Number: 200-201
Passing Score: 800
Time Limit: 120
File Version: 21.0

Exam Code: 200-201
Exam Name: Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)

Exam A

QUESTION 1
Refer to the exhibit.

Which component is identifiable in this exhibit?

A. Trusted Root Certificate store on the local machine
B. Windows PowerShell verb
C. Windows Registry hive
D. local service in the Windows Services Manager

Correct Answer: C
Section:
Explanation:
Explanation:
https://docs.microsoft.com/en-us/windows/win32/sysinfo/registry-hives
https://ldapwiki.com/wiki/HKEY_LOCAL_MACHINE#:~:text=HKEY_LOCAL_MACHINE%20Windows%20registry%20hive%20contains,detected%20hardware%20and%20device%20drivers.

QUESTION 2
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 -d" to decrease the priority state of high load processes to avoid resource exhaustion.
B. Run "ps -u" to find out who executed additional processes that caused a high load on a server.
C. Run "ps -ef" to understand which processes are taking a high amount of resources.
D. Run "ps -m" to capture the existing state of daemons and map required processes to find the gap.

Correct Answer: C
Section:

Explanation:
Explanation:
Reference: https://unix.stackexchange.com/questions/62182/please-explain-this-output-of-ps-efcommand

QUESTION 3
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:
Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/650/configuration/guide/fpmc-configguide-v65/inline_sets_and_passive_interfaces_for_firepower_threat_defense.html

QUESTION 4
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:
Explanation:

QUESTION 5
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:
Explanation:

QUESTION 6
An engineer needs to discover alive hosts within the 192.168.1.0/24 range without triggering intrusive portscan alerts on the IDS device using Nmap. Which command will accomplish this goal?

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

Correct Answer: B
Section:
Explanation:
Explanation:

QUESTION 7
An analyst is investigating a host in the network that appears to be communicating to a command and control server on the Internet. After collecting this packet capture, the analyst cannot determine the technique and payload used for the communication.

```
File     Actions     Edit     View     Help

   48 41.270348133 185.199.111.153 → 192.168.88.164 TLSv1.2 123 Application Data
   49 41.270348165 185.199.111.153 → 192.168.88.164 TLSv1.2 104 Application Data
   50 41.270356290 192.168.88.164 → 185.199.111.153 TCP 66 44736 → 443 [ACK]
Seq=834 Ack=3104 Win=64128 Len=0 TSval=3947973757 TSecr=2989424849
   51 41.270369874 192.168.88.164 → 185.199.111.153 TCP 66 44736 → 443 [ACK]
Seq=834 Ack=3142 Win=64128 Len=0 TSval=3947973757 TSecr=2989424849
   52 41.270430171 192.168.88.164 → 185.199.111.153 TLSv1.2 104 Application Data
   53 41.271767772 185.199.111.153 → 192.168.88.164 TLSv1.2 2854 Application Data
   54 41.271767817 185.199.111.153 → 192.168.88.164 TLSv1.2 904 Application Data
   55 41.271788996 192.168.88.164 → 185.199.111.153 TCP 66 44736 → 443 [ACK]
Seq=872 Ack=6768 Win=62592 Len=0 TSval=3947973758 TSecr=2989424849
   56 41.271973293 192.168.88.164 → 185.199.111.153 TLSv1.2 97 Encrypted Alert
   57 41.272411701 192.168.88.164 → 185.199.111.153 TCP 66 44736 → 443 [FIN, ACK]
Seq=903 Ack=6768 Win=64128 Len=0 TSval=3947973759 TSecr=2989424849
   58 41.283301751 185.199.111.153 → 192.168.88.164 TCP 66 443 → 44736 [ACK]
Seq=6768 Ack=903 Win=28160 Len=0 TSval=2989424852 TSecr=3947973757
   59 41.283301808 185.199.111.153 → 192.168.88.164 TLSv1.2 97 Encrypted Alert
   60 41.283321947 192.168.88.164 → 185.199.111.153 TCP 54 44736 → 443 [RST]
Seq=903 Win=0 Len=0
   61 41.283939151 185.199.111.153 → 192.168.88.164 TCP 66 443 → 44736 [FIN, ACK]
Seq=6799 Ack=903 Win=28160 Len=0 TSval=2989424852 TSecr=3947973757
   62 41.283945760 192.168.88.164 → 185.199.111.153 TCP 54 44736 → 443 [RST]
Seq=903 Win=0 Len=0
   63 41.284635561 185.199.111.153 → 192.168.88.164 TCP 66 443 → 44736 [ACK]
Seq=6800 Ack=904 Win=28160 Len=0 TSval=2989424853 TSecr=3947973759
   64 41.284642324 192.168.88.164 → 185.199.111.153 TCP 54 44736 → 443 [RST]
Seq=904 Win=0 Len=0
```

Which obfuscation technique is the attacker using?

A. Base64 encoding
B. transport layer security encryption
C. SHA-256 hashing
D. ROT13 encryption

Correct Answer: B
Section:
Explanation:
Explanation:
ROT13 is considered weak encryption and is not used with TLS (HTTPS:443). Source:
https://en.wikipedia.org/wiki/ROT13

QUESTION 8
What are two differences in how tampered and untampered disk images affect a security incident?
(Choose two.)

A. Untampered images are used in the security investigation process
B. Tampered images are used in the security investigation process
C. The image is tampered if the stored hash and the computed hash match
D. Tampered images are used in the incident recovery process
E. The image is untampered if the stored hash and the computed hash match

Correct Answer: A, E
Section:
Explanation:
Explanation:
Cert Guide by Omar Santos, Chapter 9 - Introduction to digital Forensics. "When you collect evidence, you must protect its integrity. This involves making sure that nothing is added to the evidence and that nothing is deleted or destroyed (this is known as evidence preservation)."

QUESTION 9
During which phase of the forensic process is data that is related to a specific event labeled and recorded to preserve its integrity?

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

Correct Answer: C
Section:
Explanation:
Explanation:

QUESTION 10
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

Correct Answer: A
Section:
Explanation:

Explanation:
Preparation --> Detection and Analysis --> Containment, Erradicaion and Recovery --> Post-Incident Activity Detection and Analysis --> Profile networks and systems, Understand normal behaviors, Create a log retention policy, Perform event correlation. Maintain and use a knowledge base of information.Use Internet search engines for research. Run packet sniffers to collect additional data. Filter the data.
Seek assistance from others. Keep all host clocks synchronized. Know the different types of attacks and attack vectors. Develop processes and procedures to recognize the signs of an incident.
Understand the sources of precursors and indicators. Create appropriate incident documentation capabilities and processes. Create processes to effectively prioritize security incidents. Create processes to effectively communicate incident information (internal and external communications).
Ref: Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide

QUESTION 11
A malicious file has been identified in a sandbox analysis tool.

Which piece of information is needed to search for additional downloads of this file by other hosts?

A. file type
B. file size
C. file name
D. file hash value

Correct Answer: D
Section:
Explanation:
Explanation:

QUESTION 12
Which metric in CVSS indicates an attack that takes a destination bank account number and replaces it with a different bank account number?

