well as identifying anomalies. Reference:=Cisco Certified CyberOps Associate Overview

QUESTION 33

A security analyst notices a sudden surge of incoming traffic and detects unknown packets from unknown senders. After further investigation, the analyst learns that customers claim that they cannot access company servers. According to NIST SP800-61, in which phase of the incident response process is the analyst?

- A. post-incident activity
- B. detection and analysis
- C. preparation
- D. containment, eradication, and recovery

Correct Answer: B

Section:

Explanation:

The analyst is in the detection and analysis phase of the incident response process according to NIST SP800-61. In this phase, events are detected and analyzed to determine whether they constitute incidents that require a response. It involves monitoring security events or data collection, correlation, and analysis of log entries and network flow data, among others. The goal is to identify incidents quickly so that appropriate actions can be taken. Reference:= NIST SP800-61, Computer Security Incident Handling Guide, Section 3.2: Detection and Analysis

QUESTION 34

Which vulnerability type is used to read, write, or erase information from a database?

- A. cross-site scripting
- B. cross-site request forgery
- C. buffer overflow
- D. SQL injection

Correct Answer: D

Section:

Explanation:

SQL injection is a type of vulnerability that allows an attacker to execute malicious SQL statements on a database server. This can result in reading, writing, or erasing information from the database, as well as bypassing authentication, executing commands, or compromising the server. SQL injection exploits the lack of input validation or output encoding in web applications that interact with databases. Reference:= Cisco Cybersecurity Operations Fundamentals, Module 1: Security Concepts, Lesson 1.3: Common Network Application Operations and Attacks, Topic 1.3.2: Web Application Attacks

QUESTION 35

An automotive company provides new types of engines and special brakes for rally sports cars. The company has a database of inventions and patents for their engines and technical information. Customers can access the database through the company's website after they register and identify themselves. Which type of protected data is accessed by customers?

- A. IP data
- B. PII data
- C. PSI data
- D. PHI data

Correct Answer: A

Section:**Explanation:**

IP data stands for Intellectual Property data, which is any data that represents the creations of the mind, such as inventions, patents, designs, or artistic works. IP data is protected by law and has commercial value for its owners. In this case, the automotive company has a database of IP data for their engines and technical information, which customers can access after they register and identify themselves. Reference:= Cisco Cybersecurity Operations Fundamentals, Module 1: Security Concepts, Lesson 1.2: Data Protection, Topic 1.2.1: Data Types

QUESTION 36

According to the September 2020 threat intelligence feeds a new malware called Egregor was introduced and used in many attacks. Distribution of Egregor is primarily through a Cobalt Strike that has been installed on victim's workstations using RDP exploits. Malware exfiltrates the victim's data to a command and control server. The data is used to force victims pay or lose it by publicly releasing it. Which type of attack is described?

- A. malware attack
- B. ransomware attack
- C. whale-phishing
- D. insider threat

Correct Answer: B

Section:**Explanation:**

Ransomware is a type of malware that encrypts the victim's data and demands a ransom for the decryption key. The attacker may also threaten to publish or delete the data if the ransom is not paid. In this case, the Egregor malware is distributed through a Cobalt Strike, which is a penetration testing tool that can be used to deploy payloads on compromised systems. The malware exfiltrates the victim's data to a command and control server and uses it as leverage to extort money from the victim. Reference:= Cisco Cybersecurity Operations Fundamentals, Module 1: Security Concepts, Lesson 1.3: Common Network Application Operations and Attacks, Topic 1.3.3: Malware Attacks

QUESTION 37

Syslog collecting software is installed on the server. For the log containment, a disk with FAT type partition is used. An engineer determined that log files are being corrupted when the 4 GB file size is exceeded. Which action resolves the issue?

- A. Add space to the existing partition and lower the retention period.
- B. Use FAT32 to exceed the limit of 4 GB.
- C. Use the Ext4 partition because it can hold files up to 16 TB.
- D. Use NTFS partition for log file containment

Correct Answer: B

Section:**Explanation:**

FAT is a file system that organizes and stores data on a disk. However, FAT has a limitation of 4 GB for the maximum file size, which means that any file larger than that will be corrupted. To resolve this issue, the engineer can use FAT32, which is an improved version of FAT that supports files up to 32 GB. Alternatively, the engineer can use other file systems that have higher file size limits, such as Ext4 or NTFS. Reference:= Cisco Cybersecurity Operations Fundamentals, Module 5: Security Policies and Procedures, Lesson 5.1: Data Retention, Topic 5.1.1: Data Retention Policies and Procedures

QUESTION 38

What are two categories of DDoS attacks? (Choose two.)

- A. split brain
- B. scanning
- C. phishing
- D. reflected
- E. direct

Correct Answer: D, E

Section:**Explanation:**

DDoS attacks are divided into two categories: reflected and direct. Reflected attacks use a third-party system to amplify the attack traffic and send it to the target. For example, an attacker can send a spoofed request to a DNS server, which will reply with a large amount of data to the target's IP address. Direct attacks send the attack traffic directly from the attacker's system or a botnet to the target. For example, an attacker can send a large number of SYN packets to the target's port, exhausting its resources. Reference:= Cisco Cybersecurity Operations Fundamentals, Module 1: Security Concepts, Lesson 1.3: Common Network Application Operations and Attacks, Topic 1.3.4: Denial-of-Service Attacks

QUESTION 39

What is an advantage of symmetric over asymmetric encryption?

- A. A key is generated on demand according to data type.
- B. A one-time encryption key is generated for data transmission
- C. It is suited for transmitting large amounts of data.
- D. It is a faster encryption mechanism for sessions

Correct Answer: D

Section:**Explanation:**

Symmetric encryption is a type of encryption that uses the same key to encrypt and decrypt data. Asymmetric encryption is a type of encryption that uses a pair of keys: a public key and a private key. The public key can be used to encrypt data, but only the private key can decrypt it, and vice versa. An advantage of symmetric encryption over asymmetric encryption is that it is faster and more efficient for encrypting large amounts of data, such as in sessions or bulk transfers. Asymmetric encryption is slower and more computationally intensive, but it is more secure and suitable for key exchange or digital signatures. Reference:= Cisco Cybersecurity Operations Fundamentals, Module 2: Security Monitoring, Lesson 2.3: Cryptography and PKI, Topic 2.3.1: Cryptography

QUESTION 40

What are two denial-of-service (DoS) attacks? (Choose two)

- A. port scan
- B. SYN flood
- C. man-in-the-middle
- D. phishing
- E. teardrop



Correct Answer: B, E

Section:

Explanation:

SYN flood and teardrop are two types of denial-of-service (DoS) attacks, which aim to disrupt the availability of a service or a system by overwhelming it with malicious traffic or requests. A SYN flood attack exploits the TCP three-way handshake process by sending a large number of SYN packets to the target's port, without completing the connection. This causes the target to allocate resources for half-open connections, eventually exhausting its memory or bandwidth. A teardrop attack exploits the IP fragmentation process by sending malformed or overlapping IP fragments to the target, causing it to crash or reboot when trying to reassemble them. Reference:= Cisco Cybersecurity Operations Fundamentals, Module 1: Security Concepts, Lesson 1.3: Common Network Application Operations and Attacks, Topic 1.3.4: Denial-of-Service Attacks

QUESTION 41

What is the difference between a threat and an exploit?

- A. A threat is a result of utilizing flow in a system, and an exploit is a result of gaining control over the system.
- B. A threat is a potential attack on an asset and an exploit takes advantage of the vulnerability of the asset
- C. An exploit is an attack vector, and a threat is a potential path the attack must go through.
- D. An exploit is an attack path, and a threat represents a potential vulnerability

Correct Answer: B

Section:

Explanation:

A threat is a possible danger that might exploit a vulnerability to breach the security and cause harm to an asset. An asset is anything of value that needs to be protected, such as data, systems, or networks. A vulnerability is a weakness or flaw in the security that can be exploited by a threat. An exploit is a piece of code or a technique that takes advantage of a vulnerability to compromise the security and perform malicious actions on an asset. Reference:= Cisco Cybersecurity Operations Fundamentals, Module 1: Security Concepts, Lesson 1.1: The CIA Triad and Security Concepts, Topic 1.1.3: Threats, Vulnerabilities, and Exploits

QUESTION 42

Which action prevents buffer overflow attacks?

- A. variable randomization
- B. using web based applications
- C. input sanitization
- D. using a Linux operating system

Correct Answer: C

Section:

Explanation:

Input sanitization involves cleaning up user input before processing it, ensuring that it does not contain malicious code intended for buffer overflow attacks or other types of security breaches. Reference:=New Cybersecurity Skills

QUESTION 43

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

Correct Answer: D

Section:

Explanation:



A man-in-the-middle attack occurs when a third party intercepts and potentially alters the communication between two parties (in this case, two IP phones) without them knowing. This type of attack can lead to eavesdropping, where the attacker can gain unauthorized access to sensitive data being communicated between the two parties. Reference:=Cisco Cybersecurity Operations Fundamentals - Module 5: Endpoint Threat Analysis and Computer Forensics

QUESTION 44

Refer to the exhibit.

```
- 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: 0x6b5e (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
```

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 UDP protocol.

Correct Answer: B

Section:

Explanation:

The packet capture exhibit shows that the source IP address is 192.168.122.100 and it is sending a packet from source port 50272 to destination port 80 of destination IP address 81.179.179.69 using TCP protocol. The TCP protocol is indicated by the Protocol field which has the value 6. The source and destination ports are indicated by the SrcPort and DstPort fields respectively. The source and destination IP addresses are indicated by the SrcAddr and DstAddr fields respectively. Reference:=Cisco Cybersecurity Operations Fundamentals - Module 3: Network Data and Event Analysis

QUESTION 45

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.

Correct Answer: B, C

Section:

Explanation:

Full packet captures are essential for troubleshooting security and performance issues as they provide detailed information on network traffic (option B). They also allow for reassembling fragmented traffic from raw data, enabling analysts to review complete transactions or sessions (option C). Reference:=Cisco Cybersecurity Operations Fundamentals - Module 3: Network Data and Event Analysis

QUESTION 46

Refer to the exhibit.

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	0805d0ae62f5358b9a3f4c1868d552fc3561b17
SHA256	27cced58a0fcbb0bbe3894f74d3014611039fefdf3bd2b0ba7ad85b18194c
SHA512	5a43bc7eef279b209e2590432cc3e2eb480d0f78004e265f00b98b4afdc9a
Ssdeep	1536:p0AAH2KthGBjcdBj8VETeePxsT65ZZ3pdx/ves/QR/875+.prahGV6B
PEID	None matched
Yara	<ul style="list-style-type: none">• 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)

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.

Correct Answer: C

Section:

QUESTION 47

Refer to the exhibit.

