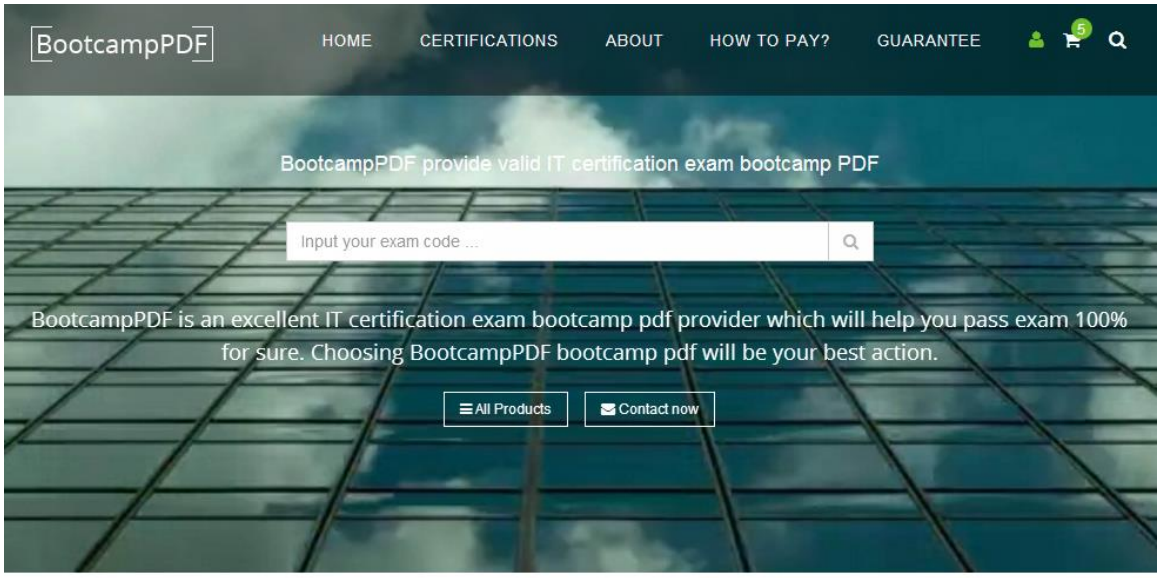
BootcampPDF



Quality and Value

BootcampPDF Practice Exams are written to the highest standards of technical accuracy, using only certified subject matter experts and published authors for development - no all vce.

Tested and Approved

We are committed to the process of vendor and third party approvals. We believe professionals and executives alike deserve the confidence of quality coverage these authorizations provide.

Easy to Pass

If you prepare for the exams using our BootcampPDF testing engine, It is easy to succeed for all certifications in the first attempt. You don't have to deal with all dumps or any free torrent / rapidshare all stuff.

Try Before Buy

BootcampPDF offers free demo of each product. You can check out the interface, question quality and usability of our practice exams before you decide to buy.

http://www.bootcamppdf.com

BootcampPDF provide valid IT certification exam bootcamp PDF

Exam : **200-201**

Title : Understanding Cisco Cybersecurity Operations Fundamentals

Vendor : Cisco

Version : DEMO

NO.1 Which process represents the application-level allow list?
A. allowing everything and denying specific applications protocols
B. allowing everything and denying specific executable files
C. allowing specific format files and deny executable files
D. allowing specific files and deny everything else
Answer: D
Explanation:
Application-level allow list refers to the practice of specifying an index of approved applications that are permitted to be executed in a system environment or network, which means only specific files are allowed while everything else is denied by default, enhancing security.

NO.2 An employee of a company receives an email with an attachment. They notice that this email is from a suspicious source, and they decide not to open the attached file. After further investigation, a security analyst concludes that this file is malware. To which category of the Cyber Kill Chain model does this event belong?
A. Weaponization
B. Installation
C. Exploitation
D. Delivery
Answer: D

NO.3 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
Answer: C
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/shand the-cflag is typical in command injection exploits to run shell commands, such asid, which returns user identity information.
References
OWASP Command Injection