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

Correct Answer: D
Section:
Explanation:
Explanation:

QUESTION 13
Refer to the exhibit.

```
192.168.10.10 – – [01/Dec/2020:11:12:22 -0200] "GET /icons/powered_by_rh.png HTT
P/1.1" 200 1213 "http://192.168.0.102/" "Mozilla/5.0 (X11; U; Linux x86_64; en-U
S; 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 2
88 "-" "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=&{()
} 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 within the exhibit?

A. regular GET requests
B. XML External Entities attack
C. insecure deserialization
D. cross-site scripting attack

Correct Answer: A
Section:
Explanation:
Explanation:
Reference: https://www.tutorialspoint.com/http/http_requests.htm
https://github.com/gwroblew/detectXSSlib/blob/master/test/attacks.txt

QUESTION 14
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]f1,3}\.){1,4}
C. ^ (?:[0-9]{1,3}\.)'
D. ^ ([0-9]-{3})

Correct Answer: A
Section:
Explanation:

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/security/security_management/cs-mars/4-3/user/guide/local_controller/appreexp.html

QUESTION 15
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:
Explanation:
A certificate authority is a computer or entity that creates and issues digital certificates. CA do not "authenticate" it validates. "D" is wrong because The digital certificate validate a user. CA --> DC --> user, server or whatever.
Reference: https://en.wikipedia.org/wiki/Certificate_authority

QUESTION 16
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:
Explanation:
Reference: https://www.cisco.com/c/en/us/products/security/what-is-a-security-platform.htmlsiem is log managment soar is vulnerability managment that automat and response

QUESTION 17
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:
Explanation:
Instead of searching for patterns linked to specific types of attacks, behavior-based IDS solutions monitor behaviors that may be linked to attacks, increasing the likelihood of identifying and mitigating a malicious action before the network is compromised. https://accedian.com/blog/whatis- the-difference-between-signature-based-and-behavior-based-ids/

QUESTION 18

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 icmpcode 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: C
Section:
Explanation:
Explanation:

QUESTION 19
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: A
Section:
Explanation:
Explanation:

QUESTION 20
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-m-the-middle attack

Correct Answer: C
Section:
Explanation:
Explanation:

QUESTION 21
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:
Explanation:
Host-based antivirus protection is also known as agent-based. Agent-based antivirus runs on every protected machine. Agentless antivirus protection performs scans on hosts from a centralized system. Agentless systems have become popular for virtualized environments in which multiple OS instances are running on a host simultaneously. Agent-based antivirus running in each virtualized system can be a serious drain on system resources. Agentless antivirus for virtual hosts involves the use of a special security virtual appliance that performs optimized scanning tasks on the virtual hosts.
An example of this is VMware's vShield.

QUESTION 22
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: B
Section:
Explanation:
Explanation:

QUESTION 23
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:
Explanation:

QUESTION 24
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:
Explanation:

QUESTION 25
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:
Explanation:

Explanation:

QUESTION 26
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:
Explanation:
Explanation:

QUESTION 27
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:
Explanation:
Explanation:

QUESTION 28
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:
Explanation:
Explanation:

QUESTION 29
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:
Explanation:
Explanation:

QUESTION 30
What is the practice of giving employees only those permissions necessary to perform their specific role within an organization?

A. least privilege
B. need to know
C. integrity validation
D. due diligence

Correct Answer: A
Section:
Explanation:
Explanation:

QUESTION 31
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

Correct Answer: D
Section:
Explanation:
Explanation:

QUESTION 32
Which security principle is violated by running all processes as root or administrator?

A. principle of least privilege
B. role-based access control
C. separation of duties
D. trusted computing base

Correct Answer: A
Section:
Explanation:
Explanation:

QUESTION 33
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

Correct Answer: D
Section:
Explanation:
Explanation:

QUESTION 34
What is the difference between deep packet inspection and stateful inspection?