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	88 - 3222 [SYN, ACK] Seq=0 Ack=1 Win=29288 Len=0 NSS=1468
3	0.005514	10.128.0.2	10.0.0.2	TCP	58	88 - 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	88 - 3220 [SYN, ACK] Seq=0 Ack=1 Win=2988 Len=0 NSS=1468
6	0.014072	10.128.0.2	10.0.0.2	TCP	58	88 - 3342 [SYN, ACK] Seq=0 Ack=1 Win=2900 Len=0 NSS=1460
7	0.016830	10.0.0.2	10.128.0.2	TCP	54	3343 - 88 [SYN] Seq=0 Win=512 Len=0
8	0.022220	10.128.0.2	10.0.0.2	TCP	58	89 - 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	89 - 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 - 88 [SYN] Seq=0 Win=512 Len=0
11	0.026672	10.128.0.2	10.0.0.2	TCP	58	89 - 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	88 - 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: 18.0.0.2, 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: 1023350884
  0101 ... = Header Length: 20 bytes (5)
  Flags: 0x002 (SYN)
  Windows Size Value: 512
  [Calculated window size: 512]
  Checksum: 0x8d5a [unverified]
  [Checksum Status: Unverified]
  Urgent pointer: 0
  [Timestamps]

```

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.

Correct Answer: A

Section:

Explanation:

The exhibit shows a high rate of SYN packets being sent from multiple sources towards a single destination IP. This is indicative of a SYN flood attack, where the attacker sends a succession of SYN requests to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic. Reference:= Cisco Cybersecurity Operations Fundamentals - Module 4: Network Intrusion Analysis

QUESTION 48

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

Correct Answer: D, E

Section:

Explanation:

Cisco Application Visibility and Control (AVC) provides features like metrics collection and exporting (D) for visibility on TCP bandwidth usage, response time, and latency. Application recognition (E) combined with deep packet inspection helps in identifying unknown software by its network traffic flow. Reference:=Cisco CyberOps Associate - Module 2: Security Concepts

QUESTION 49

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

Correct Answer: B

Section:

Explanation:

SSL Certificate guarantees the integrity and authenticity of all messages transferred to and from a web application. It encrypts the data transferred between the user's browser and the website, ensuring that all data passed between them remains private and integral. Reference:=Cisco CyberOps Engineer - Module 3: Secure Communications

QUESTION 50

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



Correct Answer: D

Section:

Explanation:

The unauthorized usage of "Tcpdump" tool indicates that the malicious insider was attempting to obtain all information within datagrams passing through a specific interface on the network. Tcpdump allows users to capture packet data from a live network or read packets from a previously saved capture file. Reference:=Cisco CyberOps - Module 3: Network Data and Event Analysis

QUESTION 51

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

Correct Answer: D

Section:

Explanation:

Social engineering is the practice of manipulating or deceiving people into performing actions or divulging information that can compromise the security of the organization. Asking questions about the company's user account format and password complexity at a party is an example of social engineering, as the guest may be trying to gather information that can be used to launch a cyberattack. Reference:= Cisco Cybersecurity Operations Fundamentals - Module 6: Security Incident Investigations

QUESTION 52

Which security monitoring data type requires the largest storage space?

- A. transaction data
- B. statistical data
- C. session data
- D. full packet capture

Correct Answer: D

Section:

Explanation:

Full packet capture data involves storing the entire content of packets that traverse a network. This type of data is comprehensive and allows for detailed analysis but requires a significant amount of storage space compared to other data types like transaction, statistical, or session data. Reference: Cisco Cybersecurity Operations Fundamentals - Module 3: Network Data and Event Analysis

QUESTION 53

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

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

Correct Answer: C, D

Section:

Explanation:

Ping of Death involves sending oversized or malformed pings to crash the target system, while UDP flooding overwhelms the target with UDP packets to consume its resources and disrupt services. These are both examples of denial of service attacks, which aim to prevent legitimate users from accessing a system or service. Reference: Cisco Cybersecurity Operations Fundamentals - Module 4: Network Intrusion Analysis

QUESTION 54

Which tool provides a full packet capture from network traffic?

- A. Nagios
- B. CAINE
- C. Hydra
- D. Wireshark

Correct Answer: D

Section:

Explanation:

Wireshark is a widely-used network protocol analyzer that allows users to capture and interactively browse the traffic running on a computer network. It provides full packet capture capabilities, enabling detailed analysis of network traffic. Reference: This is supported by the CBROPS course materials, which discuss security monitoring and the analysis of network traffic, including full packet capture tools like Wireshark

QUESTION 55

Which event is a phishing attack?

- A. obtaining disposed documents from an organization



- B. using a vulnerability scanner on a corporate network
- C. setting up a rogue access point near a public hotspot
- D. impersonating a tech support agent during a phone call

Correct Answer: D

Section:

Explanation:

Vishing is an attack where fraudsters impersonate legitimate entities via phone calls to deceive individuals into providing sensitive information or performing actions that compromise security. Reference: Cisco Cybersecurity Source Documents

QUESTION 56

What is indicated by an increase in IPv4 traffic carrying protocol 41 ?

- A. additional PPTP traffic due to Windows clients
- B. unauthorized peer-to-peer traffic
- C. deployment of a GRE network on top of an existing Layer 3 network
- D. attempts to tunnel IPv6 traffic through an IPv4 network

Correct Answer: D

Section:

Explanation:

Protocol 41 is used to encapsulate IPv6 packets in IPv4 headers for transmission over an IPv4 network. This is one of the methods to implement IPv6 transition mechanisms for hosts and routers that are located on IPv4 networks. An increase in IPv4 traffic carrying protocol 41 may indicate that some hosts or routers are trying to tunnel IPv6 traffic through an IPv4 network, which could be a legitimate or malicious activity depending on the network policy. Reference: Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) - Cisco, page 177; [IPv6 Transition Mechanisms for IPv4 Domains]

QUESTION 57

What is the impact of false positive alerts on business compared to true positive?

- A. True positives affect security as no alarm is raised when an attack has taken place, while false positives are alerts raised appropriately to detect and further mitigate them.
- B. True-positive alerts are blocked by mistake as potential attacks, while False-positives are actual attacks Identified as harmless.
- C. False-positive alerts are detected by confusion as potential attacks, while true positives are attack attempts identified appropriately.
- D. False positives alerts are manually ignored signatures to avoid warnings that are already acknowledged, while true positives are warnings that are not yet acknowledged.

Correct Answer: C

Section:

Explanation:

False-positive alerts are alerts that are triggered by benign or normal network traffic and are mistakenly identified as malicious. False positives can have a negative impact on business as they may consume the resources and time of the security team that need to analyze and verify them. True-positive alerts are alerts that correctly identify malicious traffic or activity and require proper incident response procedures. True positives can help the security team to quickly detect and mitigate threats and minimize the damage to the organization. Reference: Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) - Cisco, page 92; [Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide], page 98

QUESTION 58

An organization's security team has detected network spikes coming from the internal network. An investigation has concluded that the spike in traffic was from intensive network scanning How should the analyst collect the traffic to isolate the suspicious host?

- A. by most active source IP
- B. by most used ports
- C. based on the protocols used

D. based on the most used applications

Correct Answer: A

Section:

Explanation:

To isolate the suspicious host that is performing intensive network scanning, the analyst should collect the traffic by most active source IP. This will help to identify the IP address of the host that is generating the most traffic and sending the most packets or bytes. The analyst can then apply filters or queries to analyze the traffic from that source IP and determine the nature and scope of the scanning activity. Reference: Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) - Cisco, page 72; [Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide], page 468

QUESTION 59

What is a difference between an inline and a tap mode traffic monitoring?

- A. Inline monitors traffic without examining other devices, while a tap mode tags traffic and examines the data from monitoring devices.
- B. Tap mode monitors traffic direction, while inline mode keeps packet data as it passes through the monitoring devices.
- C. Tap mode monitors packets and their content with the highest speed, while the inline mode draws a packet path for analysis.
- D. Inline mode monitors traffic path, examining any traffic at a wire speed, while a tap mode monitors traffic as it crosses the network.

Correct Answer: D

Section:

Explanation:

Inline mode is used for monitoring the traffic path and can examine any traffic at wire speed. This means that it can analyze data packets as they pass through in real-time. On the other hand, tap mode is used for monitoring traffic as it traverses across the network but does not have the capability to examine data at wire speed like inline mode. Reference: The information can be referenced from Cisco's official documentation on cybersecurity operations and fundamentals.

QUESTION 60

A company is using several network applications that require high availability and responsiveness, such that milliseconds of latency on network traffic is not acceptable. An engineer needs to analyze the network and identify ways to improve traffic movement to minimize delays. Which information must the engineer obtain for this analysis?

- A. total throughput on the interface of the router and NetFlow records
- B. output of routing protocol authentication failures and ports used
- C. running processes on the applications and their total network usage
- D. deep packet captures of each application flow and duration

Correct Answer: A

Section:

Explanation:

For high availability and responsiveness, especially where milliseconds of latency are critical, an engineer must analyze the network's performance in detail. Total throughput on the interface of the router will provide information on the bandwidth and traffic load, which is essential for understanding if the network can handle the current and projected traffic without delays. NetFlow records are crucial for this analysis as they provide data about the traffic flow across the network, which helps in identifying patterns, peak usage times, and types of traffic. This information is vital for making informed decisions to optimize traffic movement and minimize latency.

Cisco's guide on Network Traffic Analysis¹.

Cisco's white paper on Network Security Policy: Best Practices².

Cisco's documentation on Implementation of High Availability

QUESTION 61

Refer to the exhibit.

```
root@:~# cat access-logs/access_130603.txt | grep '192.168.1.91' | cut -d "\"" -f 2 |
uniq -c
 1 GET /portal.php?mode=addevent&date=2018-05-01 HTTP/1.1
 1 GET /blog/?attachment_id=2910 HTTP/1.1
 1 GET /blog/?attachment_id=2998&feed=rss2 HTTP/1.1
 1 GET /blog/?attachment_id=3156 HTTP/1.1
```

What is depicted in the exhibit?

- A. Windows Event logs
- B. Apache logs
- C. IIS logs
- D. UNIX-based syslog

Correct Answer: B

Section:

Explanation:

The exhibit shows a UNIX command being used to filter data from an Apache access log file. The use of "cat" to display the content of the log file, "grep" to filter specific IP addresses, and "cut" to organize the output are all indicative of operations performed on a UNIX-based system. Additionally, the structure of the logs (GET requests) aligns with the format typically found in Apache server logs. Reference:= The Cisco Cybersecurity source documents or study guide are not directly referenced here as I need to search for specific content related to this question.

QUESTION 62

Which technology should be used to implement a solution that makes routing decisions based on HTTP header, uniform resource identifier, and SSL session ID attributes?

- A. AWS
- B. IIS
- C. Load balancer
- D. Proxy server

Correct Answer: C

Section:

Explanation:

A load balancer is the correct technology to implement a solution that makes routing decisions based on HTTP header, uniform resource identifier (URI), and SSL session ID attributes. Load balancers can inspect incoming traffic and make routing decisions to distribute the traffic across multiple servers based on various attributes, including the ones mentioned, to ensure optimal resource use and efficient traffic management¹².

Cisco Unified Border Element Configuration Guide¹.

URI based outbound Dial-peer configuration on CUBE - Cisco Community

QUESTION 63

An organization has recently adjusted its security stance in response to online threats made by a known hacktivist group.

What is the initial event called in the NIST SP800-61?

- A. online assault
- B. precursor
- C. trigger
- D. instigator

Correct Answer: B

Section:

Explanation:

In the context of NIST SP800-61, a precursor is an event that indicates the potential occurrence of an incident. When an organization adjusts its security stance in response to online threats made by a known hacktivist group, the initial event---the threats---would be considered a precursor.It is an indication of a potential future attack or security incident34.

NIST SP 800-61 Rev.2, Computer Security Incident Handling Guide3.

Computer Security Incident Handling Guide - NIST

QUESTION 64

Which NIST IR category stakeholder is responsible for coordinating incident response among various business units, minimizing damage, and reporting to regulatory agencies?

- A. CSIRT
- B. PSIRT
- C. public affairs
- D. management

Correct Answer: D

Section:

Explanation:

In the context of NIST's incident response guidelines, management is responsible for coordinating incident response among various business units, minimizing damage, and reporting to regulatory agencies.Management plays a key role in overseeing the incident response process to ensure that it is carried out effectively across all parts of the organization and that compliance with legal and regulatory requirements is maintained12.

NIST SP 800-61 Rev.2, Computer Security Incident Handling Guide1.

InfraExam's discussion on incident response stakeholder responsibilities

QUESTION 65

Which incidence response step includes identifying all hosts affected by an attack?

- A. detection and analysis
- B. post-incident activity
- C. preparation
- D. containment, eradication, and recovery

Correct Answer: A

Section:

Explanation:

The 'detection and analysis' phase of incident response includes identifying all hosts affected by an attack.This step involves analyzing the scope of the incident, determining which systems and data are impacted, and understanding the nature of the attack to inform subsequent containment and eradication efforts45.

CrowdStrike's overview of incident response frameworks and steps4.

VCEGuide's explanation of incident response steps

QUESTION 66

Which two elements are used for profiling a network? (Choose two.)

- A. session duration
- B. total throughput
- C. running processes
- D. listening ports
- E. OS fingerprint

Correct Answer: B, D



Section:

Explanation:

Profiling a network involves various elements that provide insights into its characteristics and behaviors. Total throughput is crucial as it measures the amount of data passing from a source to a destination in a given period, reflecting the network's capacity and usage patterns¹. Listening ports are also essential for profiling because they represent the entry points for network services, indicating which services are available and potentially vulnerable¹.

Network profiling tools and techniques discussed in online resources²³.

Direct explanations of network profile elements

QUESTION 67

Which category relates to improper use or disclosure of PII data?

- A. legal
- B. compliance
- C. regulated
- D. contractual

Correct Answer: B

Section:

Explanation:

The improper use or disclosure of Personally Identifiable Information (PII) falls under the category of compliance because organizations are required to adhere to laws and regulations that protect the privacy and security of PII. This includes following guidelines set forth by privacy laws such as GDPR, HIPAA, and others that mandate the proper handling of personal data to prevent misuse and unauthorized access¹²³.

QUESTION 68

Which type of evidence supports a theory or an assumption that results from initial evidence?

- A. probabilistic
- B. indirect
- C. best
- D. corroborative

Correct Answer: D

Section:

Explanation:

Corroborative evidence is the type of evidence that supports a theory or an assumption that results from initial evidence. It provides additional support to the initial findings, strengthening the theory or assumption by confirming the same facts or pointing towards the same conclusion with independent pieces of evidence⁴⁵⁶⁷.

QUESTION 69

Refer to the exhibit.




```
443/tcp closed https
'nap done: 1. IP address (1 host up) scanned in 0.19 seconds
Ps C:\Program Files (x86)\Nmap> nmap --top-ports 10 172.31.45.240
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-22 22:05 Coordinated Universal Time
'nap scan report for ip-172-31-45-240.us-west-2.compute.internal (172.31.45.240)
Host is up (0.00s latency).