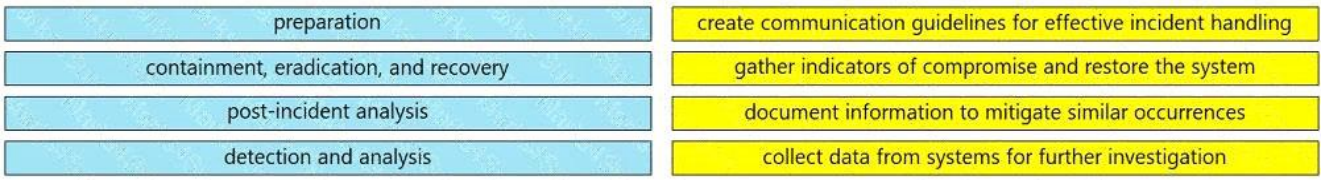
Analyzing HTTP Requests for Injection Attacks
Web Application Security Testing Guidelines

NO.4 How is symmetric encryption used for HTTPS connections?
A. The symmetric encryption algorithm uses public-private certificates
B. Encryption is based on RSA-2048
C. The symmetric key is used for encryption
D. The key exchange process is reliable and secure
Answer: C

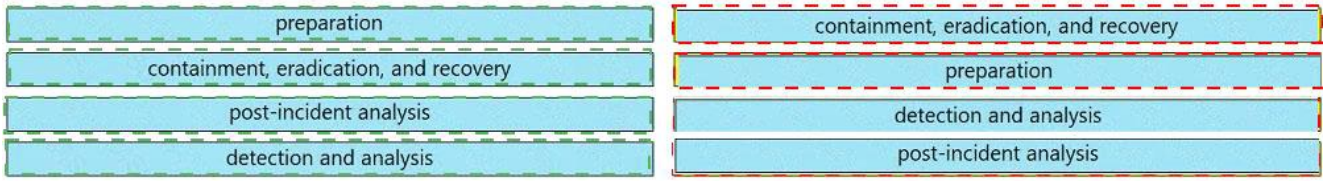
NO.5 What is the difference between inline traffic interrogation (TAPS) and traffic mirroring (SPAN)?
A. TAPS interrogation is more complex because traffic mirroring applies additional tags to data and SPAN does not alter integrity and provides full duplex network.
B. SPAN results in more efficient traffic analysis, and TAPS is considerably slower due to latency caused by mirroring.
C. TAPS replicates the traffic to preserve integrity, and SPAN modifies packets before sending them to other analysis tools
D. SPAN ports filter out physical layer errors, making some types of analyses more difficult, and TAPS receives all packets, including physical errors.
Answer: D
Explanation:
The main difference between inline traffic interrogation (TAPS) and traffic mirroring (SPAN) lies in how they handle network traffic for analysis purposes. TAPS, or Test Access Points, are hardware devices that create a copy of the traffic between two network points without altering the data. This means TAPS can transmit both send and receive data streams simultaneously on separate dedicated channels, ensuring all data, including physical layer errors, is received by the monitoring or security device in real-time. On the other hand, SPAN, or Switch Port Analyzer, is a feature that duplicates network packets seen on one port to another port for analysis. However, SPAN ports can filter out physical layer errors, which may limit the types of analyses that can be performed as some errors will not be represented in the mirrored traffic.
The distinction between TAPS and SPAN is covered in the Cisco CyberOps Associate CBROPS 200-201 course, which provides foundational knowledge for network monitoring and security analysis1. Additionally, industry resources such as Garland Technology's comparison of TAPS and SPAN highlight the differences in performance and integrity of the traffic being analyzed

NO.6 What is the functionality of an IDS'?
A. device or software that detects and blocks suspicious files
B. endpoint protection software that prevents viruses and malware
C. forensic tool used to perform an in-depth analysis and debugging
D. software or device which monitors and identifies malicious network activity
Answer: D

NO.7 Drag and drop the elements from the left into the correct order for incident handling on the right.