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

Correct Answer: D
Section:
Explanation:
Explanation:

QUESTION 35
Which evasion technique is a function of ransomware?

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

Correct Answer: B
Section:
Explanation:
Explanation:

QUESTION 36
Refer to the exhibit.

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

A. First Packet
B. Initiator User
C. Ingress Security Zone
D. Source Port
E. Initiator IP

Correct Answer: D, E
Section:
Explanation:
Explanation:

QUESTION 37
What is the difference between statistical detection and rule-based detection models?

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

Correct Answer: B
Section:
Explanation:
Explanation:

QUESTION 38
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.

Correct Answer: A
Section:
Explanation:
Explanation:
A threat is any potential danger to an asset. If a vulnerability exists but has not yet been exploited— or, more importantly, it is not yet publicly known—the threat is latent and not yet realized.

QUESTION 39
Which attack method intercepts traffic on a switched network?

A. denial of service
B. ARP cache poisoning
C. DHCP snooping
D. command and control

Correct Answer: B
Section:
Explanation:
Explanation:
An ARP-based MITM attack is achieved when an attacker poisons the ARP cache of two devices with the MAC address of the attacker's network interface card (NIC). Once the ARP caches have been successfully poisoned, each victim device sends all its packets to the attacker when communicating to the other device and puts the attacker in the middle of the communications path between the two victim devices. It allows an attacker to easily monitor all communication between victim devices. The intent is to intercept and view the information being passed between the two victim devices and potentially introduce sessions and traffic between the two victim devices

QUESTION 40
What does an attacker use to determine which network ports are listening on a potential target device?

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

Correct Answer: B
Section:
Explanation:
Explanation:

QUESTION 41
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:
Explanation:

QUESTION 42
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:
Explanation:

QUESTION 43
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:
Explanation:

QUESTION 44
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: D
Section:
Explanation:
Explanation:Attack Vector (AV) represents the level of access an attacker needs to have to exploit a vulnerability.It can assume four values: Network, Adjacent, Local and Physical. Source: Official cert Guide Cisco CyberOps Associate CBROPS 200-201 Chapter7: Introduction to Security Operations Management.

QUESTION 45
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: C
Section:
Explanation:
Explanation:

QUESTION 46
An engineer receives a security alert that traffic with a known TOR exit node has occurred on the network. What is the impact of this traffic?

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

Correct Answer: D
Section:
Explanation:
Explanation:

QUESTION 47
What is an example of social engineering attacks?

A. receiving an unexpected email from an unknown person with an attachment from someone in the same company
B. receiving an email from human resources requesting a visit to their secure website to update contact information
C. sending a verbal request to an administrator who knows how to change an account password
D. receiving an invitation to the department's weekly WebEx meeting

Correct Answer: C
Section:
Explanation:
Explanation:

QUESTION 48
Refer to the exhibit.

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

What is occurring in this network?

A. ARP cache poisoning
B. DNS cache poisoning

C. MAC address table overflow
D. MAC flooding attack

Correct Answer: A
Section:
Explanation:
Explanation:

QUESTION 49
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:
Explanation:

QUESTION 50
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:
Explanation:

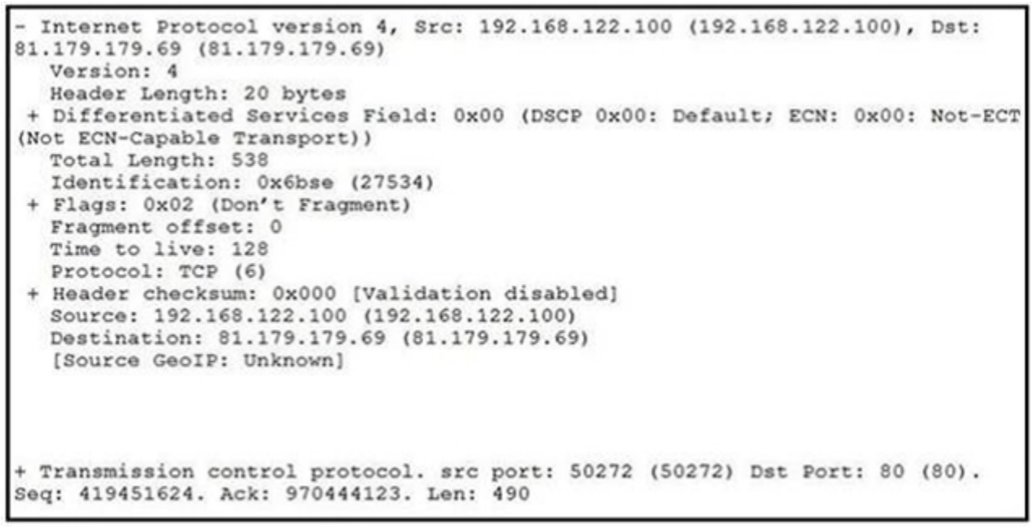
QUESTION 51
Which type of attack occurs when an attacker is successful in eavesdropping on a conversation between two IP phones?

A. known-plaintext
B. replay
C. dictionary
D. man-in-the-middle

Correct Answer: D
Section:
Explanation:
Explanation:

QUESTION 52

Refer to the exhibit.



What should be interpreted from this packet capture?

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

Correct Answer: B
Section:
Explanation:
Explanation:

QUESTION 53
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: C, E
Section:
Explanation:
Explanation:

QUESTION 54
Refer to the exhibit.

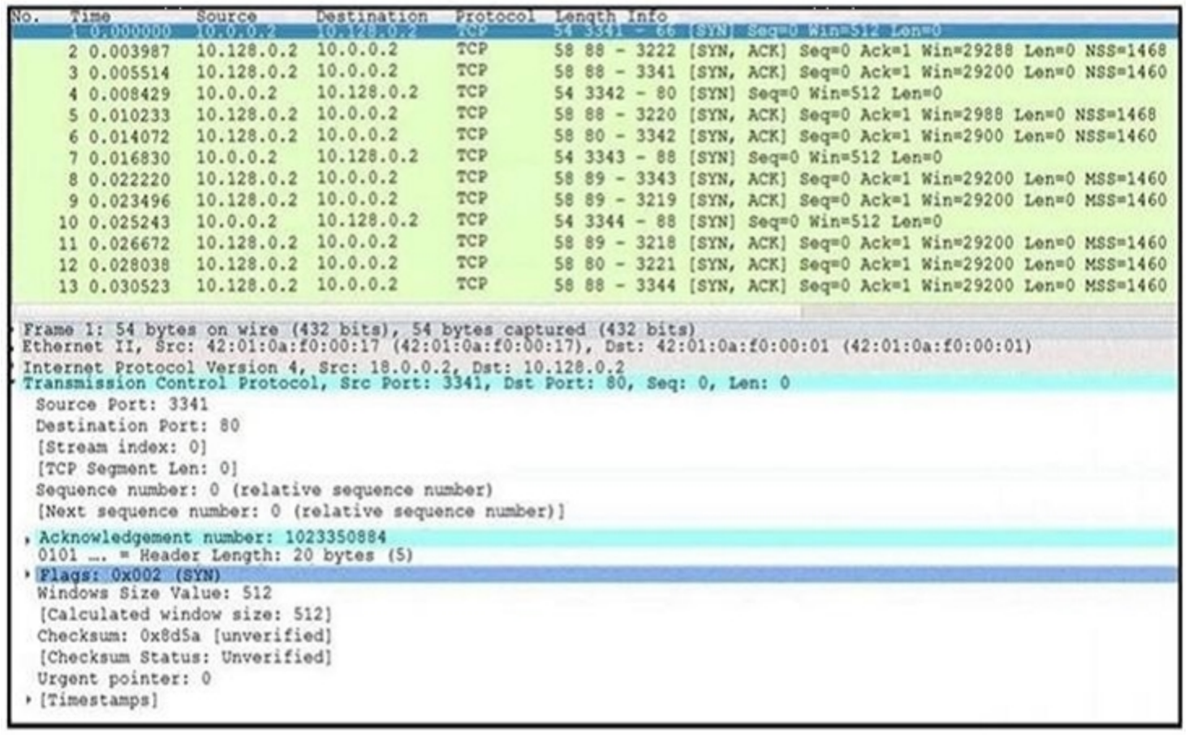
File name	CVE-2009-4324 PDF 2009-11-30 note200911.pdf
File size	400918 bytes