PORT      STATE SERVICE
21/tcp    closed ftp
22/tcp    closed ssh
23/tcp    closed telnet
25/tcp    closed smtp
80/tcp    closed http
110/tcp   closed pop3
139/tcp   open  netbios-ssn|
443/tcp   closed https
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server

'map done: 1 IP address (1 host up) scanned in 0.19 seconds PS
C:\Program Files (x86)\Nmap>
```

What does this output indicate?

- A. HTTPS ports are open on the server.
- B. SMB ports are closed on the server.
- C. FTP ports are open on the server.
- D. Email ports are closed on the server.

Correct Answer: D

Section:

Explanation:

What Are Ports 139 And 445? SMB has always been a network file sharing protocol. As such, SMB requires network ports on a computer or server to enable communication to other systems. SMB uses either IP port 139 or 445. Port 139 - SMB originally ran on top of NetBIOS using port 139. NetBIOS is an older transport layer that allows Windows computers to talk to each other on the same network. Port 445 - Later versions of SMB (after Windows 2000) began to use port 445 on top of a TCP stack. Using TCP allows SMB to work over the internet. <https://www.varonis.com/blog/smb-port> SMB Ports 139 and 445 are open Email Ports 25 and 110 are closed Therefore 'D. Email Ports are closed on the Server.'

QUESTION 70

Which metric should be used when evaluating the effectiveness and scope of a Security Operations Center?

- A. The average time the SOC takes to register and assign the incident.
- B. The total incident escalations per week.
- C. The average time the SOC takes to detect and resolve the incident.
- D. The total incident escalations per month.

Correct Answer: C

Section:

Explanation:

The average time taken by a Security Operations Center (SOC) to detect and resolve incidents is a critical metric for evaluating its effectiveness and scope. This metric reflects the SOC's efficiency in identifying security threats and its ability to respond and mitigate those threats promptly. It encompasses the entire incident lifecycle, from initial detection to final resolution, providing a comprehensive measure of the SOC's performance.
Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)

QUESTION 71

A developer is working on a project using a Linux tool that enables writing processes to obtain these required results:

If the process is unsuccessful, a negative value is returned.

If the process is successful, 0 value is returned to the child process, and the process ID is sent to the parent process. Which component results from this operation?

- A. parent directory name of a file pathname
- B. process spawn scheduled
- C. macros for managing CPU sets
- D. new process created by parent process

Correct Answer: D

Section:

Explanation:

The operation described is characteristic of the `fork()` system call in Linux, which is used to create a new process. The `fork()` system call generates a new process by duplicating the calling (parent) process. If the `fork()` is successful, the PID of the child process is returned to the parent process, and a 0 value is returned to the child process. If unsuccessful, a negative value is returned.

How to create a process in Linux? - Online Tutorials Library

QUESTION 72

An engineer discovered a breach, identified the threat's entry point, and removed access. The engineer was able to identify the host, the IP address of the threat actor, and the application the threat actor targeted. What is the next step the engineer should take according to the NIST SP 800-61 Incident handling guide?

- A. Recover from the threat.
- B. Analyze the threat.
- C. Identify lessons learned from the threat.
- D. Reduce the probability of similar threats.

Correct Answer: A

Section:

Explanation:

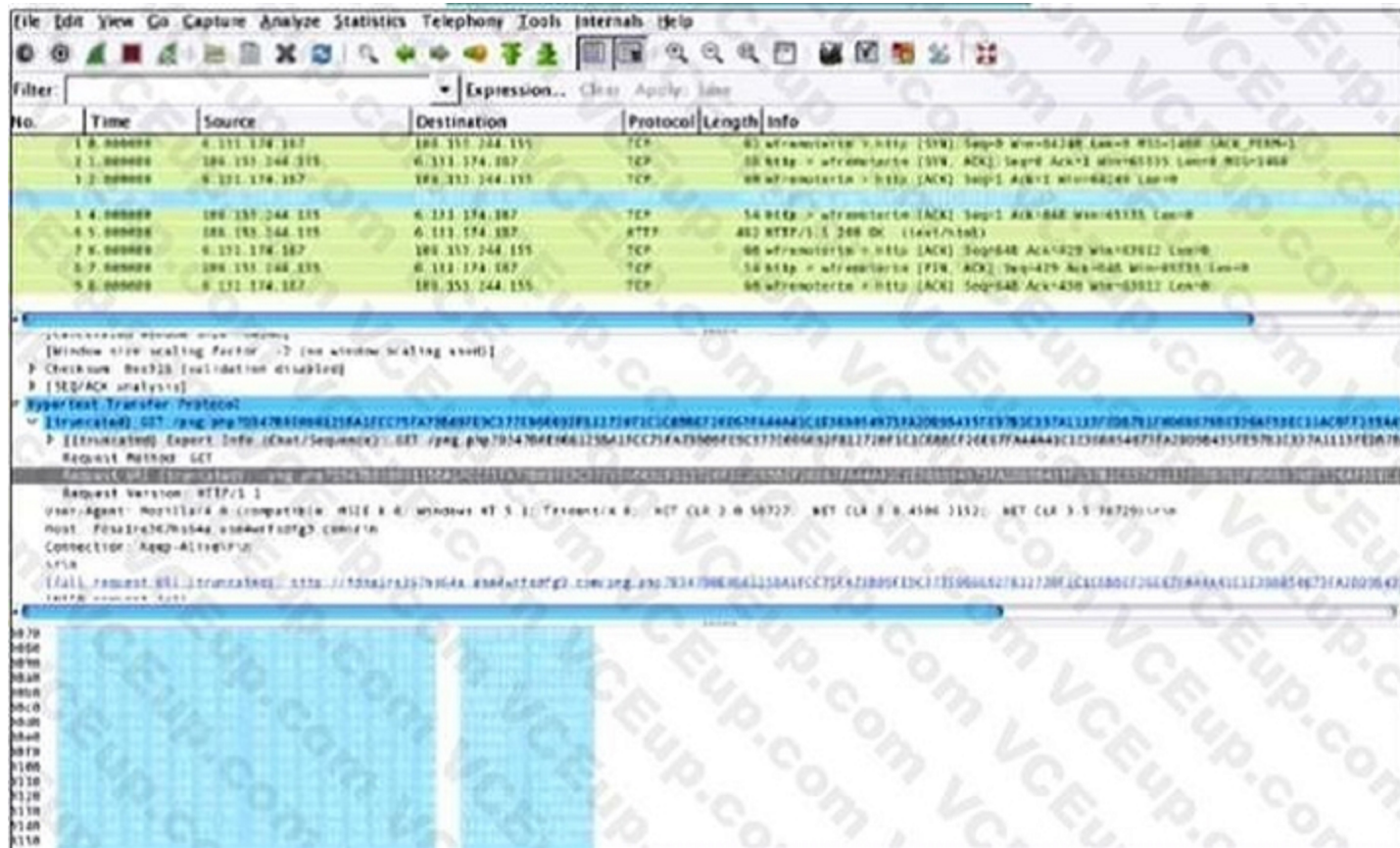
After a breach has been discovered and the immediate threat has been addressed by identifying and removing the threat's access, the next step according to the NIST SP 800-61 Incident Handling Guide is to recover from the threat. This involves restoring systems to normal operation, confirming that the systems are functioning normally, and applying patches or other remediation measures to prevent similar breaches in the future.

Understanding NIST SP 800-61: The Computer Security Incident Handling Guide

QUESTION 73

Refer to the exhibit.





What is shown in this PCAP file?

- A. Timestamps are indicated with error.
- B. The protocol is TCP.
- C. The User-Agent is Mozilla/5.0.
- D. The HTTP GET is encoded.



Correct Answer: C

Section:

Explanation:

The PCAP file shows a network packet capture of an HTTP GET request from a client to a server. The User-Agent header field identifies the type and version of the client software that generated the request. In this case, the User-Agent is Mozilla/5.0, which indicates that the client is using a Mozilla-based browser or application. The User-Agent can help the server to customize the response based on the client's capabilities and preferences. Reference: Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) v1.0, Module 3: Network Protocols and Services, Lesson 3.2: HTTP and HTTPS, Topic 3.2.1: HTTP Headers.

1of30

QUESTION 74

What is a difference between tampered and untampered disk images?

- A. Tampered images have the same stored and computed hash.
- B. Tampered images are used as evidence.
- C. Untampered images are used for forensic investigations.
- D. Untampered images are deliberately altered to preserve as evidence

Correct Answer: C

Section:

Explanation:

Tampered images are disk images that have been modified or altered in some way after they were captured from the original source. Tampered images may have different stored and computed hash values, which indicate that the integrity of the image has been compromised. Tampered images are not reliable or valid sources of evidence for forensic investigations, as they may contain false or misleading information. Untampered images are disk images that have not been changed or manipulated after they were acquired from the original source. Untampered images have the same stored and computed hash values, which verify that the image is an exact copy of the original disk. Untampered images are used for forensic investigations, as they preserve the original state and content of the disk and provide accurate and trustworthy evidence. Reference:

Contrasting tampered and untampered disk images

What is a difference between tampered and untampered disk images?

QUESTION 75

The SOC team has confirmed a potential indicator of compromise on an endpoint. The team has narrowed the executable file's type to a new trojan family. According to the NIST Computer Security Incident Handling Guide, what is the next step in handling this event?

- A. Isolate the infected endpoint from the network.
- B. Perform forensics analysis on the infected endpoint.
- C. Collect public information on the malware behavior.
- D. Prioritize incident handling based on the impact.

Correct Answer: C

Section:

Explanation:

According to the NIST Computer Security Incident Handling Guide, the next step in handling an event after confirming a potential indicator of compromise on an endpoint is to collect public information on the malware behavior. This step involves searching for information from various sources, such as antivirus vendors, security blogs, threat intelligence feeds, and online forums, to learn more about the characteristics, capabilities, and impact of the malware. This information can help the SOC team to identify the type, severity, and scope of the incident, as well as to determine the appropriate response actions and mitigation strategies. Isolating the infected endpoint, performing forensics analysis, and prioritizing incident handling are subsequent steps that follow after collecting public information on the malware behavior. Reference:

Computer Security Incident Handling Guide

SP 800-61 Rev. 2, Computer Security Incident Handling Guide



QUESTION 76

Which technology on a host is used to isolate a running application from other applications?

- A. sandbox
- B. application allow list
- C. application block list
- D. host-based firewall

Correct Answer: A

Section:

Explanation:

A sandbox is a technology on a host that is used to isolate a running application from other applications. A sandbox creates a controlled and restricted environment for the application to execute, limiting its access to system resources and data. A sandbox can prevent the application from spreading malware, stealing information, or causing damage to the host or the network. A sandbox can also be used to test and analyze the behavior of unknown or suspicious applications without risking the security of the host. Application allow list, application block list, and host-based firewall are other technologies on a host that can be used to control or restrict the execution of applications, but they do not isolate them from other applications. Reference:

How can I best isolate a particular program (game)

App isolation in Windows 10

Types of Endpoint Application Isolation and Containment Technology

QUESTION 77

An analyst received a ticket regarding a degraded processing capability for one of the HR department's servers. On the same day, an engineer noticed a disabled antivirus software and was not able to determine when or why it occurred. According to the NIST Incident Handling Guide, what is the next phase of this investigation?

- A. Recovery
- B. Detection
- C. Eradication
- D. Analysis

Correct Answer: D

Section:

Explanation:

According to the NIST Incident Handling Guide, the analysis phase is the next phase of this investigation. The analysis phase involves examining the evidence and determining the impact, scope, and cause of the incident. The analyst should also identify the attacker's methods, tools, and objectives, as well as any indicators of compromise or malicious activity. The analysis phase may also involve collecting additional data, such as logs, network traffic, or malware samples, to support the investigation. The analysis phase is crucial for developing an effective response and recovery strategy, as well as preventing or mitigating future incidents. Reference:

NIST Special Publication 800-61 Revision 2, Computer Security Incident Handling Guide, Section 3.2.4, Analysis (<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>)

Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) v1.0, Module 5: Security Incident Response, Lesson 5.2: Incident Response Process, Topic 5.2.3: Analysis Phase (<https://learningnetworkstore.cisco.com/on-demand-e-learning/understanding-cisco-cybersecurity-operations-fundamentals-cbrops-v1-0/CSCU-LP-CBROPS-V1-028093.html>)

QUESTION 78

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

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

Correct Answer: B

Section:

Explanation:

Session data is the data type that is necessary to get information about source/destination ports. Session data is the information about connections between hosts, such as IP addresses, ports, protocols, and duration. Session data can be used to identify the services and applications that are being used on the network, as well as the direction and volume of the traffic. Session data can also help to detect anomalous or malicious behavior, such as port scanning, brute force attacks, or data exfiltration. Session data can be collected from various sources, such as firewalls, routers, switches, or network monitoring tools. Reference:

Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) v1.0, Module 2: Security Monitoring, Lesson 2.2: Data Sources, Topic 2.2.2: Session Data (<https://learningnetworkstore.cisco.com/on-demand-e-learning/understanding-cisco-cybersecurity-operations-fundamentals-cbrops-v1-0/CSCU-LP-CBROPS-V1-028093.html>)

Cisco Certified CyberOps Associate Certification Guide, Chapter 3: Data Sources, Section 3.2: Session Data (<https://www.ciscopress.com/store/cisco-certified-cyberops-associate-certification-guide-9780136807834>)

<https://www.ibm.com/docs/en/networkmanager/4.2.0?topic=relationships-connectivity-data>

QUESTION 79

Refer to the exhibit.