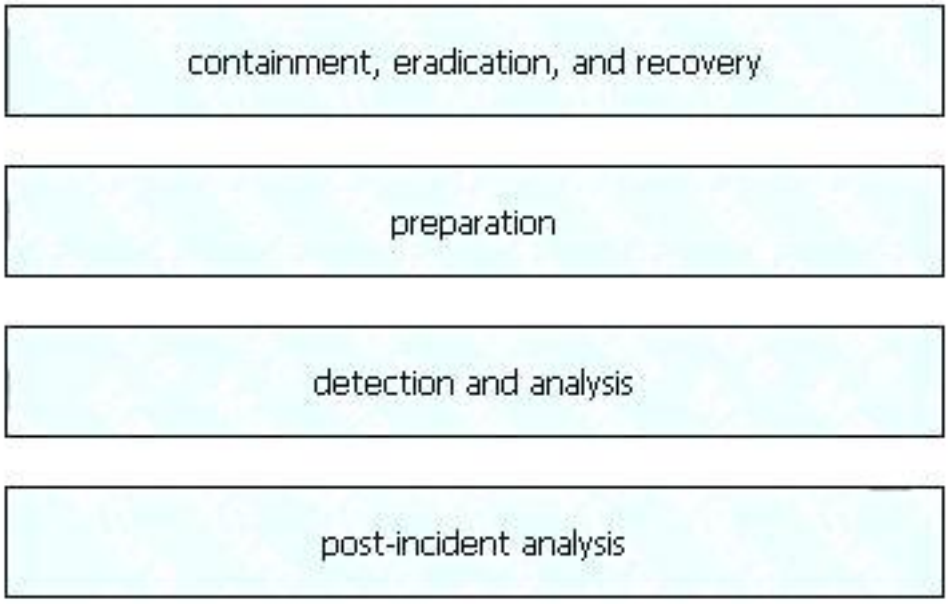


Answer:



Explanation:

A close-up of several blue rectangular boxes Description automatically generated



NO.8 Which metric in CVSS indicates an attack that takes a destination bank account number and replaces it with a different bank account number?

A. integrity

B. confidentiality

C. availability

D. scope

Answer: A

Explanation:

Integrity is a metric in CVSS that measures the impact of a vulnerability on the trustworthiness and veracity of the data or information in a system. A vulnerability that affects the integrity of a system can allow an attacker to modify, delete, or corrupt the data or information without authorization. An example of such a vulnerability is a bank account number tampering attack, where an attacker changes the destination bank account number of a transaction to redirect the funds to their own account. References: Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) - Cisco, page 2-17; 200-201 CBROPS - Cisco, exam topic 1.3.c

NO.9 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

Answer: D

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

NO.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

Answer: C

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. References: Separation of Duty (SOD) - Glossary | CSRC - NIST Computer Security ... , Separation of Duties | Imperva

NO.11 An engineer must configure network systems to detect command-and-control communications by decrypting ingress and egress perimeter traffic and allowing network security devices to detect malicious outbound communications. Which technology must be used to accomplish this task?

A. static IP addresses

B. signatures

C. digital certificates

D. cipher suite

Answer: C

Explanation:

Digital certificates are essential for decrypting ingress and egress perimeter traffic, as they provide

the necessary encryption keys for secure communications. By using digital certificates, network security devices can inspect the decrypted traffic to detect any malicious outbound communications that may indicate command-and-control activity.

NO.12 What is a benefit of agent-based protection when compared to agentless protection?
A. It lowers maintenance costs
B. It provides a centralized platform
C. It collects and detects all traffic locally
D. It manages numerous devices simultaneously
Answer: C
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. References:
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)

NO.13 What are two categories of DDoS attacks? (Choose two.)
A. split brain
B. phishing
C. direct
D. reflected
E. scanning
Answer: C D

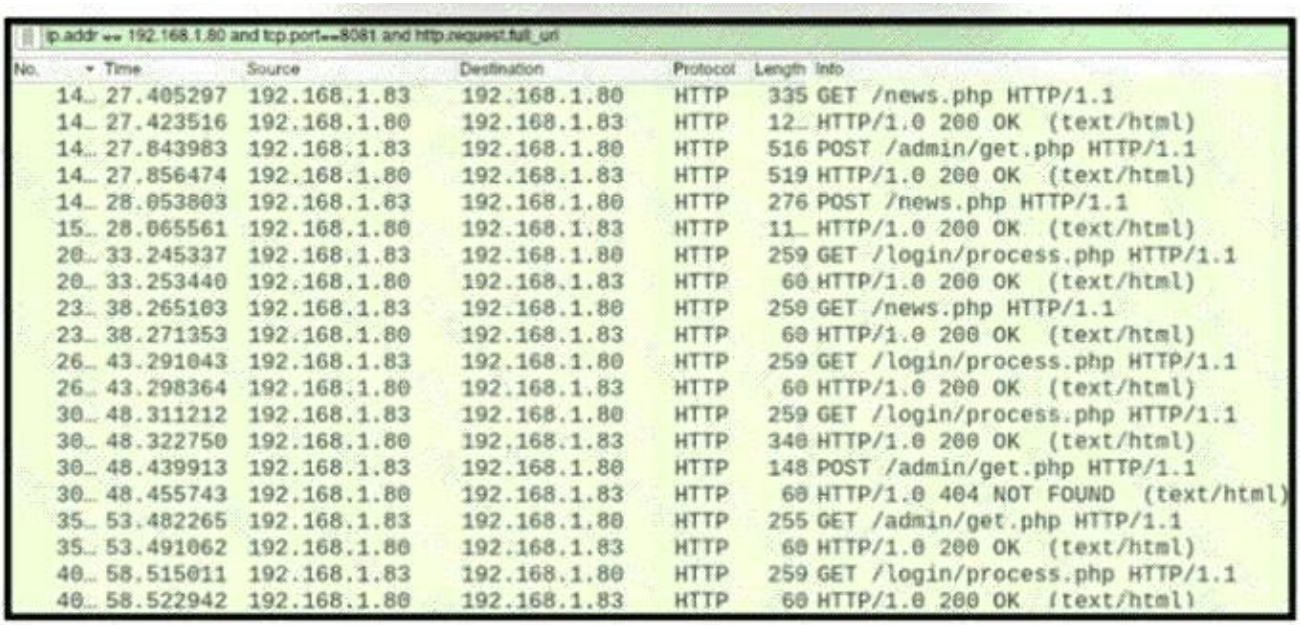
NO.14 Refer to the exhibit.