File type	PDF document, version 1.6
CRC32	11638A9B
MD5	61baabd6fc12e01ff73ceacc07c84f9a
SHA1	0805d0ae62f5358b9a3f4c1868d552fc3561b17
SHA256	27cced58a0fcbb0bbe3894f74d3014611039fefdf3bd2b0ba7ad85b18194c
SHA512	5a43bc7eef279b209e2590432cc3e2eb480d0f78004e265f00b98b4afdc9a
Ssdeep	1536:p0AAH2KthGBjcdBj8VETeePxsT65ZZ3pdx/ves/QR/875+:prahGV6B
PEID	None matched
Yara	• 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:
Explanation:
Explanation:

QUESTION 55
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 - 66 [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	80 - 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: D
Section:
Explanation:
Explanation:

QUESTION 56
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: A, E
Section:

Explanation:
Explanation:

QUESTION 57
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:
Explanation:

QUESTION 58
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: C
Section:
Explanation:
Explanation:

QUESTION 59
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:
Explanation:

QUESTION 60
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$

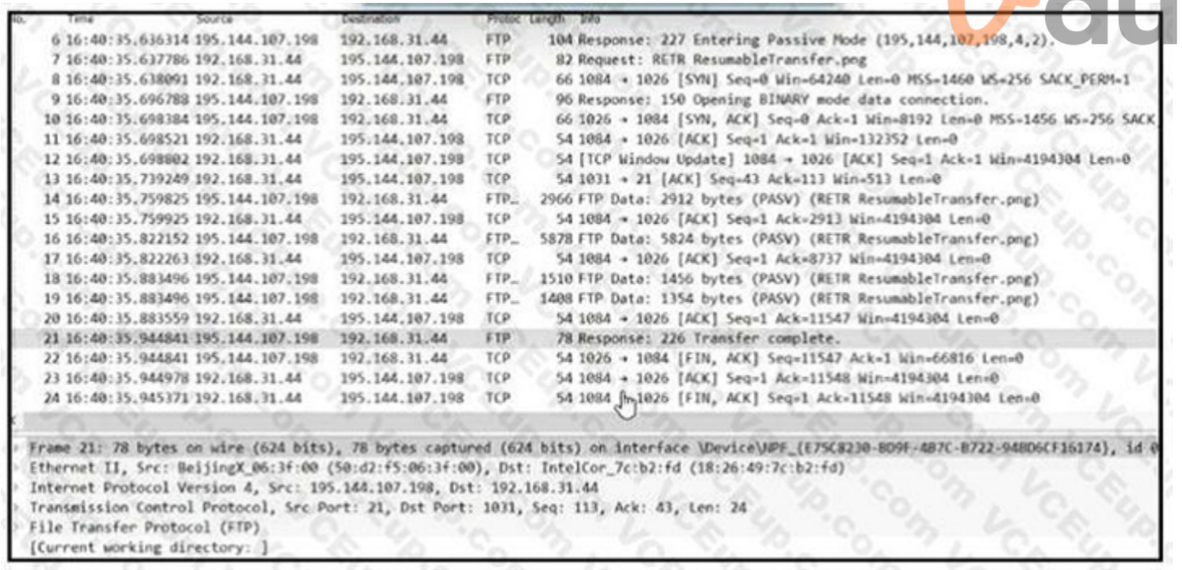
Correct Answer: A
Section:
Explanation:
Explanation:

QUESTION 61
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:
Explanation:

QUESTION 62
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

Correct Answer: B
Section:
Explanation:
Explanation:

QUESTION 63
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: D
Section:
Explanation:
Explanation:

QUESTION 64
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:
Explanation:

QUESTION 65
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:
Explanation:

QUESTION 66
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:
Explanation:

QUESTION 67
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: B
Section:
Explanation:
Explanation:

QUESTION 68
According to the September 2020 threat intelligence feeds a new malware called Egregor was introduced and used in many attacks. Distnbution of Egregor is pnmanly 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:
Explanation:

QUESTION 69
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 tile size is exceeded. Which action resolves the issue?

A. Add space to the existing partition and lower the retention penod.
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: D
Section:
Explanation:
Explanation:

QUESTION 70
What ate two categories of DDoS attacks? (Choose two.)

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

Correct Answer: D, E
Section:
Explanation:
Explanation:

QUESTION 71
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: C
Section:
Explanation:
Explanation:

QUESTION 72
What ate 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, C
Section:
Explanation:
Explanation:

QUESTION 73
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:
Explanation:

QUESTION 74
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:
Explanation:

QUESTION 75
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:
Explanation:

QUESTION 76
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:
Explanation:

QUESTION 77
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

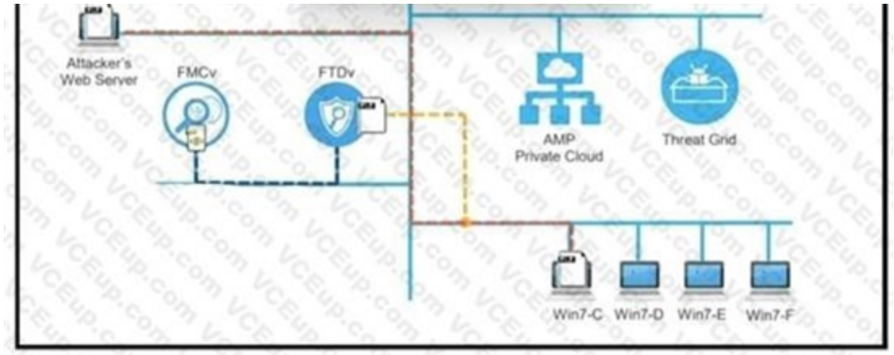
Correct Answer: B
Section:
Explanation:
Explanation:

QUESTION 78
What describes the defense-m-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: B
Section:
Explanation:
Explanation:

QUESTION 79
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

Correct Answer: B
Section:
Explanation:
Explanation:

QUESTION 80
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 binkley
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.

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:
Explanation:

QUESTION 81
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

Correct Answer: D
Section:
Explanation:
Explanation:

QUESTION 82
A company encountered a breach on its web servers using IIS 7 5 Dunng 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: B
Section:
Explanation:
Explanation:

QUESTION 83

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: A
Section:
Explanation:
Explanation:

QUESTION 84
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:
Explanation:

QUESTION 85
How does statistical detection differ from rule-based detection?

A. Statistical detection involves the evaluation of events, and rule-based detection requires an evaluated set of events to function.
B. Statistical detection defines legitimate data over time, and rule-based detection works on a predefined set of rules
C. Rule-based detection involves the evaluation of events, and statistical detection requires an evaluated set of events to function Rule-based detection defines
D. legitimate data over a period of time, and statistical detection works on a predefined set of rules

Correct Answer: B
Section:
Explanation:
Explanation:

QUESTION 86
Refer to the exhibit.