```
SELECT * FROM people WHERE username = " OR '1'='1';
```

Which type of attack is being executed?

- A. SQL injection
- B. cross-site scripting

- C. cross-site request forgery
- D. command injection

Correct Answer: A

Section:

Explanation:

The exhibit shows a SQL query that is attempting to bypass login controls by modifying the query to always return true. This is a common tactic used in SQL injection attacks where malicious SQL statements are inserted into an entry field for execution. Reference: Cisco Cybersecurity Source Documents

QUESTION 80

What describes the concept of data consistently and readily being accessible for legitimate users?

- A. integrity
- B. availability
- C. accessibility
- D. confidentiality

Correct Answer: B

Section:

Explanation:

Availability is one of the three pillars of the CIA triad, a model that defines the principles of information security. Availability describes the concept of data consistently and readily being accessible for legitimate users. Availability ensures that the network and systems are operational and resilient to disruptions, such as denial-of-service attacks, hardware failures, or natural disasters. Availability also involves maintaining backup and recovery procedures, load balancing, and redundancy mechanisms. Reference:

Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) - Cisco, Module 1: Security Concepts, Lesson 1.1: Security Principles
 200-201 CBROPS - Cisco, Exam Topics, 1.0 Security Concepts, 1.1 Explain the CIA triad
 Cisco Certified CyberOps Associate Overview - Cisco Learning Network, Videos, 1.1 Explain the CIA triad

QUESTION 81

Refer to the exhibit.

No.	Time	Source	Destination	Protocol	Length	Info
6	16:40:35.636314	195.144.107.198	192.168.31.44	FTP	104	Response: 227 Entering Passive Mode (195,144,107,108,4,2).
7	16:40:35.637786	192.168.31.44	195.144.107.198	FTP	82	Request: RETR ResumableTransfer.png
8	16:40:35.638091	192.168.31.44	195.144.107.198	TCP	66	1084 → 1026 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
9	16:40:35.696788	195.144.107.198	192.168.31.44	FTP	96	Response: 150 Opening BINARY mode data connection.
10	16:40:35.698384	195.144.107.198	192.168.31.44	TCP	66	1026 → 1084 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1456 WS=256 SACK
11	16:40:35.698521	192.168.31.44	195.144.107.198	TCP	54	1084 → 1026 [ACK] Seq=1 Ack=1 Win=132352 Len=0
12	16:40:35.698802	192.168.31.44	195.144.107.198	TCP	54	[TCP Window Update] 1084 → 1026 [ACK] Seq=1 Ack=1 Win=4194304 Len=0
13	16:40:35.739249	192.168.31.44	195.144.107.198	TCP	54	1031 → 21 [ACK] Seq=43 Ack=113 Win=513 Len=0
14	16:40:35.759825	195.144.107.198	192.168.31.44	FTP	2966	FTP Data: 2912 bytes (PASV) (RETR ResumableTransfer.png)
15	16:40:35.759925	192.168.31.44	195.144.107.198	TCP	54	1084 → 1026 [ACK] Seq=1 Ack=2913 Win=4194304 Len=0
16	16:40:35.822152	195.144.107.198	192.168.31.44	FTP	5878	FTP Data: 5824 bytes (PASV) (RETR ResumableTransfer.png)
17	16:40:35.822263	192.168.31.44	195.144.107.198	TCP	54	1084 → 1026 [ACK] Seq=1 Ack=8737 Win=4194304 Len=0
18	16:40:35.883496	195.144.107.198	192.168.31.44	FTP	1510	FTP Data: 1456 bytes (PASV) (RETR ResumableTransfer.png)
19	16:40:35.883496	195.144.107.198	192.168.31.44	FTP	1408	FTP Data: 1354 bytes (PASV) (RETR ResumableTransfer.png)
20	16:40:35.883559	192.168.31.44	195.144.107.198	TCP	54	1084 → 1026 [ACK] Seq=1 Ack=11547 Win=4194304 Len=0
21	16:40:35.944841	195.144.107.198	192.168.31.44	FTP	78	Response: 226 Transfer complete.
22	16:40:35.944841	195.144.107.198	192.168.31.44	TCP	54	1026 → 1084 [FIN, ACK] Seq=11547 Ack=1 Win=66816 Len=0
23	16:40:35.944978	192.168.31.44	195.144.107.198	TCP	54	1084 → 1026 [ACK] Seq=1 Ack=11548 Win=4194304 Len=0
24	16:40:35.945371	192.168.31.44	195.144.107.198	TCP	54	1084 → 1026 [FIN, ACK] Seq=1 Ack=11548 Win=4194304 Len=0

Frame 21: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface \Device\NPF_{E75C8230-809F-487C-B722-948D6CF16174}, id 0
 Ethernet II, Src: BeijingX_06:3f:00 (50:d2:f5:06:3f:00), Dst: IntelCor_7c:b2:fd (18:26:49:7c:b2:fd)
 Internet Protocol Version 4, Src: 195.144.107.198, Dst: 192.168.31.44
 Transmission Control Protocol, Src Port: 21, Dst Port: 1031, Seq: 113, Ack: 43, Len: 24
 File Transfer Protocol (FTP)
 [Current working directory:]

Which frame numbers contain a file that is extractable via TCP stream within Wireshark?

- A. 7,14, and 21
- B. 7 and 21
- C. 14,16,18, and 19
- D. 7 to 21

Correct Answer: A

Section:

Explanation:

The file that is extractable via TCP stream within Wireshark is the one that has the Content-Type header set to application/octet-stream, which indicates binary data. This header is present in frames 7, 14, and 21, which are part of the same TCP stream. The other frames have different Content-Type headers, such as text/html or image/jpeg, which are not extractable as binary files. Reference:= Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) v1.0, Module 3: Network Intrusion Analysis, Lesson 3.2: Analyze Data from Common TCP/IP Protocols, Topic 3.2.3: HTTP

QUESTION 82

Refer to the exhibit.

Employee Name	Role
Employee 1	Chief Accountant
Employee 2	Head of Managed Cyber Security Services
Employee 3	System Administration
Employee 4	Security Operation Center Analyst
Employee 5	Head of Network & Security Infrastructure Services
Employee 6	Financial Manager
Employee 7	Technical Director



Which stakeholders must be involved when a company workstation is compromised?

- A. Employee 1 Employee 2, Employee 3, Employee 4, Employee 5, Employee 7
- B. Employee 1, Employee 2, Employee 4, Employee 5
- C. Employee 4, Employee 6, Employee 7
- D. Employee 2, Employee 3, Employee 4, Employee 5

Correct Answer: C

Section:

Explanation:

When a company workstation is compromised, the stakeholders that must be involved are the ones who are responsible for the security incident response process. According to the table, these are Employee 4 (Security Operation Center Analyst), Employee 6 (Head of Network and Security Infrastructure Services), and Employee 7 (Technical Director). The other employees have different roles that are not directly related to the incident response process, such as accounting, financial management, or system administration. Reference:= Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) v1.0, Module 1: Security Concepts, Lesson 1.4: Security Monitoring, Topic 1.4.1: Security Operations Center

QUESTION 83

How does an attack surface differ from an attack vector?

- A. An attack vector recognizes the potential outcomes of an attack, and the attack surface is choosing a method of an attack.
- B. An attack surface identifies vulnerable parts for an attack, and an attack vector specifies which attacks are feasible to those parts.

- C. An attack surface mitigates external vulnerabilities, and an attack vector identifies mitigation techniques and possible workarounds.
- D. An attack vector matches components that can be exploited, and an attack surface classifies the potential path for exploitation

Correct Answer: B

Section:

Explanation:

An attack surface is the sum of all the points where an attacker can try to enter or extract data from an environment. It includes all the hardware, software, network, and human components that are exposed to potential threats. An attack vector is the path or means by which an attacker can exploit a vulnerability in the attack surface. It describes the type, source, and technique of an attack, such as phishing, malware, denial-of-service, etc. Reference:= Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) v1.0, Module 1: Security Concepts, Lesson 1.1: The CIA Triad and Security Concepts, Topic 1.1.3: Threats, Vulnerabilities, and Exploits

QUESTION 84

Which attack represents the evasion technique of resource exhaustion?

- A. SQL injection
- B. man-in-the-middle
- C. bluesnarfing
- D. denial-of-service

Correct Answer: D

Section:

Explanation:

A denial-of-service attack represents the evasion technique of resource exhaustion, where the attacker overwhelms a system's resources, making the system unusable and unable to handle legitimate requests. Reference:=Cisco Cybersecurity Source Documents

QUESTION 85

A threat actor penetrated an organization's network. Using the 5-tuple approach, which data points should the analyst use to isolate the compromised host in a grouped set of logs?

- A. event name, log source, time, source IP, and host name
- B. protocol, source IP, source port, destination IP, and destination port
- C. event name, log source, time, source IP, and username
- D. protocol, log source, source IP, destination IP, and host name

Correct Answer: B

Section:

Explanation:

The 5-tuple approach consists of protocol, source IP address, source port number, destination IP address, and destination port number to uniquely identify sessions between endpoints on a network. Reference:=Cisco Cybersecurity Source Documents

QUESTION 86

Which regular expression is needed to capture the IP address 192.168.20.232?

- A. `^(?:[0-9]{1,3}\.){3}[0-9]{1,3}`
- B. `^(?:[0-9]{1,3}\.){1,4}`
- C. `^(?:[0-9]{1,3}\.).'`
- D. `^([0-9]{-3})`

Correct Answer: A

Section:

Explanation:

The regular expression `^(?:[0-9]{1,3}){3}[0-9]{1,3}` is needed to capture the IP address 192.168.20.232. This regex matches any string that starts with three groups of one to three digits followed by a dot, and ends with one group of one to three digits. The IP address 192.168.20.232 matches this pattern exactly. The other options are either invalid or do not match the IP address format. Reference:= Cisco Cybersecurity Operations Fundamentals, Module 5: Security Policies and Procedures, Lesson 5.3: Data and Event Analysis, Topic 5.3.2: Regular Expressions

QUESTION 87

How does a certificate authority impact security?

- A. It validates client identity when communicating with the server.
- B. It authenticates client identity when requesting an SSL certificate.
- C. It authenticates domain identity when requesting an SSL certificate.
- D. It validates the domain identity of the SSL certificate.

Correct Answer: D

Section:

Explanation:

A certificate authority (CA) is a trusted entity that issues and manages digital certificates for secure communication over the internet. A digital certificate is a document that contains the public key and the identity of the owner of the key. A CA impacts security by validating the domain identity of the SSL certificate, which is a type of digital certificate that enables encrypted communication between a web server and a web browser. The CA verifies that the domain name in the certificate matches the domain name of the web server, and signs the certificate with its own private key. The web browser can then verify the signature of the CA and trust the identity of the web server. Reference:= Cisco Cybersecurity Operations Fundamentals, Module 2: Security Monitoring, Lesson 2.3: Cryptography and PKI, Topic 2.3.2: Public Key Infrastructure Reference: https://en.wikipedia.org/wiki/Certificate_authority

QUESTION 88

What is a difference between SIEM and SOAR?

- A. SOAR predicts and prevents security alerts, while SIEM 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. SIEM predicts and prevents security alerts, while SOAR checks attack patterns and applies the mitigation.
- D. SOAR's primary function is to collect and detect anomalies, while SIEM is more focused on security operations automation and response.

Correct Answer: B

Section:

Explanation:

SIEM (Security Information and Event Management) systems are solutions that provide real-time analysis of security alerts generated by applications and network hardware. They collect, store, analyze, and report on log data for incident response, forensics, and regulatory compliance. On the other hand, SOAR (Security Orchestration Automation and Response) platforms allow organizations to collect data about security threats from multiple sources and respond to low-level security events without human assistance. Reference: Cisco Cybersecurity Operations Fundamentals

QUESTION 89

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.

Correct Answer: B

Section:

Explanation:

Behavior-based detection monitors the behavior of programs in real-time. If a piece of software acts similarly to known malware after it's been executed, behavior-based detection can stop it in its tracks. Signature-based detection involves searching for known patterns of data within executable code; if a pattern matches a "signature" in the system's database that is considered malicious. Reference: Cisco Cybersecurity Operations Fundamentals

QUESTION 90

Refer to the exhibit.