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
Answer: C
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. References := Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) v1.0, Module 1: Security Concepts, Lesson 1.4: Security Monitoring, Topic 1.4.1: Security Operations Center

NO.15 Refer to the exhibit.


ip.addr == 192.168.1.80 and tcp.port==8081 and http.request.full_uri

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
Answer: D
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.

NO.16 Which tool is used by threat actors on a webpage to take advantage of the software

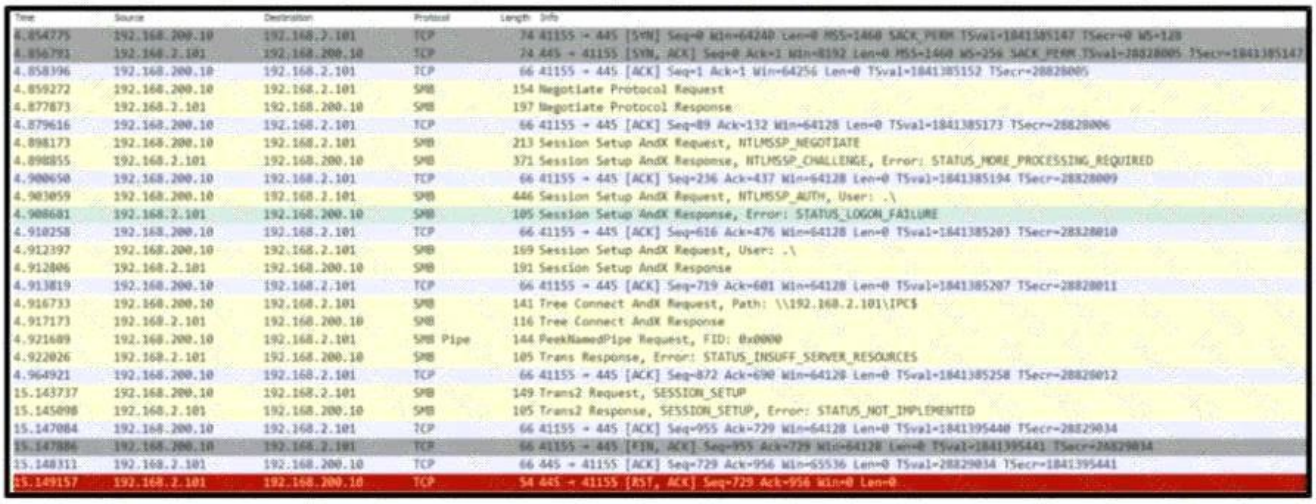
vulnerabilities of a system to spread malware?
A. script kiddie kit
B. exploit kit
C. vulnerability kit
D. root kit
Answer: B

NO.17 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
Answer: B
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.
Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) course materials discuss various attack methods, including dictionary attacks, and how they can be used to compromise networks

NO.18 Which step in the incident response process researches an attacking host through logs in a SIEM?
A. detection and analysis
B. preparation
C. eradication
D. containment
Answer: A
Explanation:
In the incident response process, detection and analysis involve researching an attacking host through logs in a Security Information and Event Management (SIEM) system. This step helps in identifying, validating, and managing potential security incidents. References := Cisco CyberOps Associate - Module 3: Security Monitoring

NO.19 What is session data used for in network security?
A. It is the transaction log between monitoring software.
B. It contains the set of parameters used for fetching logs.
C. It is the summary of the transmission between two network devices.
D. It tracks cookies within each session initiated from a user.
Answer: C

NO.20



Refer to the exhibit. Based on the .pcap file, which protocol's vulnerability has been exploited to establish a session?

A. SMB

B. TCP

C. Negotiate

D. IP

Answer: A

NO.21 What is corroborating evidence?

A. Evidence that can be provided to cyber police for further restrictive actions over threat actors

B. Evidence that can be presented in court in the original form, such as an exact copy of a hard drive

C. Evidence that tends to support a theory or an assumption deduced by some initial evidence

D. Evidence that relies on an extrapolation to a conclusion of fact, such as fingerprints

Answer: C

NO.22 What is the difference between a threat and a risk?

A. Threat represents a potential danger that could take advantage of a weakness in a system

B. Risk represents the known and identified loss or danger in the system

C. Risk represents the nonintentional interaction with uncertainty in the system

D. Threat represents a state of being exposed to an attack or a compromise, either physically or logically.

Answer: A

Explanation:

A threat represents a potential danger that could exploit a weakness in a system while risk is associated with the potential impact or loss that could occur if a threat exploits a vulnerability in the system. So, option A which states "Threat represents a potential danger that could take advantage of a weakness in a system" is correct. References := Cisco Certified CyberOps Associate Overview

NO.23 Which option describes indicators of attack?

A. spam emails on an employee workstation

B. virus detection by the AV software

C. blocked phishing attempt on a company

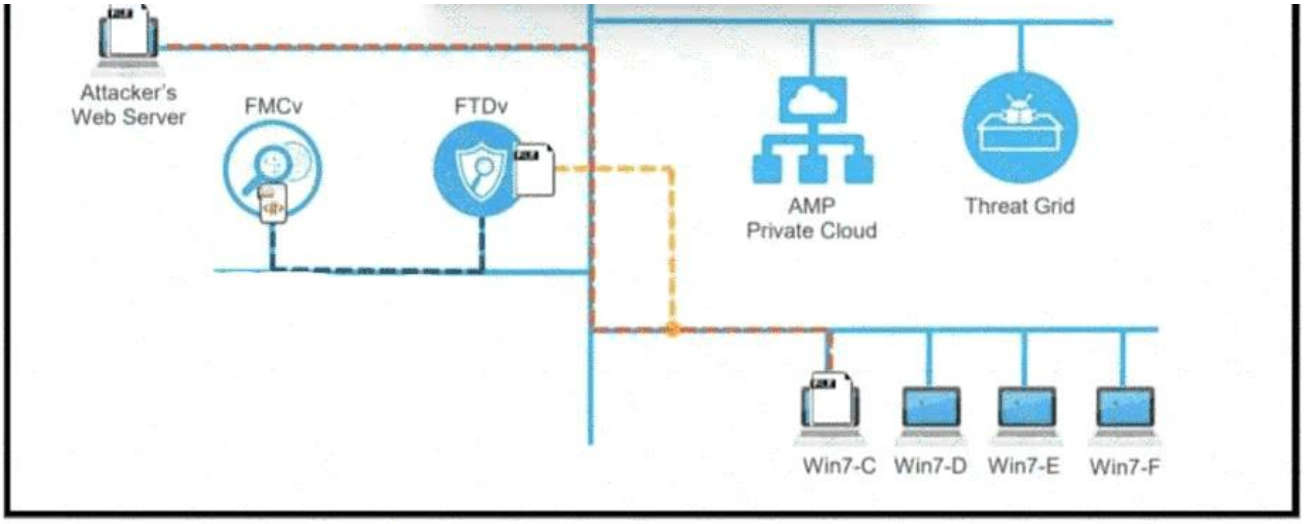
D. malware reinfection within a few minutes of removal

Answer: D

Explanation:

Indicators of attack (IoAs) are signs that an attack may be in progress or imminent. Malware reinfection within a few minutes of removal (D) is a strong IoA because it suggests that the attacker has a persistent mechanism to redeploy malware, indicating an active compromise of the system. Cisco's Cybersecurity Operations Fundamentals documents

NO.24 Refer to the exhibit.



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

Answer: D

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. References := Cisco Cybersecurity Operations Fundamentals

NO.25 What is a scareware attack?

A. using the spoofed email addresses to trick people into providing login credentials

B. overwhelming a targeted website with fake traffic

C. gaming access to your computer and encrypting data stored on it

D. inserting malicious code that causes popup windows with flashing colors

Answer: D

Explanation:

Scareware is a type of malware attack that tricks users into believing their computer is infected with a virus, prompting them to download and pay for fake antivirus software. The attack often uses popup

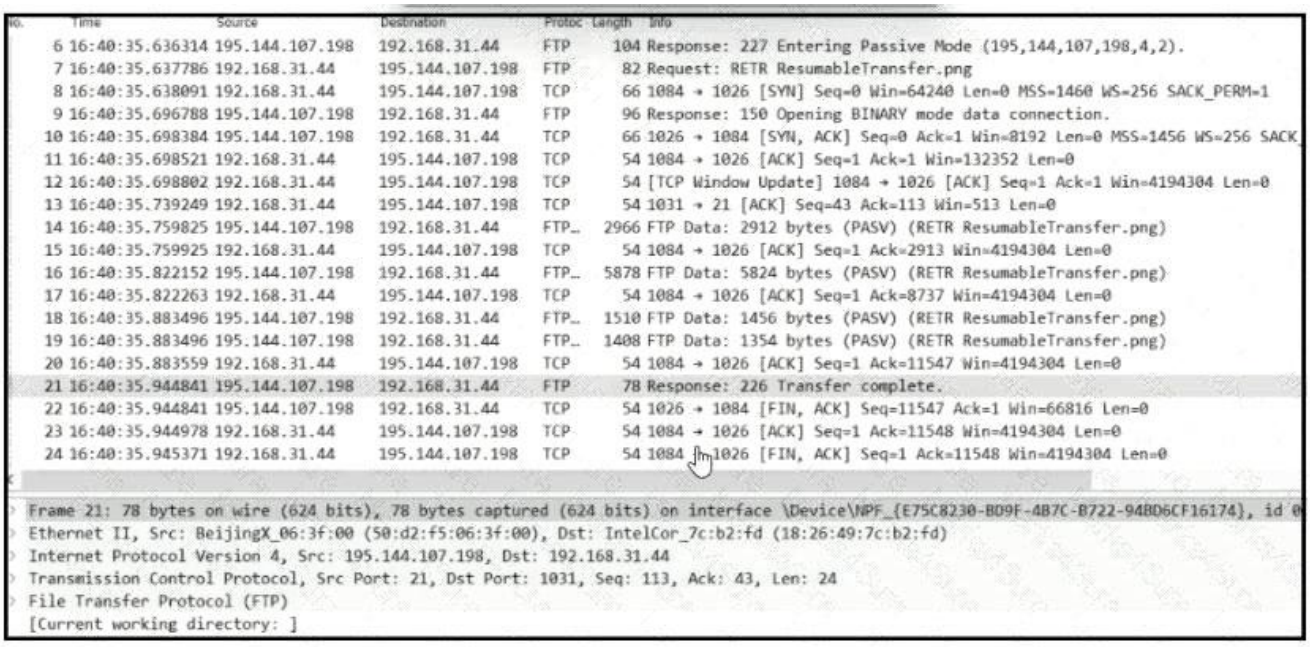
windows with flashing colors (D) to create a sense of urgency and scare the user into taking immediate action.
Cisco Certified CyberOps Associate certification materials

NO.26 Which technique is a low-bandwidth attack?
A. social engineering
B. session hijacking
C. evasion
D. phishing
Answer: D
Explanation:
Phishing is considered a low-bandwidth attack because it does not require the use of significant network resources. Instead, it relies on social engineering to deceive individuals into providing sensitive information or clicking on malicious links, often through email or other communication methods1.

NO.27 What is rule-based detection when compared to statistical detection?
A. proof of a user's identity
B. proof of a user's action
C. likelihood of user's action
D. falsification of a user's identity
Answer: B
Explanation:
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. References:
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)

NO.28 What is a difference between authorization and authentication from an access control perspective?
A. Authorization defines the author of a specific resource and authentication gives access to the resource itself
B. Authentication is when the system validates if the user is valid, and authorization enforces and provides resources assigned and required.
C. Authentication is responsible for accounting access on system resources and the authorization process defines if a user is allowed to author the resource
D. Authorization tracks if a certain user is authenticated within the system, and authentication is responsible for identifying the authorization method
Answer: B

NO.29 Refer to the exhibit.