```
Capturing on 'eth0'
    1 0.000000000 ca:4f:4d:4b:38:5a ? Broadcast    ARP 42 Who has 192.168.88.149?
Tell 192.168.88.12
    2 0.000055428 82:69:61:3e:fa:99 ? ca:4f:4d:4b:38:5a ARP 42 192.168.88.149 is at
82:69:61:3e:fa:99
    3 0.000080556 192.168.88.12 ? 192.168.88.149 TCP 74 49098 ? 80 [SYN] Seq=0
Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=65609529 TSecr=0 WS=128
```

What must be interpreted from this packet capture?

A. IP address 192.168.88 12 is communicating with 192 168 88 149 with a source port 74 to destination port 49098 using TCP protocol
B. IP address 192.168.88.12 is communicating with 192 168 88 149 with a source port 49098 to destination port 80 using TCP protocol.
C. IP address 192.168.88.149 is communicating with 192.168 88.12 with a source port 80 to destination port 49098 using TCP protocol.
D. IP address 192.168.88.149 is communicating with 192.168.88.12 with a source port 49098 to destination port 80 using TCP protocol.

Correct Answer: B
Section:
Explanation:
Explanation:

QUESTION 87
What is a benefit of using asymmetric cryptography?

A. decrypts data with one key
B. fast data transfer
C. secure data transfer
D. encrypts data with one key

Correct Answer: B
Section:
Explanation:
Explanation:

QUESTION 88
An organization is cooperating with several third-party companies. Data exchange is on an unsecured channel using port 80 Internal employees use the FTP service to upload and download sensitive data An engineer must ensure confidentiality while preserving the integrity of the communication. Which technology must the engineer implement in this scenario'?

A. X 509 certificates
B. RADIUS server
C. CA server
D. web application firewall

Correct Answer: A
Section:
Explanation:
Explanation:

QUESTION 89
A security engineer notices confidential data being exfiltrated to a domain "Ranso4134-mware31- 895" address that is attributed to a known advanced persistent threat group The engineer discovers that the activity is part of a real attack and not a network misconfiguration. Which category does this event fall under as defined in the Cyber Kill Chain?

A. reconnaissance
B. delivery
C. action on objectives
D. weaponization

Correct Answer: D
Section:
Explanation:
Explanation:

QUESTION 90
How does agentless monitoring differ from agent-based monitoring?

A. Agentless can access the data via API. while agent-base uses a less efficient method and accesses log data through WMI.
B. Agent-based monitoring is less intrusive in gathering log data, while agentless requires open ports to fetch the logs
C. Agent-based monitoring has a lower initial cost for deployment, while agentless monitoring requires resource-intensive deployment.