```
#Time Format: Local
#Fields: date time action protocol src-ip dst-ip src-port dst-port size tcpflags tcpsyn tcpack tcpwin icmptype icmcode info path
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63064 135 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.14 63065 49156 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63066 65386 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63067 389 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW UDP 10.40.4.182 10.40.1.14 62292 389 0 - - - - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63068 389 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63069 445 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW UDP 10.40.4.182 10.40.1.13 62293 389 0 - - - - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.13 63070 88 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63071 445 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63072 445 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63073 445 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.13 63074 88 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.13 63075 88 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.13 63076 88 0 - 0 0 0 - - - SEND
2015-07-16 11:35:27 ALLOW UDP 10.40.4.182 10.40.1.11 55053 53 0 - - - - - - SEND
2015-07-16 11:35:27 ALLOW UDP 10.40.4.182 10.40.1.11 50845 53 0 - - - - - - SEND
2015-07-16 11:35:30 ALLOW UDP fe80::29ea:1a3c:24d6:fb49 ff02::1:3 57333 5355 0 - - - - - - RECEIVE
2015-07-16 11:35:30 ALLOW UDP 10.40.4.252 224.0.0.252 59629 5355 0 - - - - - - RECEIVE
2015-07-16 11:35:30 ALLOW UDP fe80::4c2e:505d:b3a7:caaf ff02::1:3 58846 5355 0 - - - - - - SEND
2015-07-16 11:35:30 ALLOW UDP 10.40.4.182 224.0.0.252 58846 5355 0 - - - - - - SEND
2015-07-16 11:35:31 ALLOW UDP 10.40.4.182 224.0.0.252 137 137 0 - - - - - - SEND
2015-07-16 11:35:31 ALLOW UDP fe80::4c2e:505d:b3a7:caaf ff02::1:3 63504 5355 0 - - - - - - SEND
2015-07-16 11:35:31 ALLOW UDP 10.40.4.182 224.0.0.252 63504 5355 0 - - - - - - SEND
```

An engineer received an event log file to review. Which technology generated the log?

- A. NetFlow
- B. proxy
- C. firewall
- D. IDS/IPS



Correct Answer: D

Section:

Explanation:

The exhibit shows an event log file with fields like date time action protocol src-ip dst-ip src-port dst-port etc., which are typical in Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS). These systems monitor network traffic for suspicious activity or violations of policies and produce reports as seen in the exhibit. Reference: Cisco Certified CyberOps Associate Overview

QUESTION 91

What is the difference between inline traffic interrogation and traffic mirroring?

- A. Inline interrogation is less complex as traffic mirroring applies additional tags to data.
- B. Traffic mirroring copies the traffic rather than forwarding it directly to the analysis tools
- C. Inline replicates the traffic to preserve integrity rather than modifying packets before sending them to other analysis tools.
- D. Traffic mirroring results in faster traffic analysis and inline is considerably slower due to latency.

Correct Answer: B

Section:

Explanation:

Traffic mirroring is a technique that copies the traffic from a source port or VLAN to a destination port or VLAN, where it can be analyzed by a security device or tool. Traffic mirroring does not affect the original traffic flow and

does not introduce any latency or modification to the packets. Inline traffic interrogation is a technique that forwards the traffic directly to the security device or tool, where it can be inspected and modified before being sent to the destination. Inline traffic interrogation can introduce latency and affect the performance of the network. Reference:

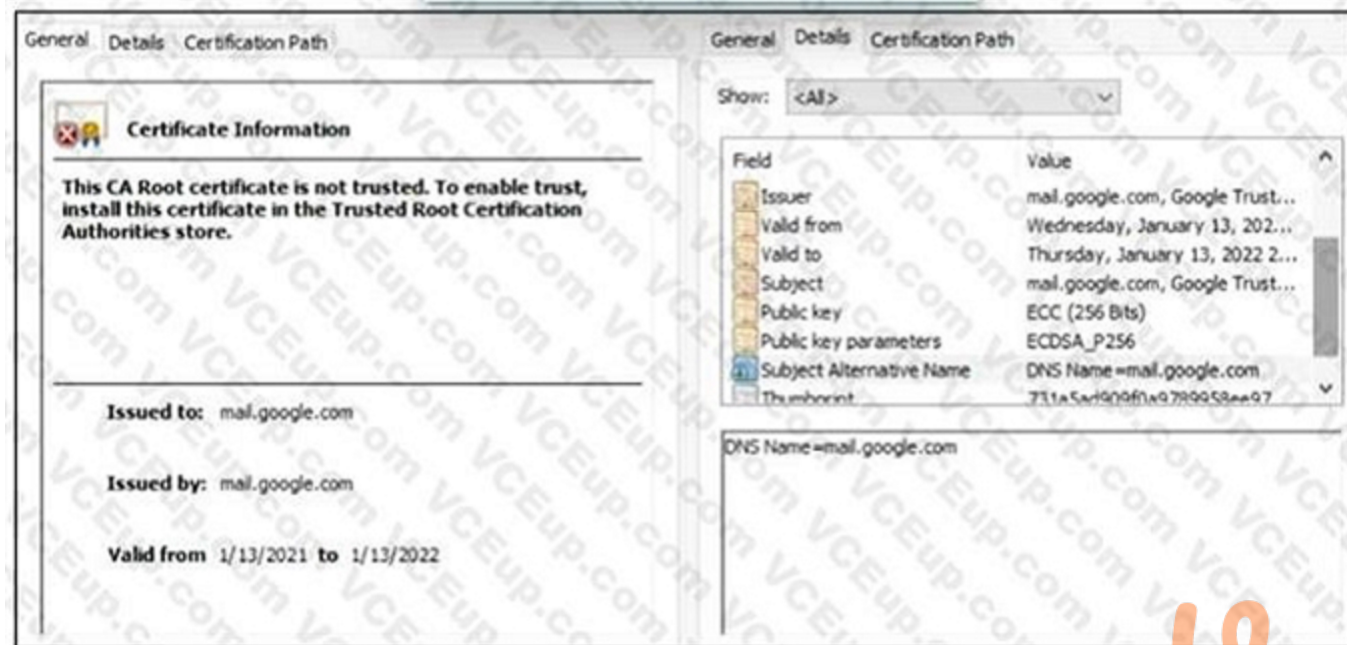
Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) - Cisco, Module 2: Security Monitoring, Lesson 2.2: Network Security Monitoring Tools

200-201 CBROPS - Cisco, Exam Topics, 2.0 Security Monitoring, 2.2 Describe the impact of various technologies on security monitoring

Cisco Certified CyberOps Associate Overview - Cisco Learning Network, Videos, 2.2 Describe the impact of various technologies on security monitoring

QUESTION 92

Refer to the exhibit.



A company employee is connecting to mail.google.com from an endpoint device. The website is loaded but with an error. What is occurring?

- A. DNS hijacking attack
- B. Endpoint local time is invalid.
- C. Certificate is not in trusted roots.
- D. man-in-the-middle attack

Correct Answer: D

Section:

Explanation:

A man-in-the-middle attack is a type of cyberattack where an attacker intercepts and alters the communication between two parties who believe they are directly communicating with each other. In this case, the attacker is impersonating mail.google.com and presenting a fake certificate to the endpoint device. The endpoint device detects that the certificate is not issued by a trusted authority and displays an error message. The attacker can then monitor or modify the traffic between the endpoint device and mail.google.com. Reference:

Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) - Cisco, Module 3: Host-Based Analysis, Lesson 3.2: Endpoint Security Technologies

200-201 CBROPS - Cisco, Exam Topics, 3.0 Host-Based Analysis, 3.2 Compare and contrast the functionality of these endpoint security technologies

Cisco Certified CyberOps Associate Overview - Cisco Learning Network, Videos, 3.2 Compare and contrast the functionality of these endpoint security technologies

QUESTION 93

An analyst is using the SIEM platform and must extract a custom property from a Cisco device and capture the phrase, 'File: Clean.' Which regex must the analyst import?

- A. File: Clean
- B. ^Parent File Clean\$
- C. File: Clean (.*)
- D. ^File: Clean\$

Correct Answer: A

Section:

Explanation:

A regular expression (regex) is a sequence of characters that defines a search pattern for text. A regex can be used to extract custom properties from log messages or events in a SIEM platform. In this case, the regex that matches the phrase "File: Clean" exactly is ^File: Clean\$. The ^ symbol indicates the beginning of the line and the \$ symbol indicates the end of the line. The regex ensures that no other characters are before or after the phrase. Reference:

Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) - Cisco, Module 5: Security Policies and Procedures, Lesson 5.3: Data and Event Analysis

200-201 CBROPS - Cisco, Exam Topics, 5.0 Security Policies and Procedures, 5.3 Analyze data as part of security monitoring activities

Cisco Certified CyberOps Associate Overview - Cisco Learning Network, Videos, 5.3 Analyze data as part of security monitoring activities

QUESTION 94

How does TOR alter data content during transit?

- A. It spoofs the destination and source information protecting both sides.
- B. It encrypts content and destination information over multiple layers.
- C. It redirects destination traffic through multiple sources avoiding traceability.
- D. It traverses source traffic through multiple destinations before reaching the receiver

Correct Answer: B

Section:

Explanation:

TOR is a network that enables anonymous communication over the internet by routing the traffic through a series of relays or nodes. TOR alters the data content during transit by encrypting it and the destination information over multiple layers, using a technique called onion routing. Each layer of encryption can only be decrypted by a specific relay in the network, which reveals the next destination. This way, no single relay knows the complete path or the content of the data, making it difficult to trace or monitor the communication. Reference: Cisco Cybersecurity Operations Fundamentals, Module 2: Security Monitoring, Lesson 2.1: The Network as a Sensor, Topic 2.1.3: Network Data Exfiltration Techniques

QUESTION 95

Refer to the exhibit.

```
192.168.10.10 -- [01/Dec/2020:11:12:22 -0200] "GET /icons/powered_by_rh.png HTTP/1.1" 200 1213 "http://192.168.0.102/" "Mozilla/5.0 (X11; U; Linux x86_64; en-US; rv:1.9.0.12) Gecko/2009070812 Ubuntu/8.04 (hardy) Firefox/3.0.12"
192.168.10.10 -- [01/Dec/2020:11:13:15 -0200] "GET /favicon.ico HTTP/1.1" 404 288 "-" "Mozilla/5.0 (X11; U; Linux x86_64; en-US; rv:1.9.0.12) Gecko/2009070812 Ubuntu/8.04 (hardy) Firefox/3.0.12"
192.168.10.10 -- [01/Dec/2020:11:14:22 -0200] "GET /%27%27;!-%22%3CXSS%3E=&{0} HTTP/1.1" 404 310 "-" "Mozilla/5.0 (X11; U; Linux x86_64; en-US; rv:1.9.0.12) Gecko/2009070812 Ubuntu/8.04 (hardy) Firefox/3.0.12"
```

What is occurring?

- A. Cross-Site Scripting attack
- B. XML External Entities attack

- C. Insecure Deserialization
- D. Regular GET requests

Correct Answer: A

Section:

Explanation:

The exhibit shows a log of HTTP GET requests, one of which includes a suspicious string that is indicative of a Cross-Site Scripting (XSS) attack. XSS attacks involve injecting malicious scripts into webpages viewed by other users. These scripts can be used to steal information, redirect users to malicious websites, or perform actions on behalf of the user without their consent. Reference: Cisco Cybersecurity Operations Fundamentals, Module 1: Security Concepts, Lesson 1.3: Common Network Application Operations and Attacks, Topic 1.3.2: Web Application Attacks

QUESTION 96

What is a collection of compromised machines that attackers use to carry out a DDoS attack?

- A. subnet
- B. botnet
- C. VLAN
- D. command and control

Correct Answer: B

Section:

Explanation:

A botnet is a network of compromised computers controlled by an attacker. Botnets are often used to carry out Distributed Denial of Service (DDoS) attacks, where the compromised machines are directed to flood a target with traffic, rendering it inaccessible. Reference: Cisco Cybersecurity Operations Fundamentals, Module 1: Security Concepts, Lesson 1.3: Common Network Application Operations and Attacks, Topic 1.3.4: Denial-of-Service Attacks



QUESTION 97

Which type of access control depends on the job function of the user?

- A. discretionary access control
- B. nondiscretionary access control
- C. role-based access control
- D. rule-based access control

Correct Answer: C

Section:

Explanation:

Role-Based Access Control (RBAC) is an approach to restricting system access to authorized users based on their roles within an organization. It depends on the job functions that individual users have as part of their responsibilities and is designed to reduce administrative work by assigning roles based on job competency, authority, and responsibility. Reference: Cisco Cybersecurity Operations Fundamentals, Module 1: Security Concepts, Lesson 1.2: Data Protection, Topic 1.2.2: Access Control Models

QUESTION 98

The security team has detected an ongoing spam campaign targeting the organization. The team's approach is to push back the cyber kill chain and mitigate ongoing incidents. At which phase of the cyber kill chain should the security team mitigate this type of attack?

- A. actions
- B. delivery
- C. reconnaissance
- D. installation

Correct Answer: B

Section:

Explanation:

In the context of the cyber kill chain model, spam campaigns fall under the "delivery" phase where attackers deliver malicious payloads via email or other means to target systems or networks. Reference: Cisco Cybersecurity Operations Fundamentals, Module 1: Security Concepts, Lesson 1.4: Security Monitoring, Topic 1.4.2: The Cyber Kill Chain Model

QUESTION 99

What describes the defense-in-depth principle?

- A. defining precise guidelines for new workstation installations
- B. categorizing critical assets within the organization
- C. isolating guest Wi-Fi from the focal network
- D. implementing alerts for unexpected asset malfunctions

Correct Answer: D

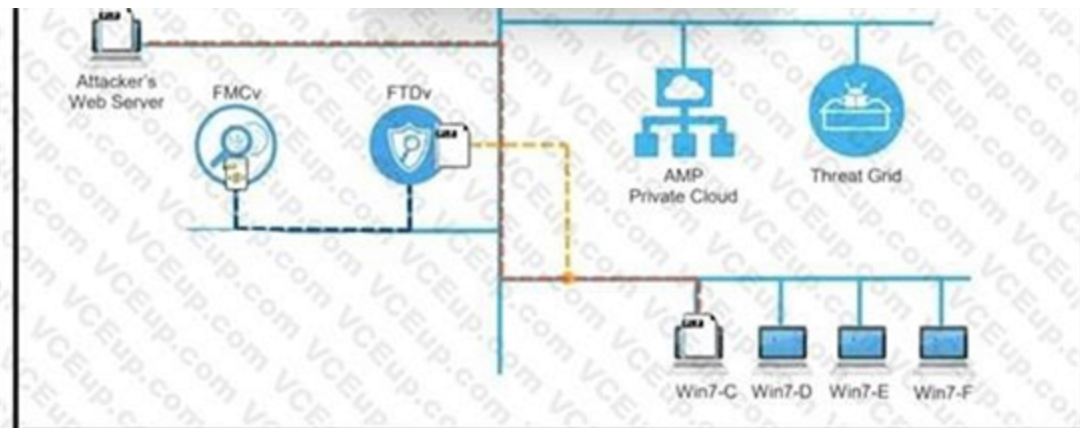
Section:

Explanation:

The defense-in-depth principle is a strategy of applying multiple layers of security controls to protect an asset from threats. It is based on the assumption that no single security measure is sufficient to prevent all attacks, and that each layer adds more protection and reduces the risk of compromise. One example of applying the defense-in-depth principle is implementing alerts for unexpected asset malfunctions, which can indicate a potential security breach or incident. Reference: Cisco Cybersecurity Operations Fundamentals, Module 1: Security Concepts, Lesson 1.1: The CIA Triad and Security Concepts, Topic 1.1.4: Defense-in-Depth Principle

QUESTION 100

Refer to the exhibit.



vdumps

A workstation downloads a malicious docx file from the Internet and a copy is sent to FTDv. The FTDv sends the file hash to FMC and the tile event is recorded what would have occurred with stronger data visibility.

- A. The traffic would have been monitored at any segment in the network.
- B. Malicious traffic would have been blocked on multiple devices
- C. An extra level of security would have been in place
- D. Detailed information about the data in real time would have been provided

Correct Answer: D

Section:

Explanation:

With stronger data visibility, detailed information about the data in real-time is provided. This enhanced visibility allows for a more comprehensive analysis of network traffic, enabling security professionals to identify and mitigate threats more effectively. Reference: Cisco Cybersecurity Operations Fundamentals

QUESTION 101

What is the impact of encryption?

- A. Confidentiality of the data is kept secure and permissions are validated
- B. Data is accessible and available to permitted individuals
- C. Data is unaltered and its integrity is preserved
- D. Data is secure and unreadable without decrypting it

Correct Answer: D

Section:

Explanation:

Encryption ensures that data is secure and unreadable to unauthorized individuals without the proper decryption key. It is a critical aspect of maintaining data confidentiality and security, especially in the transmission of sensitive information over potentially insecure networks.

QUESTION 102

An engineer is analyzing a recent breach where confidential documents were altered and stolen by the receptionist. Further analysis shows that the threat actor connected an external USB device to bypass security restrictions and steal data. The engineer could not find an external USB device. Which piece of information must an engineer use for attribution in an investigation?

- A. list of security restrictions and privileges boundaries bypassed
- B. external USB device
- C. receptionist and the actions performed
- D. stolen data and its criticality assessment

Correct Answer: C

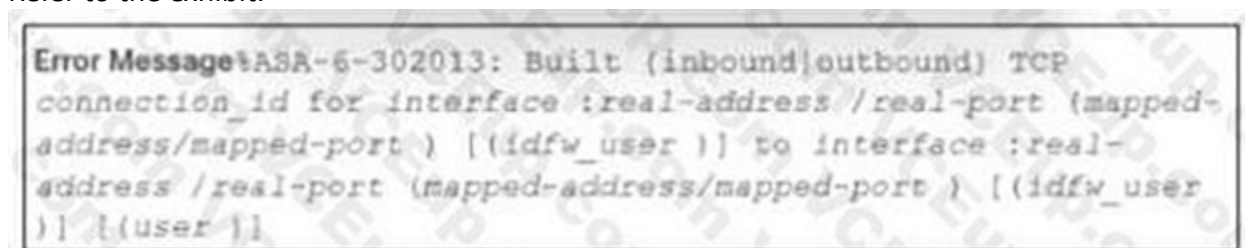
Section:

Explanation:

In the context of a cybersecurity breach, attribution involves identifying the responsible party. Since the external USB device was not found, the focus shifts to the actions performed by the receptionist. Analyzing these actions can provide insights into how the breach occurred and may help in attributing the incident to the threat actor.

QUESTION 103

Refer to the exhibit.