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

Answer: A

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. Thisheader 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. References := 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

NO.30 What is the function of a command and control server?

A. It enumerates open ports on a network device

B. It drops secondary payload into malware

C. It is used to regain control of the network after a compromise

D. It sends instruction to a compromised system

Answer: D

Explanation:

A command and control server (C2 or C&C) is a server that is used by attackers to communicate with and control compromised systems, such as bots, zombies, or backdoors. The C2 server can send instructions to the compromised systems, such as executing commands, downloading files, uploading data, or launching attacks.

The C2 server can alsoreceive information from the compromised systems, such as system information, keystrokes, screenshots, or credentials. References:

Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) v1.0, Module 3: Network Intrusion Analysis, Lesson 3.4: Malware Cisco Certified CyberOps Associate Overview, Exam Topics,

3.4 Compare and contrast types of malware

NO.31 The SOC team detected an ongoing port scan. After investigation, the team concluded that the scan was targeting the company servers. According to the Cyber Kill Chain model, which step must be assigned to this type of event?

A. actions on objectives

B. delivery

C. reconnaissance

D. exploitation

Answer: C

NO.32 A network engineer noticed in the NetFlow report that internal hosts are sending many DNS requests to external DNS servers A SOC analyst checked the endpoints and discovered that they are infected and became part of the botnet Endpoints are sending multiple DNS requests but with spoofed IP addresses of valid external sources What kind of attack are infected endpoints involved in1?

A. DNS hijacking

B. DNS tunneling

C. DNS flooding

D. DNS amplification

Answer: D

Explanation:

The attack described is a DNS amplification attack. It involves infected endpoints sending DNS requests with spoofed IP addresses to external DNS servers. The DNS servers then send large responses to the spoofed addresses, which are actually the targets of the attack. This can result in a significant amount of traffic being directed at the target, overwhelming their network resources. DNS amplification is a type of Distributed Denial of Service (DDoS) attack that leverages the DNS protocol to amplify the attack traffic.

NO.33 Which of these describes SOC metrics in relation to security incidents?

A. time it takes to detect the incident

B. time it takes to assess the risks of the incident

C. probability of outage caused by the incident

D. probability of compromise and impact caused by the incident

Answer: A

Explanation:

SOC metrics in relation to security incidents typically refer to the time it takes to detect the incident. These metrics are crucial for evaluating the effectiveness of incident response and remediation efforts by SOC teams. For example, metrics like the Mean Time to Detect (MTTD) enable organizations to assess how quickly they can identify a security incident, which is essential for reducing the impact of the incident on the organization.

NO.34 Which filter allows an engineer to filter traffic in Wireshark to further analyze the PCAP file by only showing the traffic for LAN 10.11.x.x, between workstations and servers without the Internet?

A. src=10.11.0.0/16 and dst=10.11.0.0/16
B. ip.src==10.11.0.0/16 and ip.dst==10.11.0.0/16
C. ip.src=10.11.0.0/16 and ip.dst=10.11.0.0/16
D. src==10.11.0.0/16 and dst==10.11.0.0/16
Answer: B
Explanation:
In Wireshark, to filter traffic for a specific LAN, the correct syntax uses ip.src== and ip.dst== to specify the source and destination IP addresses. The /16 denotes the subnet mask, indicating that we are interested in the entire 10.11.x.x range. This filter will show all traffic where both the source and destination IP addresses fall within the specified LAN, excluding any internet traffic. References: The information is based on the Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) course, which covers network intrusion analysis and the use of tools like Wireshark for traffic analysis1.

NO.35 What is the virtual address space for a Windows process?
A. physical location of an object in memory
B. set of pages that reside in the physical memory
C. system-level memory protection feature built into the operating system
D. set of virtual memory addresses that can be used
Answer: D
Explanation:
The virtual address space for a Windows process is the set of virtual memory addresses that can be used by the process. Each process has its own virtual address space that is isolated from other processes. The virtual address space is divided into regions that have different attributes, such as read-only, read-write, execute, and so on. The virtual address space is mapped to the physical memory by the operating system using a data structure called a page table. References: Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) v1.0, Module 4: Host-Based Analysis, Lesson 4.1: Windows Operating System Virtual Address Space