D. Agent-based has a possibility to locally filter and transmit only valuable data, while agentless has much higher network utilization

Correct Answer: B
Section:
Explanation:
Explanation:

QUESTION 91
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

Correct Answer: A
Section:
Explanation:
Explanation:

QUESTION 92
What is the difference between the ACK flag and the RST flag?

A. The RST flag approves the connection, and the ACK flag terminates spontaneous connections.
B. The ACK flag confirms the received segment, and the RST flag terminates the connection.
C. The RST flag approves the connection, and the ACK flag indicates that a packet needs to be resent
D. The ACK flag marks the connection as reliable, and the RST flag indicates the failure within TCP Handshake

Correct Answer: B
Section:
Explanation:
Explanation:

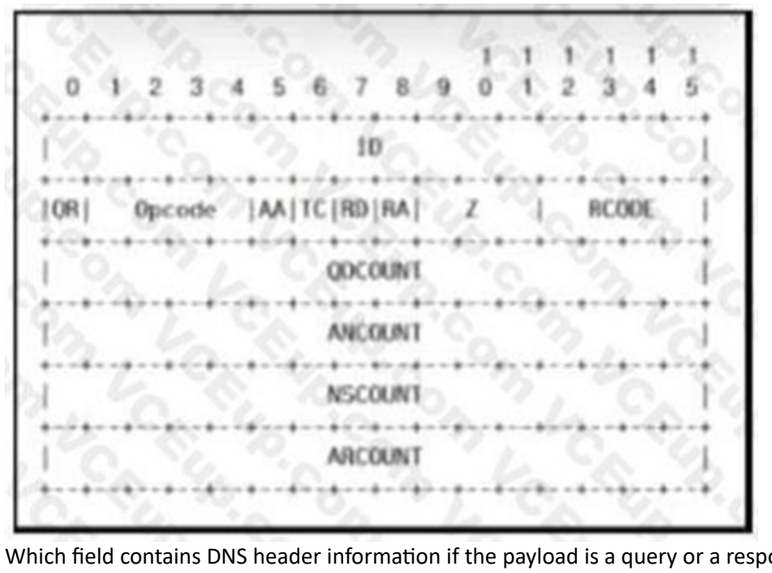
QUESTION 93
Refer to the exhibit.

An engineer is analyzing a PCAP file after a recent breach An engineer identified that the attacker used an aggressive ARP scan to scan the hosts and found web and SSH servers. Further analysis showed several SSH Server Banner and Key Exchange Initiations. The engineer cannot see the exact data being transmitted over an encrypted channel and cannot identify how the attacker gained access How did the attacker gain access?

A. by using the buffer overflow in the URL catcher feature for SSH
B. by using an SSH Tectia Server vulnerability to enable host-based authentication
C. by using an SSH vulnerability to silently redirect connections to the local host
D. by using brute force on the SSH service to gain access

Correct Answer: C
Section:
Explanation:
Explanation:

QUESTION 94
Refer to the exhibit.



Which field contains DNS header information if the payload is a query or a response?

A. Z
B. ID

C. TC
D. QR

Correct Answer: B
Section:
Explanation:
Explanation:

QUESTION 95
Refer to the exhibit.

What is occurring?

A. ARP flood
B. DNS amplification
C. ARP poisoning
D. DNS tunneling

Correct Answer: D
Section:
Explanation:
Explanation:

QUESTION 96
What is the difference between vulnerability and risk?

A. A vulnerability is a sum of possible malicious entry points, and a risk represents the possibility of the unauthorized entry itself.
B. A risk is a potential threat that an exploit applies to, and a vulnerability represents the threat itself
C. A vulnerability represents a flaw in a security that can be exploited, and the risk is the potential damage it might cause.
D. A risk is potential threat that adversaries use to infiltrate the network, and a vulnerability is an exploit

Correct Answer: C
Section:
Explanation:

Explanation:

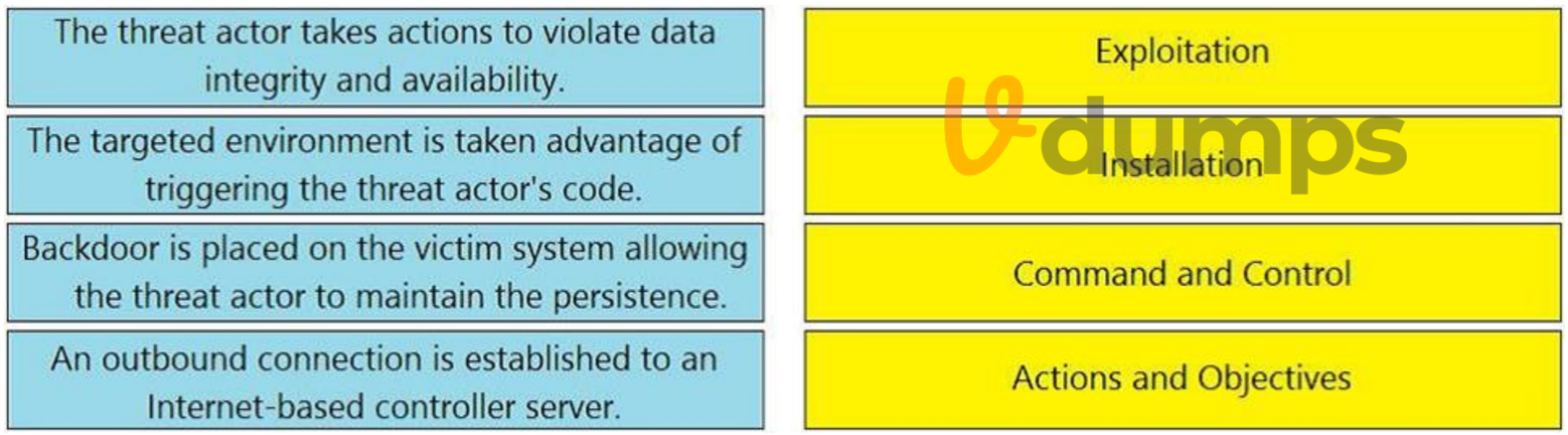
QUESTION 97