```
Error Message: ASA-6-302013: Built (inbound|outbound) TCP
connection_id for interface :real-address /real-port (mapped-
address/mapped-port) [(idfw_user)] to interface :real-
address /real-port (mapped-address/mapped-port) [(idfw_user
)] [(user)]
```

During the analysis of a suspicious scanning activity incident, an analyst discovered multiple local TCP connection events. Which technology provided these logs?

- A. antivirus
- B. proxy
- C. IDS/IPS
- D. firewall

Correct Answer: D

Section:

Explanation:

The logs indicating multiple local TCP connection events are typically provided by a firewall. Firewalls are responsible for monitoring and controlling incoming and outgoing network traffic based on predetermined security

rules, and they generate logs that detail such events, which can be used for further analysis and incident response. Reference:= Cisco Cybersecurity Operations Fundamentals

QUESTION 104

Refer to the exhibit.

No.	Time	Source	Destination	Protocol	Length	Info
27336	245.7615440	192.168.154.129	192.168.154.131	FTP	79	Request: USER bjones
27337	245.7615820	192.168.154.129	192.168.154.131	FTP	79	Request: USER bjones
27338	245.7616210	192.168.154.129	192.168.154.131	FTP	79	Request: USER bjones
27340	245.7616680	192.168.154.129	192.168.154.131	FTP	80	Request: PASS blinkley
27343	245.7617170	192.168.154.129	192.168.154.131	FTP	84	Request: PASS bloomcounty
27344	245.7617400	192.168.154.131	192.168.154.129	FTP	100	Response: 331 Please specify the password.
27345	245.7617580	192.168.154.129	192.168.154.131	FTP	78	Request: PASS brown
27346	245.7617890	192.168.154.131	192.168.154.129	FTP	100	Response: 331 Please specify the password.
27347	245.7618140	192.168.154.129	192.168.154.131	FTP	78	Request: PASS bloom
27348	245.7618360	192.168.154.131	192.168.154.129	FTP	100	Response: 331 Please specify the password.
27349	245.7618550	192.168.154.129	192.168.154.131	FTP	80	Request: PASS blondie
27350	245.7618920	192.168.154.129	192.168.154.131	FTP	77	Request: PASS capp
27351	245.7653470	192.168.154.129	192.168.154.131	FTP	79	Request: PASS caucas
27352	245.7692450	192.168.154.129	192.168.154.131	FTP	80	Request: PASS cerebus
27353	245.7693080	192.168.154.129	192.168.154.131	FTP	81	Request: PASS catwoman
27355	245.7771480	192.168.154.131	192.168.154.129	FTP	88	Response: 530 Login incorrect.
27356	245.7772540	192.168.154.131	192.168.154.129	FTP	88	Response: 530 Login incorrect.

An analyst was given a PCAP file, which is associated with a recent intrusion event in the company FTP server Which display filters should the analyst use to filter the FTP traffic?

- A. dstport == FTP
- B. tcp.port==21
- C. tcpport = FTP
- D. dstport = 21

Correct Answer: B

Section:

Explanation:

The correct display filter for analyzing FTP traffic in a PCAP file is "tcp.port==21". This filter will show all TCP packets where the port number is 21, which is the standard port for FTP control messages.



QUESTION 105

Refer to the exhibit.

No.	Time	Source	Destination	Protocol	Length	Info
14	27.405297	192.168.1.83	192.168.1.80	HTTP	335	GET /news.php HTTP/1.1
14	27.423516	192.168.1.80	192.168.1.83	HTTP	12	HTTP/1.0 200 OK (text/html)
14	27.843983	192.168.1.83	192.168.1.80	HTTP	516	POST /admin/get.php HTTP/1.1
14	27.856474	192.168.1.80	192.168.1.83	HTTP	519	HTTP/1.0 200 OK (text/html)
14	28.053803	192.168.1.83	192.168.1.80	HTTP	276	POST /news.php HTTP/1.1
15	28.065561	192.168.1.80	192.168.1.83	HTTP	11	HTTP/1.0 200 OK (text/html)
20	33.245337	192.168.1.83	192.168.1.80	HTTP	259	GET /login/process.php HTTP/1.1
20	33.253440	192.168.1.80	192.168.1.83	HTTP	60	HTTP/1.0 200 OK (text/html)
23	38.265103	192.168.1.83	192.168.1.80	HTTP	250	GET /news.php HTTP/1.1
23	38.271353	192.168.1.80	192.168.1.83	HTTP	60	HTTP/1.0 200 OK (text/html)
26	43.291043	192.168.1.83	192.168.1.80	HTTP	259	GET /login/process.php HTTP/1.1
26	43.298364	192.168.1.80	192.168.1.83	HTTP	60	HTTP/1.0 200 OK (text/html)
30	48.311212	192.168.1.83	192.168.1.80	HTTP	259	GET /login/process.php HTTP/1.1
30	48.322750	192.168.1.80	192.168.1.83	HTTP	340	HTTP/1.0 200 OK (text/html)
30	48.439913	192.168.1.83	192.168.1.80	HTTP	148	POST /admin/get.php HTTP/1.1
30	48.455743	192.168.1.80	192.168.1.83	HTTP	60	HTTP/1.0 404 NOT FOUND (text/html)
35	53.482265	192.168.1.83	192.168.1.80	HTTP	255	GET /admin/get.php HTTP/1.1
35	53.491062	192.168.1.80	192.168.1.83	HTTP	60	HTTP/1.0 200 OK (text/html)
40	58.515011	192.168.1.83	192.168.1.80	HTTP	259	GET /login/process.php HTTP/1.1
40	58.522942	192.168.1.80	192.168.1.83	HTTP	60	HTTP/1.0 200 OK (text/html)

A network administrator is investigating suspicious network activity by analyzing captured traffic. An engineer notices abnormal behavior and discovers that the default user agent is present in the headers of requests and data being transmitted What is occurring?

- A. indicators of denial-of-service attack due to the frequency of requests
- B. garbage flood attack attacker is sending garbage binary data to open ports
- C. indicators of data exfiltration HTTP requests must be plain text
- D. cache bypassing attack: attacker is sending requests for noncacheable content

Correct Answer: D

Section:

Explanation:

The presence of a default user agent in the headers of requests and data being transmitted suggests a cache bypassing attack. In this scenario, the attacker is likely requesting noncacheable content to avoid detection by caching mechanisms that could otherwise identify and block malicious traffic.

QUESTION 106

A company encountered a breach on its web servers using IIS 7.5. During the investigation, an engineer discovered that an attacker read and altered the data on a secure communication using TLS 1.2 and intercepted sensitive information by downgrading a connection to export-grade cryptography. The engineer must mitigate similar incidents in the future and ensure that clients and servers always negotiate with the most secure protocol versions and cryptographic parameters. Which action does the engineer recommend?

- A. Upgrade to TLS v1.3.
- B. Install the latest IIS version.
- C. Downgrade to TLS 1.1.
- D. Deploy an intrusion detection system

Correct Answer: A

Section:

Explanation:

Upgrading to TLS v1.3 is recommended because it eliminates outdated cryptographic functions and reduces the risk of downgrade attacks, which can occur when attackers force connections to use weaker encryption. TLS v1.3 only supports secure cipher suites and algorithms, enhancing the security of communications.

QUESTION 107

What is the difference between discretionary access control (DAC) and role-based access control (RBAC)?

- A. DAC requires explicit authorization for a given user on a given object, and RBAC requires specific conditions.
- B. RBAC access is granted when a user meets specific conditions, and in DAC, permissions are applied on user and group levels.
- C. RBAC is an extended version of DAC where you can add an extra level of authorization based on time.
- D. DAC administrators pass privileges to users and groups, and in RBAC, permissions are applied to specific groups

Correct Answer: B

Section:

Explanation:

In RBAC, access is based on the roles that users have within an organization, and permissions to perform certain operations are assigned to specific roles. DAC, on the other hand, is a type of access control where the access rights are determined by the owner of the resource or the resource itself.

QUESTION 108

Which technology prevents end-device to end-device IP traceability?

- A. encryption
- B. load balancing



- C. NAT/PAT
- D. tunneling

Correct Answer: C

Section:

Explanation:

NAT (Network Address Translation) and PAT (Port Address Translation) are technologies that modify the IP address information in packet headers as they pass through a router or firewall, making it difficult to trace the communication back to the originating end-device.

QUESTION 109

What are the two differences between stateful and deep packet inspection? (Choose two)

- A. Stateful inspection is capable of TCP state tracking, and deep packet filtering checks only TCP source and destination ports
- B. Deep packet inspection is capable of malware blocking, and stateful inspection is not
- C. Deep packet inspection operates on Layer 3 and 4. and stateful inspection operates on Layer 3 of the OSI model
- D. Deep packet inspection is capable of TCP state monitoring only, and stateful inspection can inspect TCP and UDP.
- E. Stateful inspection is capable of packet data inspections, and deep packet inspection is not

Correct Answer: A, B

Section:

Explanation:

A: Stateful inspection tracks the state of network connections, such as TCP streams, to determine if a packet is part of an established connection.

B: Deep packet inspection examines the data part (payload) of a packet and can identify, block, or reroute packets with specific types of malware. Stateful inspection does not inspect the payload for malware.

QUESTION 110

What is the purpose of command and control for network-aware malware?

- A. It contacts a remote server for commands and updates
- B. It takes over the user account for analysis
- C. It controls and shuts down services on the infected host.
- D. It helps the malware to profile the host

Correct Answer: A

Section:

Explanation:

The purpose of command and control (C&C) for network-aware malware is to allow an attacker to remotely control compromised systems. This includes sending commands to the malware, receiving data from the infected host, and updating the malware to evade detection or enhance its capabilities.

QUESTION 111

What do host-based firewalls protect workstations from?

- A. zero-day vulnerabilities
- B. unwanted traffic
- C. malicious web scripts
- D. viruses

Correct Answer: B



Section:

Explanation:

Host-based firewalls are designed to protect individual workstations from unwanted traffic by filtering incoming and outgoing network communications based on predefined security rules. They can block unauthorized access attempts and prevent potentially harmful traffic from reaching the system.

QUESTION 112

Refer to exhibit.

The exhibit displays a network traffic capture. The top portion is a table of captured packets:

No.	Time	Source	Destination	Protocol	Length	Info
62477	1012.633697	157.240.9.18	192.168.164.3	TLSv1.3	237	Application Data
62478	1012.633698	157.240.9.18	192.168.164.3	TLSv1.3	146	Application Data
62479	1012.633699	157.240.9.18	192.168.164.3	TLSv1.3	118	Application Data
62481	1012.634343	192.168.164.3	157.240.9.18	TLSv1.3	97	Application Data
62482	1012.693551	157.240.9.18	192.168.164.3	TLSv1.3	707	Application Data
62485	1016.598525	193.182.61.9	192.168.164.3	TLSv1.3	602	Application Data
62496	1018.263201	192.168.164.3	157.240.9.53	TLSv1.2	97	Application Data
62499	1018.570285	192.168.164.3	157.240.9.18	TLSv1.3	162	Application Data
62500	1018.571198	192.168.164.3	157.240.9.18	TLSv1.3	330	Application Data
62501	1018.571198	192.168.164.3	157.240.9.18	TLSv1.3	97	Application Data
62502	1018.574960	157.240.9.53	192.168.164.3	TLSv1.2	104	Application Data
62507	1018.662809	157.240.9.18	192.168.164.3	TLSv1.3	101	Application Data
62509	1019.251166	157.240.9.18	192.168.164.3	TCP	1446	443 → 64543 [ACK] Seq=4209 Ack=1692 Win=69888 Len=1388
62510	1019.251174	157.240.9.18	192.168.164.3	TLSv1.3	499	Application Data, Application Data

The bottom portion shows a detailed view of frame 62304:

- Frame 62304: 602 bytes on wire (4816 bits), 602 bytes captured (4816 bits) on interface en0, id 0
- Ethernet II, Src: f6:4e:bf:78:6d:15 (f6:4e:bf:78:6d:15), Dst: Apple_73:7b:a6 (88:e9:fe:73:7b:a6)
- Internet Protocol Version 4, Src: 193.182.61.9, Dst: 192.168.164.3
- Transmission Control Protocol, Src Port: 443, Dst Port: 64313, Seq: 42451286, Ack: 1415858, Len: 536
 - Source Port: 443
 - Destination Port: 64313
 - [Stream index: 9]
 - [Conversation completeness: Incomplete, DATA (15)]
 - [TCP Segment Len: 536]
 - Sequence Number: 42451286 (relative sequence number)
 - Sequence Number (raw): 293575394
 - [Next Sequence Number: 42451822 (relative sequence number)]

Below the packet details is a hex dump of the data, with a large 'Vdumps' watermark overlaid on the right side.

An analyst performs the analysis of the pcap file to detect the suspicious activity. What challenges did the analyst face in terms of data visibility?

- A. data encapsulation
- B. IP fragmentation
- C. code obfuscation
- D. data encryption

Correct Answer: D

Section:

Explanation:

When analyzing a pcap file, data encryption can pose a significant challenge in terms of visibility. Encrypted data cannot be easily inspected, which means that the analyst may not be able to view the contents of the network packets to detect suspicious activity.

QUESTION 113

Which two measures are used by the defense-in-depth strategy? (Choose two)

- A. Bridge the single connection into multiple.
- B. Divide the network into parts
- C. Split packets into pieces.
- D. Reduce the load on network devices.
- E. Implement the patch management process

Correct Answer: B, E

Section:

Explanation:

The defense-in-depth strategy is a layered approach to security that includes multiple defensive measures to protect against threats. Dividing the network into parts (B) helps isolate potential breaches, making it harder for an attacker to move laterally across the network. Implementing the patch management process (E) ensures that systems are up-to-date with the latest security patches, reducing vulnerabilities that attackers could exploit.

QUESTION 114

An engineer must compare NIST vs ISO frameworks The engineer decided to compare as readable documentation and also to watch a comparison video review. Using Windows 10 OS. the engineer started a browser and searched for a NIST document and then opened a new tab in the same browser and searched for an ISO document for comparison

The engineer tried to watch the video, but there 'was an audio problem with OS so the engineer had to troubleshoot it At first the engineer started CMD and looked for a driver path then looked for a corresponding registry in the registry editor The engineer enabled 'Audiosrv' in task manager and put it on auto start and the problem was solved Which two components of the OS did the engineer touch? (Choose two)

- A. permissions
- B. PowerShell logs
- C. service
- D. MBR
- E. process and thread

Correct Answer: C, E

Section:

Explanation:

The engineer engaged with the service component by enabling "Audiosrv," which is the Windows Audio Service responsible for managing audio for Windows-based programs. By setting it to auto-start, the engineer ensured that the service would run automatically upon system startup. Additionally, the engineer interacted with process and thread management by using the Task Manager to modify the behavior of the "Audiosrv" service.

QUESTION 115

During which phase of the forensic process are tools and techniques used to extract information from the collected data?

- A. investigation
- B. examination
- C. reporting
- D. collection

Correct Answer: B

Section:

Explanation:

During the examination phase of the forensic process, digital forensic investigators use various tools and techniques to extract and analyze information from the collected data. This phase involves detailed scrutiny of the data to uncover relevant evidence and is critical for the success of the forensic investigation.

QUESTION 116

Which attack method is being used when an attacker tries to compromise a network with an authentication system that uses only 4-digit numeric passwords and no username?

- A. SQL injection
- B. dictionary
- C. replay
- D. cross-site scripting

Correct Answer: B

Section:

Explanation:

A dictionary attack is a method used to break into a password-protected computer or server by systematically entering every word in a dictionary as a password. In the context of an authentication system that uses only 4-digit numeric passwords, a dictionary attack would involve trying all possible combinations of 4-digit numbers until the correct one is found.

QUESTION 117

Refer to the exhibit.

16	0.000188	76.196.12.250	192.168.0.1	TCP	54	12033	→ 80	[SYN]	Seq=0	Win=16384	Len=0
17	0.000189	164.124.33.94	192.168.0.1	TCP	54	35181	→ 80	[SYN]	Seq=0	Win=16384	Len=0
18	0.000191	164.124.33.160	192.168.0.1	TCP	54	35247	→ 80	[SYN]	Seq=0	Win=16384	Len=0
19	0.000193	38.198.26.94	192.168.0.1	TCP	54	14463	→ 80	[SYN]	Seq=0	Win=16384	Len=0
20	0.000195	132.212.36.219	192.168.0.1	TCP	54	31962	→ 80	[SYN]	Seq=0	Win=16384	Len=0
21	0.000466	164.124.33.172	192.168.0.1	TCP	54	35259	→ 80	[SYN]	Seq=0	Win=16384	Len=0
22	0.000468	164.124.33.90	192.168.0.1	TCP	54	35177	→ 80	[SYN]	Seq=0	Win=16384	Len=0
23	0.000470	132.212.36.218	192.168.0.1	TCP	54	31961	→ 80	[SYN]	Seq=0	Win=16384	Len=0
24	0.000471	164.124.33.70	192.168.0.1	TCP	54	35157	→ 80	[SYN]	Seq=0	Win=16384	Len=0
25	0.000473	76.196.12.237	192.168.0.1	TCP	54	12020	→ 80	[SYN]	Seq=0	Win=16384	Len=0
26	0.000475	164.124.33.73	192.168.0.1	TCP	54	35160	→ 80	[SYN]	Seq=0	Win=16384	Len=0
27	0.000476	189.109.37.206	192.168.0.1	TCP	54	36102	→ 80	[SYN]	Seq=0	Win=16384	Len=0
28	0.000478	164.124.33.71	192.168.0.1	TCP	54	35158	→ 80	[SYN]	Seq=0	Win=16384	Len=0

Which application-level protocol is being targeted?

- A. HTTPS
- B. FTP
- C. HTTP
- D. TCP

Correct Answer: C

Section:



QUESTION 118

Which statement describes patch management?

- A. scanning servers and workstations for missing patches and vulnerabilities
- B. managing and keeping previous patches lists documented for audit purposes
- C. process of appropriate distribution of system or software updates
- D. workflow of distributing mitigations of newly found vulnerabilities

Correct Answer: C

Section:

Explanation:

Patch management is the process of distributing and managing updates to software and systems. These updates can include patches for security vulnerabilities, bug fixes, and enhancements to improve performance or add new features. It ensures that systems are up-to-date, secure, and performing optimally. Reference:=Cisco Cybersecurity Training

QUESTION 119

Refer to the exhibit.