An engineer received a flood of phishing emails from HR with the source address HRjacobm@companycom. What is the threat actor in this scenario?

A. phishing email
B. sender
C. HR
D. receiver

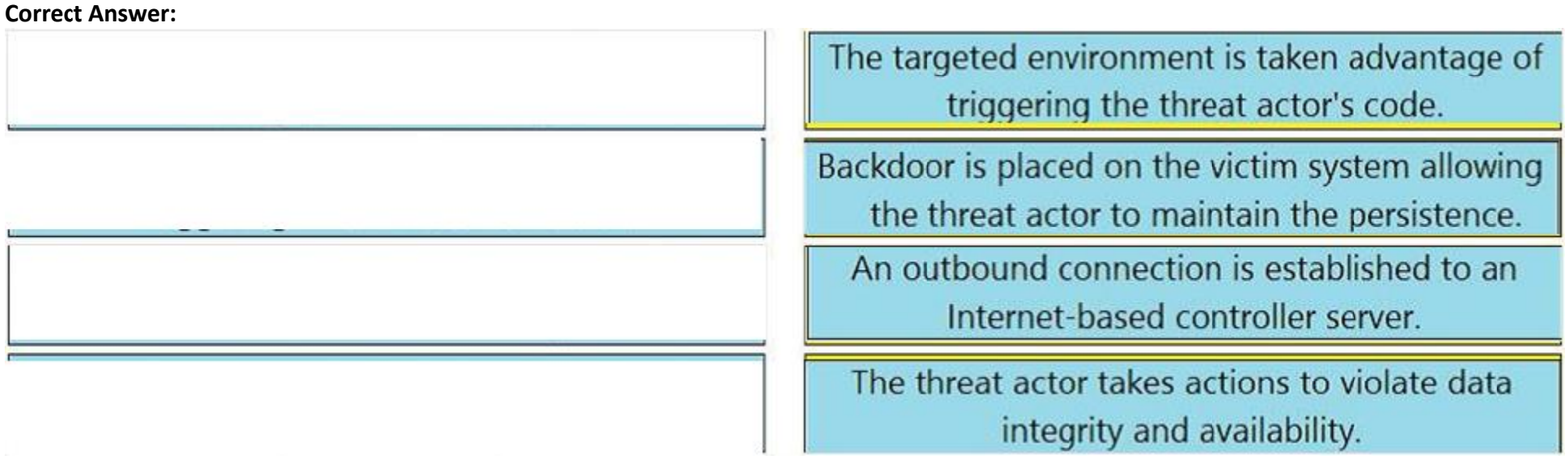
Correct Answer: B
Section:
Explanation:
Explanation:

QUESTION 98
DRAG DROP
Drag and drop the definition from the left onto the phase on the right to classify intrusion events according to the Cyber Kill Chain model.

Select and Place:



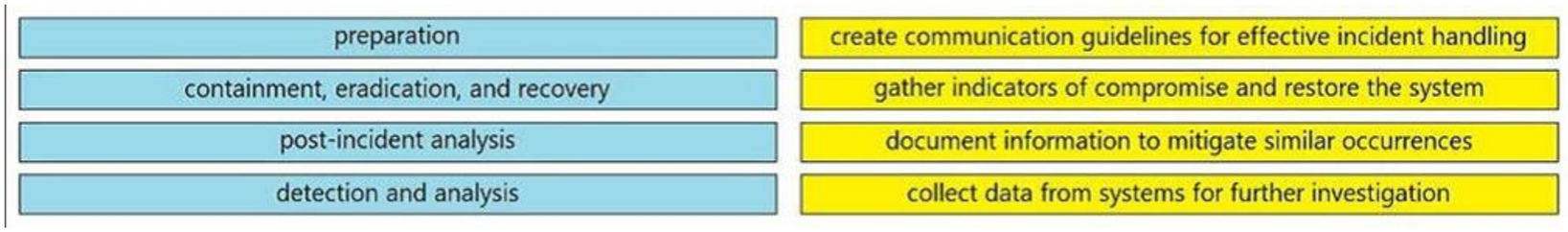
Correct Answer:



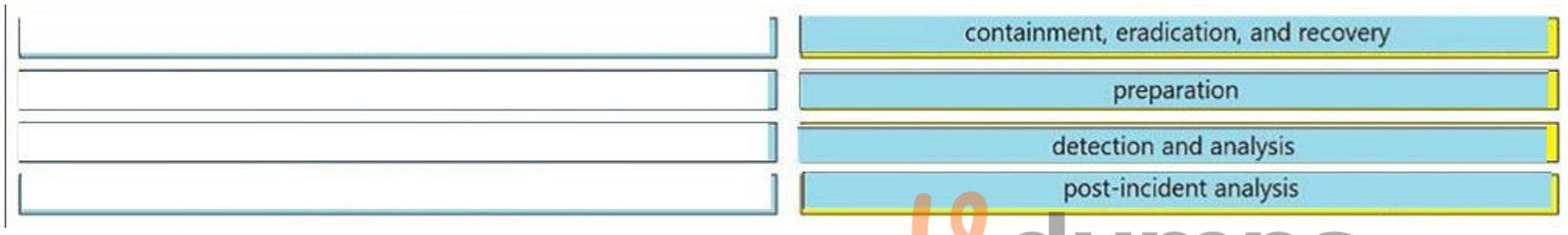
Section:
Explanation:

QUESTION 99
DRAG DROP
Drag and drop the elements from the left into the correct order for incident handling on the right.

Select and Place:



Correct Answer:



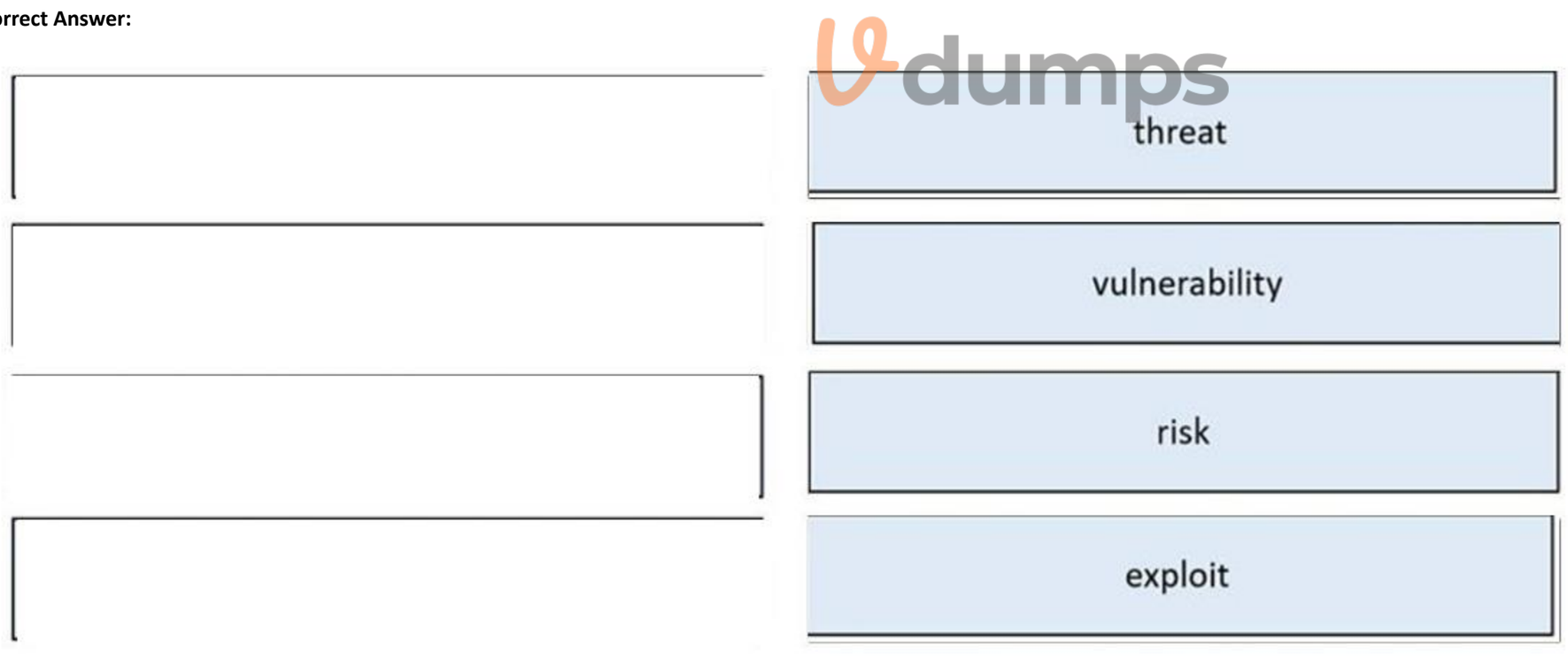
Section:
Explanation:

QUESTION 100
DRAG DROP
Drag and drop the security concept from the left onto the example of that concept on the right.

Select and Place:

threat	anything that can exploit a weakness that was not mitigated
risk	a gap in security or software that can be utilized by threats
vulnerability	possibility for loss and damage of an asset or information
exploit	taking advantage of a software flaw to compromise a resource

Correct Answer:



Section:
Explanation:

QUESTION 101
A user received a targeted spear-phishing email and identified it as suspicious before opening the content. To which category of the Cyber Kill Chain model does to this type of event belong?

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

Correct Answer: B
Section:

QUESTION 102
According to the NIST SP 800-86. which two types of data are considered volatile? (Choose two.)

A. swap files
B. temporary files
C. login sessions
D. dump files
E. free space

Correct Answer: C, E
Section:

QUESTION 103
Refer to the exhibit.

An engineer is reviewing a Cuckoo report of a file. What must the engineer interpret from the report?

A. The file will appear legitimate by evading signature-based detection.
B. The file will not execute its behavior in a sandbox environment to avoid detection.
C. The file will insert itself into an application and execute when the application is run.

D. The file will monitor user activity and send the information to an outside source.

Correct Answer: B
Section:

QUESTION 104
What is the difference between deep packet inspection and stateful inspection?

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

Correct Answer: D
Section:

QUESTION 105
What should an engineer use to aid the trusted exchange of public keys between user tom0411976943 and dan1968754032?

A. central key management server
B. web of trust
C. trusted certificate authorities
D. registration authority data

Correct Answer: C
Section:

QUESTION 106
Which tool gives the ability to see session data in real time?