```
nmap 10.19.140.2

Starting Nmap 6.40 ( http://nmap.org ) at 2019-07-21 16:39 EDT
Nmap scan report for 10.19.140.2
Host is up (0.061s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
199/tcp   open  smux
443/tcp   open  https
8000/tcp  open  http-alt
8181/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 14.18 seconds
```

An attacker gained initial access to the company's network and ran an Nmap scan to advance with the lateral movement technique and to search the sensitive data. Which two elements can an attacker identify from the scan? (Choose two.)

- A. workload and the configuration details
- B. user accounts and SID
- C. number of users and requests that the server is handling
- D. functionality and purpose of the server
- E. running services

Correct Answer: D, E

Section:

Explanation:

An Nmap scan can provide detailed information about a network including the functionality and purpose of servers on that network as well as any services that are currently running on those servers. This information can be used by an attacker to identify potential vulnerabilities or targets for exploitation during a cyber attack. Reference: Cisco Cybersecurity Training

QUESTION 120

Why should an engineer use a full packet capture to investigate a security breach?

- A. It captures the TCP flags set within each packet for the engineer to focus on suspicious packets to identify malicious activity
- B. It collects metadata for the engineer to analyze, including IP traffic packet data that is sorted, parsed, and indexed.
- C. It provides the full TCP streams for the engineer to follow the metadata to identify the incoming threat.
- D. It reconstructs the event allowing the engineer to identify the root cause by seeing what took place during the breach

Correct Answer: D

Section:

Explanation:

Full packet capture (FPC) is a valuable tool for investigating security breaches because it provides comprehensive data that can be used to reconstruct the event and identify the root cause. By capturing every packet, FPC allows engineers to see exactly what took place during the breach, including the TCP flags set within each packet, which can help focus on suspicious packets to identify malicious activity. It also collects metadata, including IP traffic packet data that is sorted, parsed, and indexed, and provides the full TCP streams to follow the metadata to identify the incoming threat

QUESTION 121

Refer to the exhibit.



No.	Time	Source	Destination	Protocol	Length	Info
25	0.153298	10.0.0.2	10.128.0.2	HTTP	351	GET / HTTP/1.1
28	0.154677	10.0.0.2	10.128.0.2	HTTP	302	POST / HTTP/1.1
30	0.154919	10.128.0.2	10.0.0.2	HTTP	86	HTTP/1.1 200 OK (text/html)
33	0.155401	10.0.0.2	10.128.0.2	HTTP	329	POST / HTTP/1.1
36	0.156368	10.128.0.2	10.0.0.2	HTTP	71	HTTP/1.1 403 FORBIDDEN (text/html)
38	0.157187	10.128.0.2	10.0.0.2	HTTP	71	HTTP/1.1 403 FORBIDDEN (text/html)
40	0.167339	10.0.0.2	10.128.0.2	HTTP	351	POST / HTTP/1.1
43	0.168800	10.128.0.2	10.0.0.2	HTTP	71	HTTP/1.1 403 FORBIDDEN (text/html)
45	0.185975	10.0.0.2	10.128.0.2	HTTP	307	GET / HTTP/1.1
48	0.187666	10.128.0.2	10.0.0.2	HTTP	86	HTTP/1.1 200 OK (text/html)
52	0.212016	10.0.0.2	10.128.0.2	HTTP	331	GET / HTTP/1.1
55	0.213994	10.128.0.2	10.0.0.2	HTTP	86	HTTP/1.1 200 OK (text/html)
60	0.251596	10.0.0.2	10.128.0.2	HTTP	351	POST / HTTP/1.1
63	0.253226	10.128.0.2	10.0.0.2	HTTP	71	HTTP/1.1 403 FORBIDDEN (text/html)
89	0.322338	10.0.0.2	10.128.0.2	HTTP	366	POST / HTTP/1.1
92	0.323724	10.128.0.2	10.0.0.2	HTTP	71	HTTP/1.1 403 FORBIDDEN (text/html)
100	0.369008	10.0.0.2	10.128.0.2	HTTP	307	GET / HTTP/1.1
103	0.370831	10.128.0.2	10.0.0.2	HTTP	86	HTTP/1.1 200 OK (text/html)
116	0.409372	10.0.0.2	10.128.0.2	HTTP	278	GET / HTTP/1.1
120	0.411609	10.128.0.2	10.0.0.2	HTTP	86	HTTP/1.1 200 OK (text/html)
122	0.413962	10.0.0.2	10.128.0.2	HTTP	371	POST / HTTP/1.1
125	0.415392	10.128.0.2	10.0.0.2	HTTP	71	HTTP/1.1 403 FORBIDDEN (text/html)
136	0.450272	10.0.0.2	10.128.0.2	HTTP	346	GET / HTTP/1.1
139	0.452288	10.128.0.2	10.0.0.2	HTTP	86	HTTP/1.1 200 OK (text/html)
140	0.452400	10.0.0.2	10.128.0.2	HTTP	351	POST / HTTP/1.1

Frame 25: 351 bytes on wire (2808 bits), 351 bytes captured (2808 bits)
 Encapsulation type: Ethernet (1)
 Arrival Time: Jul 26, 2018 06:34:55.417126000 UTC
 [Time shift for this packet: 0.000000000 seconds]
 Epoch Time: 1532586895.417126000 seconds
 [Time delta from previous captured frame: 0.000165000 seconds]

An engineer received a ticket about a slowdown of a web application, Drug analysis of traffic, the engineer suspects a possible attack on a web server. How should the engineer interpret the Wiresharat traffic capture?

- A. 10.0.0.2 sends GET/ HTTP/1.1 And Post request and the target responds with HTTP/1.1. 200 OC and HTTP/1.1 403 accordingly. This is an HTTP flood attempt.
- B. 10.0.0.2 sends HTTP FORBIDDEN /1.1 And Post request, while the target responds with HTTP/1.1 200 Get and HTTP/1.1 403. This is an HTTP GET flood attack.
- C. 10.128.0.2 sends POST/1.1 And POST requests, and the target responds with HTTP/1.1 200 Ok and HTTP/1.1 403 accordingly. This is an HTTP Reserve Bandwidth flood.
- D. 10.128.0.2 sends HTTP/FORBIDDEN/ 1.1 and Get requests, and the target responds with HTTP/1.1 200 OK and HTTP/1.1 403. This is an HTTP cache bypass attack.

Correct Answer: B

Section:

Explanation:

When analyzing Wireshark traffic for potential attacks, an engineer should look for patterns that indicate abnormal behavior, such as:

Excessive Requests: A high number of requests over a short period could suggest an attempt to overwhelm the server, known as an HTTP flood.

Status Codes: Repeated 403 Forbidden responses may indicate that the server is rejecting requests due to a security rule being triggered.

Request Types: A mix of GET and POST requests could be used in various attack scenarios, including bandwidth flooding or cache bypassing.

QUESTION 124

Refer to the exhibit.

```
C:\>nmap -p U:53,67-68,T:21-25,80,135 192.168.233.128
Starting Nmap 7.70 ( https://nmap.org ) at 2018-07-21 13:11 GMT Summer Time
Nmap scan report for 192.168.233.128
Host is up (0.0011s latency).

```

PORT	STATE	SERVICE
21/tcp	filtered	ftp
22/tcp	filtered	ssh
23/tcp	filtered	telnet
24/tcp	filtered	priv-mail
25/tcp	filtered	smtp
80/tcp	filtered	http

```
MAC Address: 08:0C:29:A2:6A:81 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 22.87 seconds
```

An attacker scanned the server using Nmap.
What did the attacker obtain from this scan?

- A. Identified a firewall device preventing the port state from being returned
- B. Identified open SMB ports on the server
- C. Gathered information on processes running on the server
- D. Gathered a list of Active Directory users.

Correct Answer: A

Section:



QUESTION 125

Which classification of cross-site scripting attack executes the payload without storing it for repeated use?

- A. stored
- B. reflective
- C. DOM
- D. CSRF

Correct Answer: B

Section:

Explanation:

Reflective XSS, also known as Non-Persistent XSS, occurs when an attacker sends a malicious script to a user through a web application, and the script is executed immediately in the user's browser without being stored on the server. This type of attack is typically carried out by including the malicious script in a URL, which is then sent to the victim. When the victim clicks on the link, the script runs in their browser, reflecting the attacker's actions without storing the payload for repeated use. Reference: OWASP Foundation's documentation on Cross-Site Scripting (XSS) provides detailed information on the different types of XSS attacks, including Reflective XSS

QUESTION 126

An engineer received an alert affecting the degraded performance of a critical server Analysis showed a heavy CPU and memory load What is the next step the engineer should take to investigate this resource usage?

- A. Run 'ps -ef' to understand which processes are taking a high amount of resources
- B. Run 'ps -u' to find out who executed additional processes that caused a high load on a server
- C. Run 'ps -m' to capture the existing state of daemons and map the required processes to find the gap
- D. Run 'ps -d' to decrease the priority state of high-load processes to avoid resource exhaustion

Correct Answer: A

Section:

Explanation:

When a server is experiencing high CPU and memory load, the first step is to identify the processes that are consuming the most resources. The command "ps -ef" is used to display information about all the running processes, including their IDs, memory and CPU usage, and the commands that started them. This allows the engineer to pinpoint which processes are responsible for the high load and take appropriate action, such as terminating unnecessary processes or optimizing resource usage³⁴⁵. Reference:: Various resources on server management and troubleshooting recommend using the "ps -ef" command as a starting point for investigating high resource usage on servers

QUESTION 127

Which type of data must an engineer capture to analyze payload and header information?

- A. frame check sequence
- B. alert data
- C. full packet
- D. session logs

Correct Answer: C

Section:

Explanation:

To analyze both payload and header information, an engineer must capture the full packet data. This includes all protocol and payload information for the traffic, allowing for a comprehensive analysis of the data being transmitted⁵⁶⁷⁸. Reference:: Full packet capture is a common practice in network monitoring and security, as it provides detailed insights into the data transmitted over the network, including both payload and header information

QUESTION 128

What are two differences between tampered disk images and untampered disk images? (Choose two.)

- A. Tampered Images are used in a security investigation process
- B. Untampered images can be used as law enforcement evidence.
- C. The image is untampered if the existing stored hash matches the computed one
- D. The image is tampered if the stored hash and the computed hash are identical
- E. Tampered images are used as an element for the root cause analysis report

Correct Answer: C, E

Section:

Explanation:

An untampered disk image is one that has not been altered since its creation. This is verified by comparing the stored hash of the image at the time of creation with a newly computed hash; if they match, the image is considered untampered. Tampered images, on the other hand, may be used during the root cause analysis process to understand how and what was altered¹². Reference:: The differences between tampered and untampered disk images are discussed in cybersecurity literature, including Cisco's certification guides, which explain the importance of hash matching for verifying the integrity of disk images

QUESTION 129

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

Correct Answer:

	Threat
	Vulnerability
	Risk Assessment
	Exploit

Section:

Explanation:

QUESTION 130

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
web content filtering	full packet capture
traditional stateful firewall	transaction data
NetFlow	connection event

Correct Answer:

	web content filtering
	tcpdump
	NetFlow
	traditional stateful firewall

Section:

Explanation:

QUESTION 131

DRAG DROP



No.	Time	Source	Destination	Protocol	Length	Info
17	0.011641	10.0.2.15	192.124.249.9	TCP	76	50586-443 [SYN] Seq=0 Win=
18	0.011918	10.0.2.15	192.124.249.9	TCP	76	50588-443 [SYN] Seq=0 Win=
19	0.022656	192.124.249.9	10.0.2.15	TCP	62	443-50588 [SYN, ACK] Seq=0
20	0.022702	10.0.2.15	192.124.249.9	TCP	56	50588-443 [ACK] Seq=1 Ack=
21	0.022988	192.124.249.9	10.0.2.15	TCP	62	443-50586 [SYN, ACK] Seq=0
22	0.022996	10.0.2.15	192.124.249.9	TCP	56	50586-443 [ACK] Seq=1 Ack=
23	0.023212	10.0.2.15	192.124.249.9	TLSv1.2	261	Client Hello
24	0.023373	10.0.2.15	192.124.249.9	TLSv1.2	261	Client Hello
25	0.023445	192.124.249.9	10.0.2.15	TCP	62	443-50588 [ACK] Seq=1 Ack=
26	0.023617	192.124.249.9	10.0.2.15	TCP	62	443-50586 [ACK] Seq=1 Ack=
27	0.037413	192.124.249.9	10.0.2.15	TLSv1.2	2792	Server Hello
28	0.037426	10.0.2.15	192.124.249.9	TCP	56	50586-443 [ACK] Seq=206 Ac

<

> Frame 23: 261 bytes on wire (2088 bits), 261 bytes captured (2088 bits)
 > Linux cooked capture
 > Internet Protocol Version 4, Src: 10.0.2.15 (10.0.2.15), Dst: 192.124.249.9 (192.124.249.9)
 > Transmission Control Protocol, Src Port: 50588 (50588), Dst Port: 443 (443), Seq: 1, Ack:1,
 > Secure Sockets Layer

```

0000  00 04 00 01 00 06 08 00 27 7a 3c 93 00 00 08 00  ..... *z<.....
0010  45 00 00 f5 eb 3e 40 00 40 06 89 2f 0a 00 02 0f  E.....>@. @../....
0020  c0 7c f9 09 c5 9c 01 bb 4d db 7f f7 00 b3 b0 02  .|..... M.....
0030  50 18 72 10 c6 7c 00 00 16 03 01 00 c8 01 00 00  P.r..|.. .....
0040  c4 03 03 d1 08 45 78 b7 2c 90 04 ee 51 16 f1 82  .....Ex. ....0...
0050  16 43 ec d4 89 60 34 4a 7b 80 a6 d1 72 d5 11 87  .C....4J {...r...
0060  10 57 cc 00 00 1e c0 2b c0 2f cc a9 cc a8 c0 2c  .W.....+.../.....
0070  c0 30 c0 0a c0 09 c0 13 c0 14 00 33 00 39 00 2f  .0.....3.9./
0080  00 35 00 0a 01 00 00 7d 00 00 00 16 00 14 00 00  .5.....} .....
0090  11 77 77 77 2e 6c 69 6e 75 78 6d 69 6e 74 2e 63  .wwwlin uxmint.c
00a0  6f 6d 00 17 00 00 ff 01 00 01 00 00 0a 00 08 00  om.....
00b0  06 00 17 00 18 00 19 00 0b 00 02 01 00 00 23 00  .....
00c0  00 33 74 00 00 00 10 00 17 00 15 02 68 32 08 73  .3t..... .h2.s
00d0  70 64 79 2f 33 2e 31 08 68 74 74 70 2f 31 2e 31  pdy/3.2. http/1.1
00e0  00 05 00 05 01 00 00 00 00 00 0d 00 18 00 16 04  .....
00f0  01 05 01 06 01 02 01 04 03 05 03 06 03 02 03 05  .....
0100  02 04 02 02 02  .....
  
```

Refer to the exhibit. Drag and drop the element name from the left onto the correct piece of the PCAP file on the right.

Select and Place:

source address	10.0.2.15
destination address	50588
source port	443
destination port	192.124.249.9
Network Protocol	Transmission Control Protocol
Transport Protocol	Internet Protocol v4
Application Protocol	Transport Layer Security v1.2

Correct Answer:

	source address
	source port
	destination port
	destination address
	Transport Protocol
	Network Protocol
	Application Protocol

Section:

Explanation:

QUESTION 132

DRAG DROP

Drag and drop the access control models from the left onto the correct descriptions on the right.

Select and Place:

MAC	object owner determines permissions
ABAC	OS determines permissions
RBAC	role of the subject determines permissions
DAC	attributes of the subject determines permissions

Correct Answer:

	DAC
	MAC
	RBAC
	ABAC

Section:

Explanation:



QUESTION 133

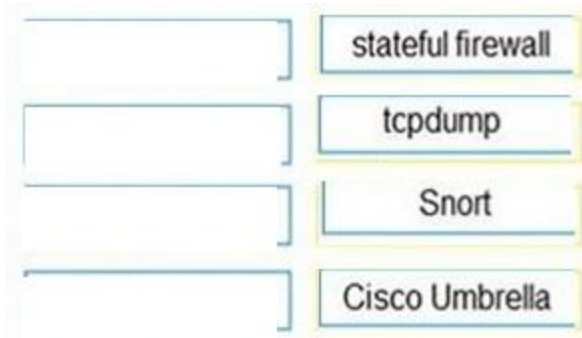
DRAG DROP

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

Correct Answer:



Section:

Explanation:

QUESTION 134

Refer to the exhibit.

```
10.20.1.21 -- [05/Mar/2018:20:04:30 +0000] "GET /user?name=%3B/bin/sh%20-c%20id HTTP/1.1" 200 178 "-" "Wget/1.17.1 (linux-gnu)"
```

Which attack is being attempted against a web application?

- A. SQL injection
- B. man-in-the-middle
- C. command injection
- D. denial of service

Correct Answer: C

Section:

Explanation:

The exhibit shows an HTTP GET request with a parameter that includes ; /bin/sh -c id.

This indicates a command injection attempt, where the attacker is trying to execute shell commands on the server.

Command injection vulnerabilities allow an attacker to execute arbitrary commands on the host operating system via a vulnerable application.

The use of /bin/sh and the -c flag is typical in command injection exploits to run shell commands, such as id, which returns user identity information.

OWASP Command Injection

Analyzing HTTP Requests for Injection Attacks

Web Application Security Testing Guidelines

QUESTION 135

A security engineer must investigate a recent breach within the organization. An engineer noticed that a breached workstation is trying to connect to the domain 'Ranso4730-mware92-647'. which is known as malicious. In which step of the Cyber Kill Chain is this event?

- A. Vaporization
- B. Delivery
- C. reconnaissance
- D. Action on objectives

Correct Answer: D

Section:



Explanation:

The event where a breached workstation is trying to connect to a known malicious domain suggests that the attacker is moving towards their end goals, which typically involves actions on objectives. In the Cyber Kill Chain framework, 'Action on objectives' refers to the steps taken by an attacker to achieve their intended outcomes, such as data exfiltration, destruction, or ransom demands. This phase involves the attacker executing their final mission within the target environment, leveraging access gained in earlier stages of the attack.

Lockheed Martin Cyber Kill Chain

Understanding the Stages of Cyber Attacks

Incident Response and the Cyber Kill Chain

QUESTION 136

What is data encapsulation?

- A. Browsing history is erased automatically with every session.
- B. The protocol of the sending host adds additional data to the packet header.
- C. Data is encrypted backwards, which makes it unusable.
- D. Multiple hosts can be supported with only a few public IP addresses.

Correct Answer: B

Section:

Explanation:

Data encapsulation is a process in networking where the protocol stack of the sending host adds headers (and sometimes trailers) to the data.

Each layer of the OSI or TCP/IP model adds its own header to the data as it passes down the layers, preparing it for transmission over the network.

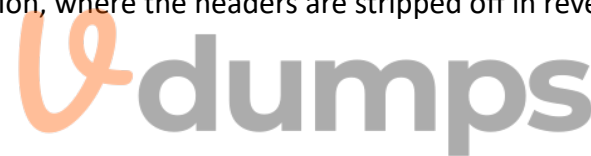
For example, in the TCP/IP model, data starts at the application layer and is encapsulated at each subsequent layer (Transport, Internet, and Network Access) before being transmitted.

This encapsulation ensures that the data is correctly formatted and routed to its destination, where the headers are stripped off in reverse order by the receiving host.

Networking Fundamentals by Cisco

OSI Model and Data Encapsulation Process

Understanding TCP/IP Encapsulation

**QUESTION 137**

Which type of attack uses a botnet to reflect requests off of an NTP server to overwhelm a target?

- A. Display
- B. Man-in-the-middle
- C. Distributed denial of service
- D. Denial of service

Correct Answer: C

Section:

Explanation:

A Distributed Denial of Service (DDoS) attack involves multiple compromised devices (botnet) sending a large number of requests to a target server to overwhelm it.

In a specific type of DDoS attack known as an NTP amplification attack, the attacker exploits the Network Time Protocol (NTP) servers by sending small queries with a spoofed source IP address (the target's IP).

The NTP server responds with a much larger reply to the target's IP address, thereby amplifying the traffic directed at the target.

This reflection and amplification technique significantly increases the volume of traffic sent to the target, causing denial of service.

OWASP DDoS Attack Overview

NTP Amplification Attack Explained

Understanding Botnets and Distributed Attacks

QUESTION 138

Which of these is a defense-in-depth strategy principle?

- A. identify the minimum resource required per employee.
- B. Assign the least network privileges to segment network permissions.
- C. Provide the minimum permissions needed to perform Job functions.
- D. Disable administrative accounts to avoid unauthorized changes.

Correct Answer: C

Section:

Explanation:

Defense-in-depth is a layered security strategy that aims to protect information and resources through multiple security measures.

One of its key principles is the concept of least privilege, which means providing users and systems with the minimum level of access necessary to perform their job functions.

By assigning only the necessary permissions, the attack surface is reduced, and the potential damage from a compromised account or system is minimized.

This principle helps in mitigating the risk of unauthorized access and limits the capabilities of an attacker if they gain access to an account.

Defense-in-Depth Strategy by NIST

Principle of Least Privilege in Cybersecurity

Layered Security Approach Explained

QUESTION 139

How low does rule-based detection differ from behavioral detection?

- A. Behavioral systems find sequences that match particular attack behaviors, and rule-based systems identify potential zero-day attacks.
- B. Rule-based systems search for patterns linked to specific types of attacks, and behavioral systems identify attacks per signature.
- C. Behavioral systems have patterns for complex environments, and rule-based systems can be used on low-mid-sized businesses.
- D. Rule-based systems have predefined patterns, and behavioral systems learn the patterns that are specific to the environment.

Correct Answer: D

Section:

Explanation:

Rule-based detection systems operate using predefined patterns and signatures to identify known threats. These patterns are based on prior knowledge of attack methods and vulnerabilities.

Behavioral detection systems, on the other hand, analyze the normal behavior of a network or system to establish a baseline. They then monitor for deviations from this baseline, which may indicate potential threats.

Rule-based systems are effective at detecting known threats but may struggle with novel or zero-day attacks that do not match existing signatures.

Behavioral systems can detect unknown threats by recognizing abnormal activities, making them useful in identifying zero-day exploits and other sophisticated attacks.

Comparison of Rule-based and Behavioral Detection Methods in IDS

Advantages of Behavioral Analysis in Network Security

Cybersecurity Detection Techniques