A. tcpdstat
B. trafdump
C. tcptrace
D. trafshow

Correct Answer: C
Section:

QUESTION 107
Refer to the exhibit.

A security analyst is investigating unusual activity from an unknown IP address Which type of evidence is this file1?

A. indirect evidence
B. best evidence
C. corroborative evidence
D. direct evidence

Correct Answer: A
Section:
Explanation:
Explanation:

QUESTION 108
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

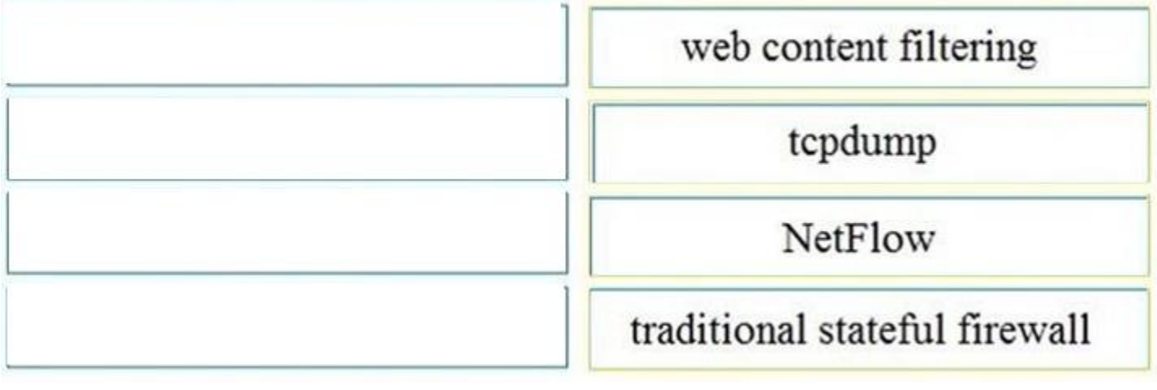
Correct Answer:

Section:
Explanation:

QUESTION 109
DRAG DROP
Drag and drop the technology on the left onto the data type the technology provides on the right.

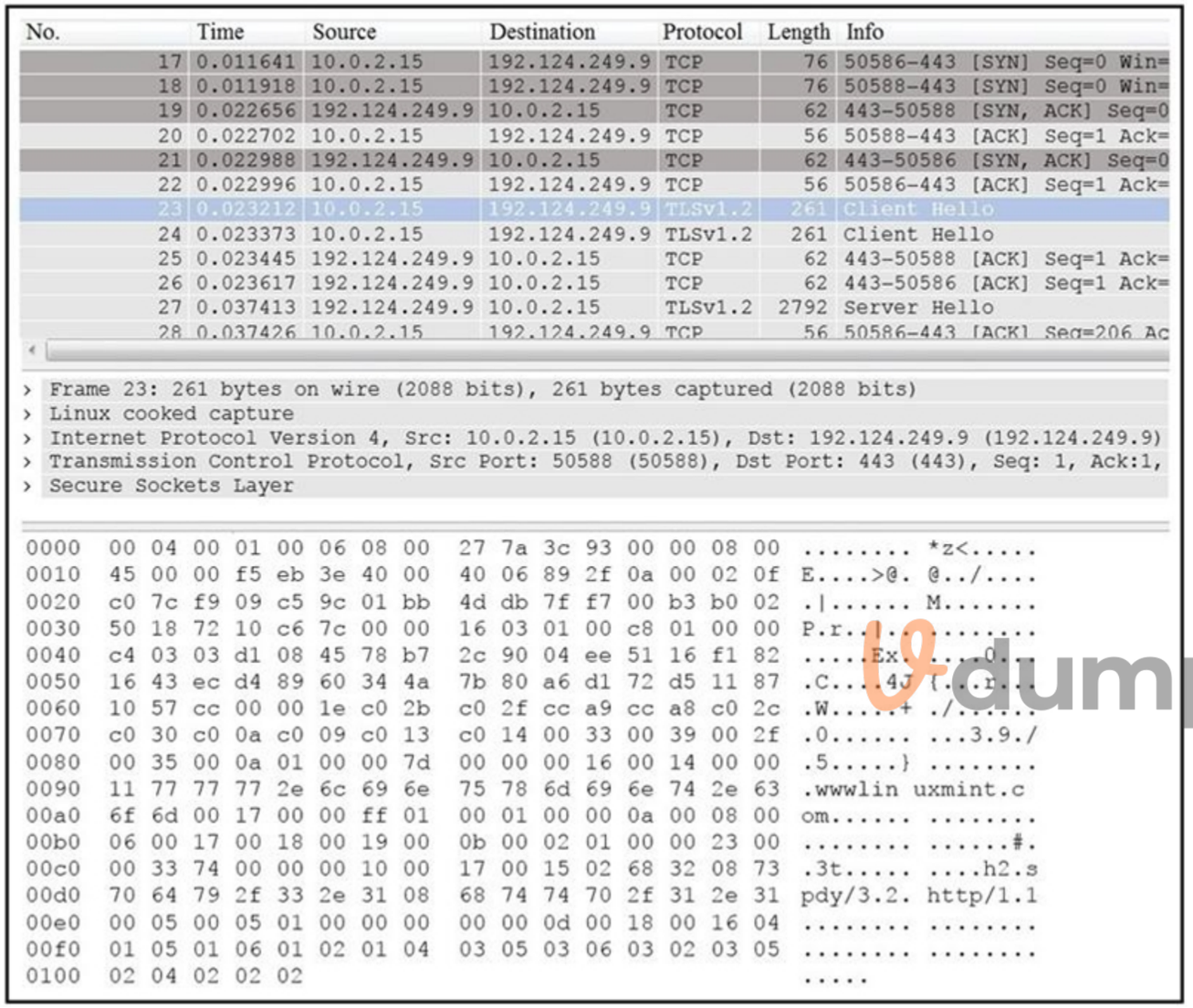
Select and Place:

Correct Answer:



Section:
Explanation:

QUESTION 110
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. ....Q...
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  .www.lin 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 111
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:

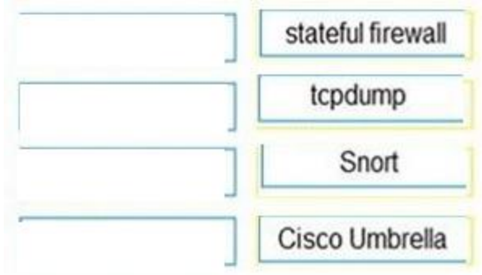
Explanation:

QUESTION 112
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

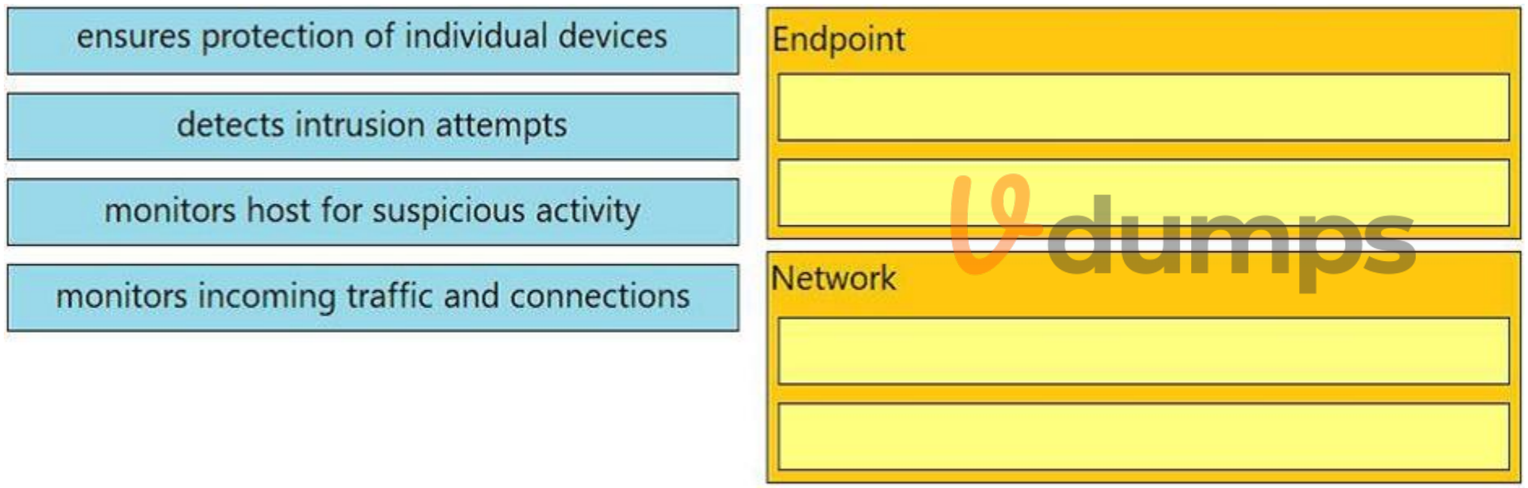
Correct Answer:



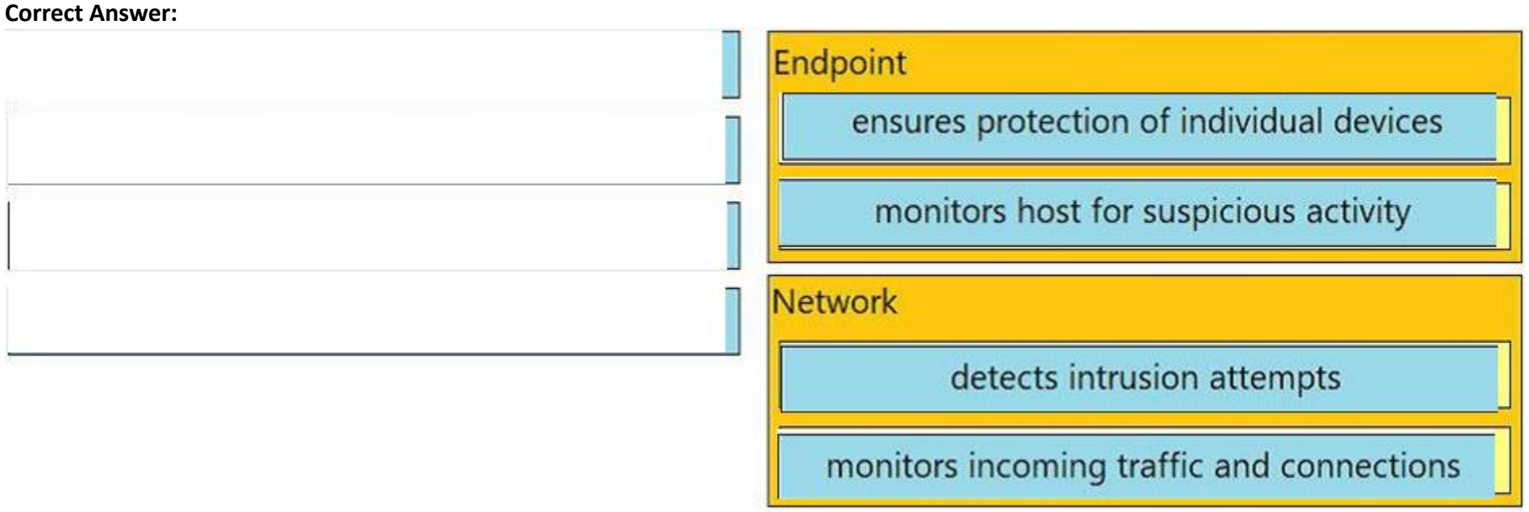
Section:
Explanation:

QUESTION 113
DRAG DROP
Drag and drop the uses on the left onto the type of security system on the right.

Select and Place:



Correct Answer:



Section:
Explanation:

QUESTION 114
Which two measures are used by the defense-m-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

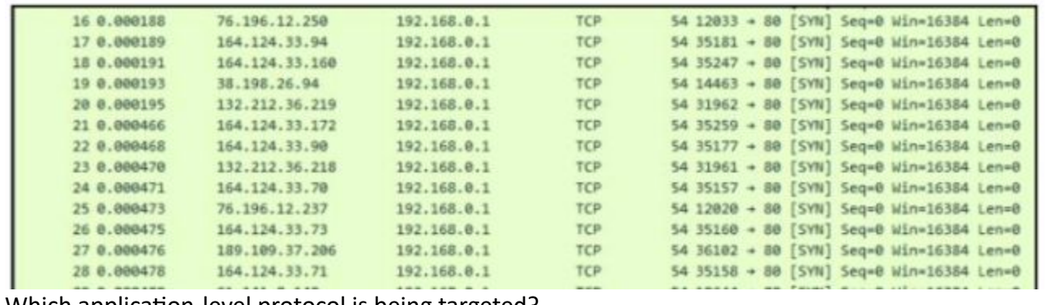
Correct Answer: B, E
Section:

QUESTION 115
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

Correct Answer: D
Section:

QUESTION 116
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 117
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:

QUESTION 118
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:

QUESTION 119
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: B, C
Section:

QUESTION 120
According to CVSS, what is a description of the attack vector score?

A. The metric score will be larger when it is easier to physically touch or manipulate the vulnerable component
B. It depends on how many physical and logical manipulations are possible on a vulnerable component
C. The metric score will be larger when a remote attack is more likely.
D. It depends on how far away the attacker is located and the vulnerable component

Correct Answer: C
Section:

QUESTION 121
Endpoint logs indicate that a machine has obtained an unusual gateway address and unusual DNS servers via DHCP Which type of attack is occurring?

A. command injection
B. man in the middle attack
C. evasion methods
D. phishing

Correct Answer: B
Section: