Cisco

Exam Questions 200-201

Understanding Cisco Cybersecurity Operations Fundamentals

NEW QUESTION 1
What is vulnerability management?

A. A security practice focused on clarifying and narrowing intrusion points.
B. A security practice of performing actions rather than acknowledging the threats.
C. A process to identify and remediate existing weaknesses.
D. A process to recover from service interruptions and restore business-critical applications

Answer: C

NEW QUESTION 2
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

Answer: C

Explanation:
https://docs.microsoft.com/en-us/windows/win32/sysinfo/registry-hives
https://ldapwiki.com/wiki/HKEY_LOCAL_MACHINE#:~:text=HKEY_LOCAL_MACHINE%20Windows%2

NEW QUESTION 3
An engineer must compare NIST vs ISO frameworks The engineer deeded to compare as readable documentation and also to watch a comparison video review. Using Windows 10 OS. the engineer started a browser and searched for a NIST document and then opened a new tab in the same browser and searched for an ISO document for comparison
The engineer tried to watch the video, but there 'was an audio problem with OS so the engineer had to troubleshoot it At first the engineer started CMD and looked fee a driver path then locked for a corresponding registry in the registry editor The engineer enabled "Audiosrv" in task manager and put it on auto start and the problem was solved Which two components of the OS did the engineer touch? (Choose two)

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

Answer: AC

NEW QUESTION 4
What is the difference between the ACK flag and the RST flag in the NetFlow log session?

A. The RST flag confirms the beginning of the TCP connection, and the ACK flag responds when the datafor the payload is complete
B. The ACK flag confirms the beginning of the TCP connection, and the RST flag responds when the data for the payload is complete
C. The RST flag confirms the receipt of the prior segment, and the ACK flag allows for the spontaneous termination of a connection
D. The ACK flag confirms the receipt of the prior segment, and the RST flag allows for the spontaneous termination of a connection

Answer: D

NEW QUESTION 5
What is a difference between inline traffic interrogation and traffic mirroring?

A. Inline inspection acts on the original traffic data flow
B. Traffic mirroring passes live traffic to a tool for blocking
C. Traffic mirroring inspects live traffic for analysis and mitigation
D. Inline traffic copies packets for analysis and security

Answer: A

Explanation:
Inline traffic interrogation analyzes traffic in real time and has the ability to prevent certain traffic from being forwarded Traffic mirroring doesn't pass the live traffic instead it copies traffic from one or more source ports and sends the copied traffic to one or more destinations for analysis by a network analyzer or other monitoring device

NEW QUESTION 6
Which incidence response step includes identifying all hosts affected by an attack?

A. detection and analysis

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

Answer: D

Explanation:
* 3.3.3 Identifying the Attacking Hosts During incident handling, system owners and others sometimes want to or need to identify the attacking host or hosts. Although this information can be important, incident handlers should generally stay focused on containment, eradication, and recovery.
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
The response phase, or containment, of incident response, is the point at which the incident response team begins interacting with affected systems and attempts to keep further damage from occurring as a result of the incident.

NEW QUESTION 7
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

Answer: B

NEW QUESTION 8
What are two denial of service attacks? (Choose two.)

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

Answer: CD

NEW QUESTION 9
A user received an email attachment named "Hr405-report2609-empl094.exe" but did not run it. Which category of the cyber kill chain should be assigned to this type of event?

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

Answer: D

NEW QUESTION 10
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$

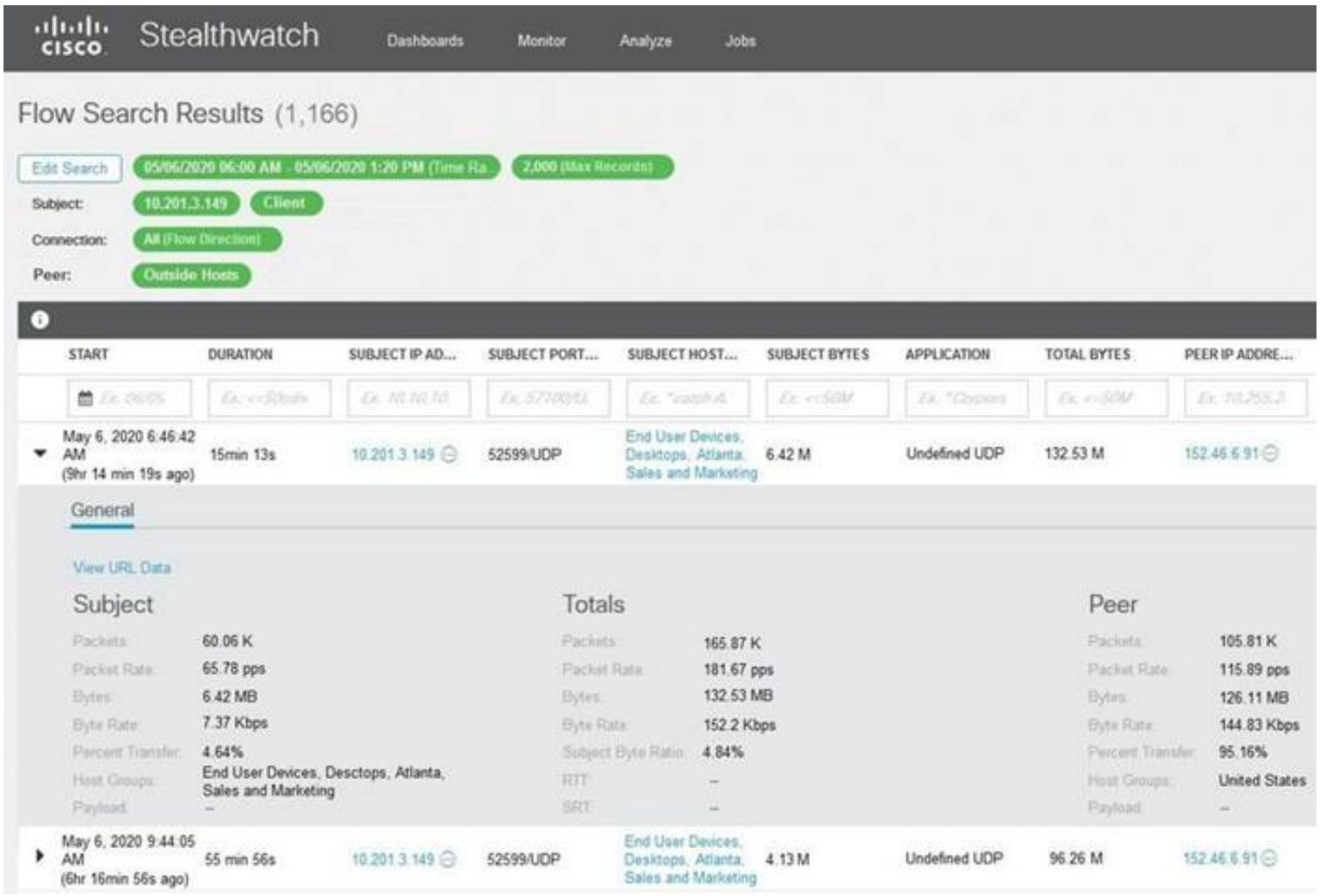
Answer: A

NEW QUESTION 10
Why is HTTPS traffic difficult to screen?

A. HTTPS is used internally and screening traffic (or external parties is hard due to isolation.
B. The communication is encrypted and the data in transit is secured.
C. Digital certificates secure the session, and the data is sent at random intervals.
D. Traffic is tunneled to a specific destination and is inaccessible to others except for the receiver.

Answer: B

NEW QUESTION 12
Refer to the exhibit.



What is the potential threat identified in this Stealthwatch dashboard?

A. Host 10.201.3.149 is sending data to 152.46.6.91 using TCP/443.
B. Host 152.46.6.91 is being identified as a watchlist country for data transfer.
C. Traffic to 152.46.6.149 is being denied by an Advanced Network Control policy.
D. Host 10.201.3.149 is receiving almost 19 times more data than is being sent to host 152.46.6.91.

Answer: D

NEW QUESTION 17
When an event is investigated, which type of data provides the investigate capability to determine if data exfiltration has occurred?

A. full packet capture
B. NetFlow data
C. session data
D. firewall logs

Answer: A

NEW QUESTION 18
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

Answer: B

NEW QUESTION 20
Which evasion technique is indicated when an intrusion detection system begins receiving an abnormally high volume of scanning from numerous sources?

A. resource exhaustion
B. tunneling
C. traffic fragmentation
D. timing attack

Answer: A

Explanation:
Resource exhaustion is a type of denial-of-service attack; however, it can also be used to evade detection by security defenses. A simple definition of resource exhaustion is “consuming the resources necessary to
perform an action.” Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide

NEW QUESTION 25
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

Answer: C

NEW QUESTION 26
Which piece of information is needed for attribution in an investigation?

A. proxy logs showing the source RFC 1918 IP addresses
B. RDP allowed from the Internet
C. known threat actor behavior
D. 802.1x RADIUS authentication pass arid fail logs

Answer: C

Explanation:
Actually this is the most important thing: know who, what, how, why, etc.. attack the network.

NEW QUESTION 30
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.

Answer: A

NEW QUESTION 31
Refer to the exhibit.

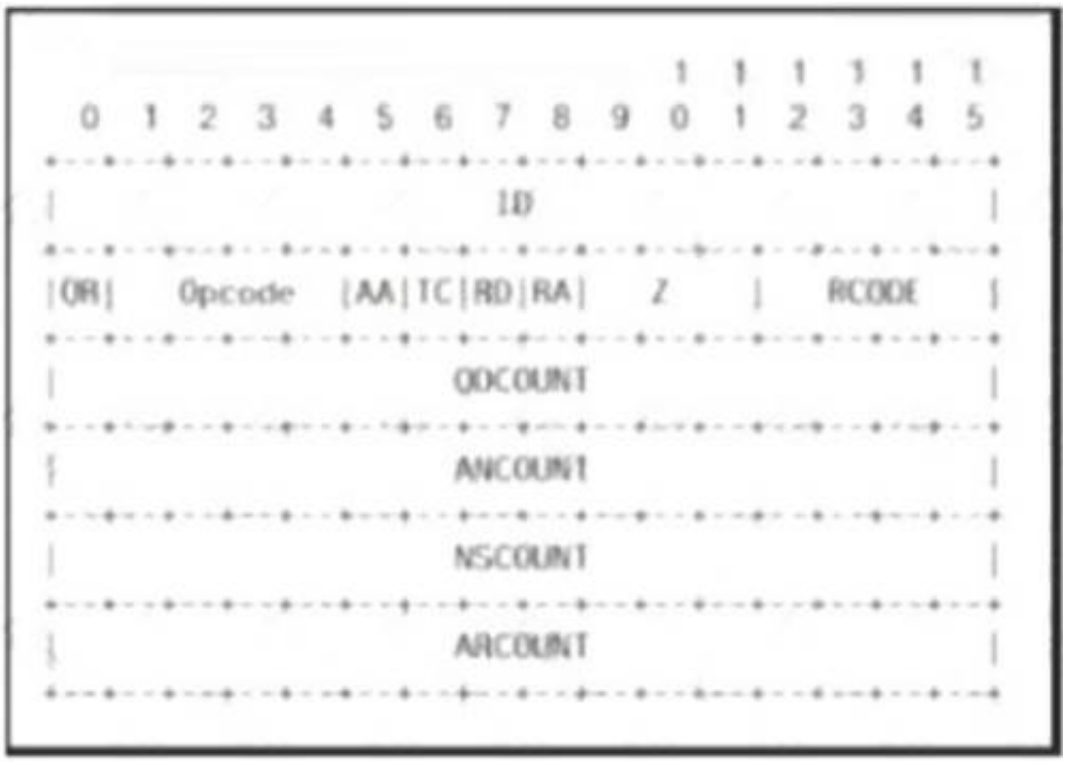
No.	Time	Source	Destination	Protocol	Length	Info
27336	245.7615440	192.168.154.129	192.168.154.131	FTP	79	Request: USER bjones
27337	245.7615820	192.168.154.129	192.168.154.131	FTP	79	Request: USER bjones
27338	245.7616210	192.168.154.129	192.168.154.131	FTP	79	Request: USER bjones
27340	245.7616680	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

Answer: B

NEW QUESTION 35
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

Answer: B

NEW QUESTION 36
An investigator is examining a copy of an ISO file that is stored in CDFS format. What type of evidence is this file?

A. data from a CD copied using Mac-based system
B. data from a CD copied using Linux system
C. data from a DVD copied using Windows system
D. data from a CD copied using Windows

Answer: B

Explanation:
CDfs is a virtual file system for Unix-like operating systems; it provides access to data and audio tracks on Compact Discs. When the CDfs driver mounts a Compact Disc, it represents each track as a file. This is consistent with the Unix convention "everything is a file". Source: https://en.wikipedia.org/wiki/CDfs

NEW QUESTION 41
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

Answer: AE

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)."

NEW QUESTION 43
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

Answer: B

NEW QUESTION 46
Which artifact is used to uniquely identify a detected file?

A. file timestamp
B. file extension
C. file size
D. file hash

Answer: D

NEW QUESTION 47
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

Answer: B

NEW QUESTION 49
How does agentless monitoring differ from agent-based monitoring?

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

Answer: B

NEW QUESTION 52
Which type of verification consists of using tools to compute the message digest of the original and copied data, then comparing the similarity of the digests?

A. evidence collection order
B. data integrity
C. data preservation
D. volatile data collection

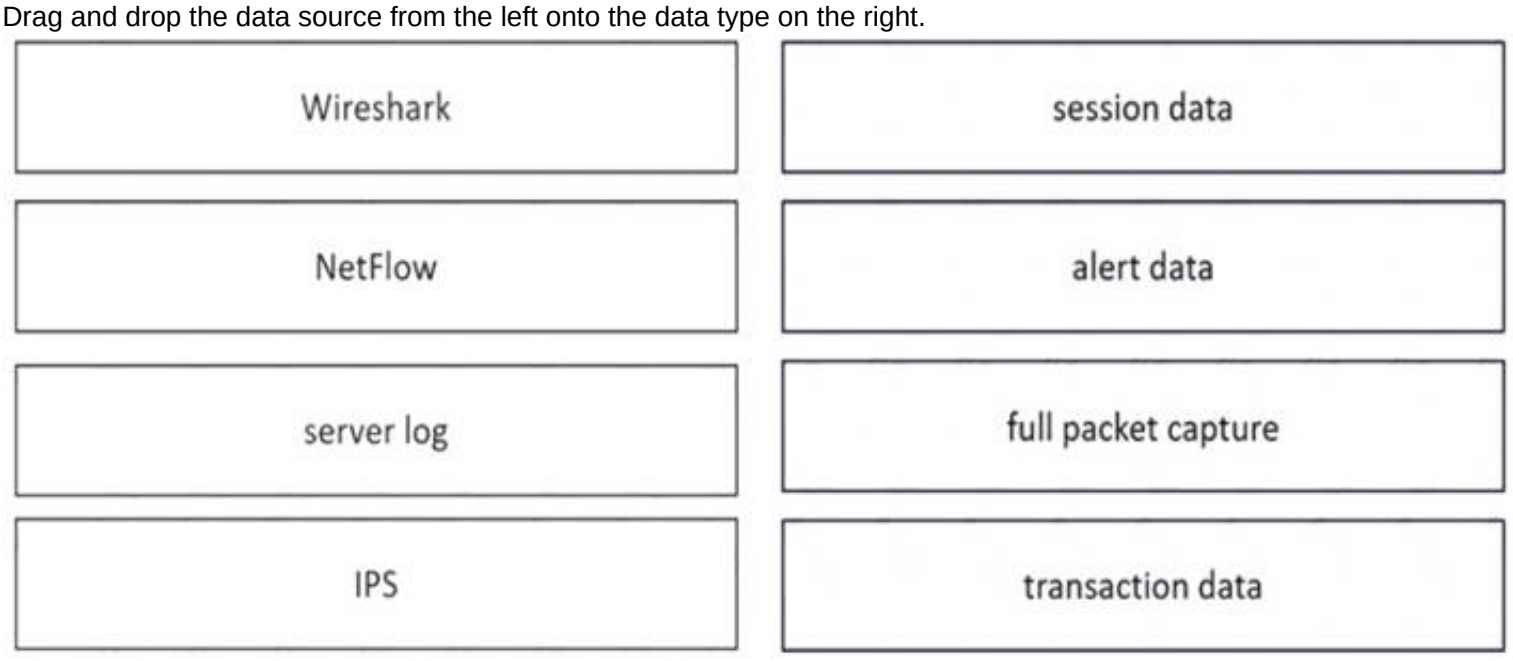
Answer: B

NEW QUESTION 56
Which type of data consists of connection level, application-specific records generated from network traffic?

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

Answer: A

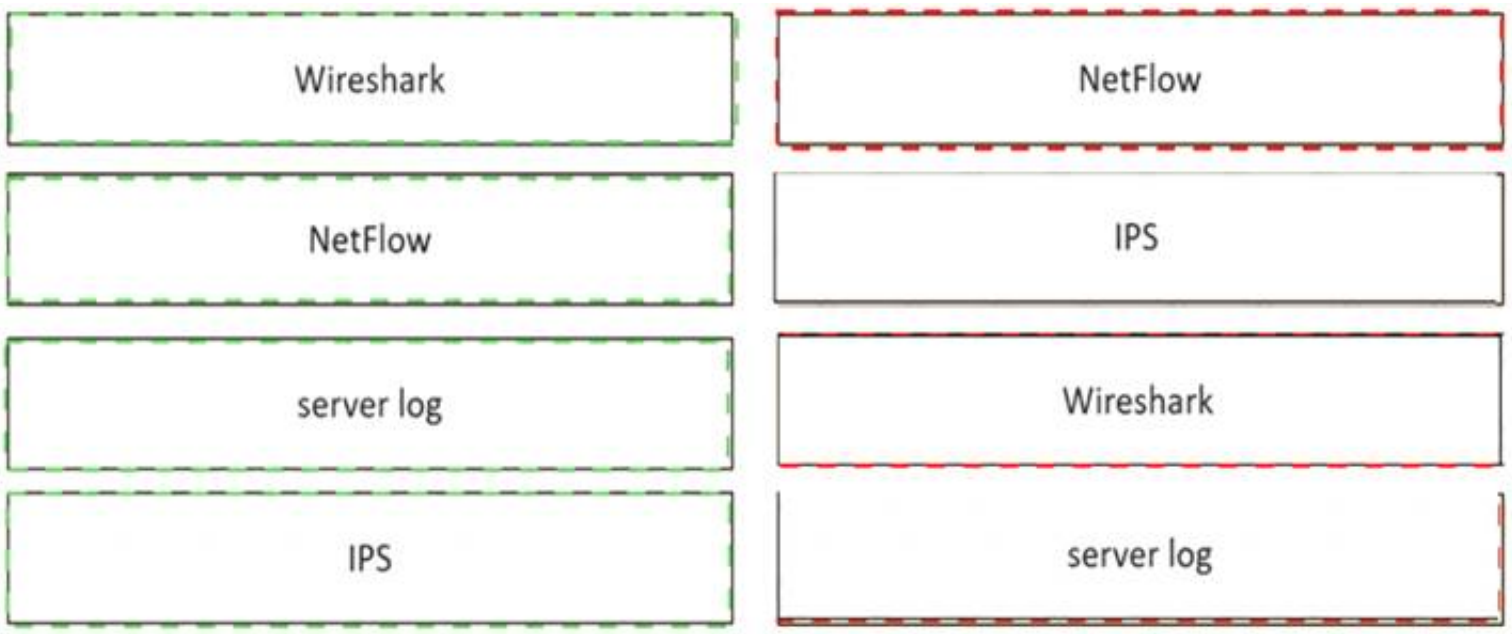
NEW QUESTION 61
Drag and drop the data source from the left onto the data type on the right.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 65
During which phase of the forensic process are tools and techniques used to extract information from the collected data?

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

Answer: D

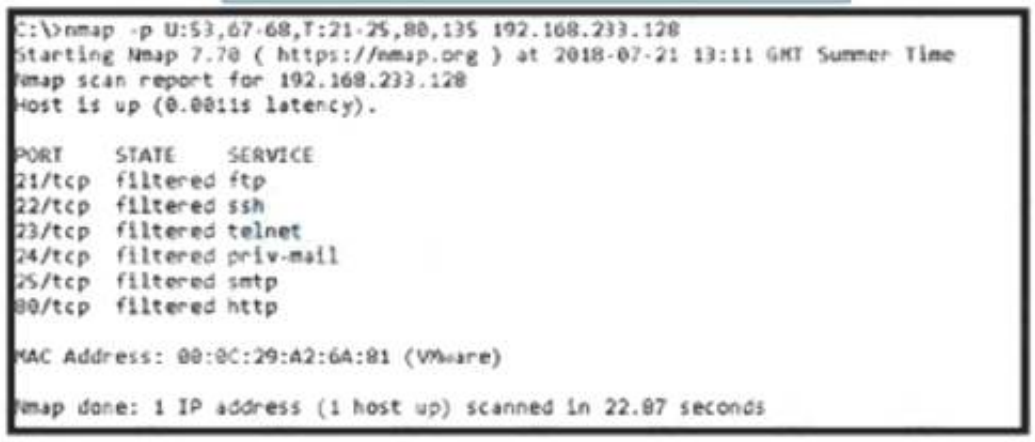
NEW QUESTION 70
Which step in the incident response process researches an attacking host through logs in a SIEM?

A. detection and analysis
B. preparation
C. eradication
D. containment

Answer: A

Explanation:
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

NEW QUESTION 73
Refer to the exhibit.



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

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

Answer: C

NEW QUESTION 76
Which technology prevents end-device to end-device IP traceability?

A. encryption
B. load balancing
C. NAT/PAT

D. tunneling

Answer: C

NEW QUESTION 78
Which event artifact is used to identify HTTP GET requests for a specific file?

A. destination IP address
B. TCP ACK
C. HTTP status code
D. URI

Answer: D

NEW QUESTION 83
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

Answer: B

NEW QUESTION 85
Refer to the exhibit.

```
Nov 30 17:48:43 ip-172-31-27-153 sshd[23001]: Invalid user password from 218.26.11.11
Nov 30 17:48:44 ip-172-31-27-153 sshd[23001]: Invalid user password from 218.26.11.11
Nov 30 17:48:46 ip-172-31-27-153 sshd[23003]: Invalid user password from 218.26.11.11
Nov 30 17:48:46 ip-172-31-27-153 sshd[23003]: Invalid user password from 218.26.11.11
Nov 30 17:48:46 ip-172-31-27-153 sshd[23003]: Invalid user password from 218.26.11.11
Nov 30 17:48:46 ip-172-31-27-153 sshd[23003]: Invalid user password from 218.26.11.11
Nov 30 17:48:48 ip-172-31-27-153 sshd[23005]: Invalid user password from 218.26.11.11
Nov 30 17:48:48 ip-172-31-27-153 sshd[23005]: Invalid user password from 218.26.11.11
Nov 30 17:48:48 ip-172-31-27-153 sshd[23005]: Invalid user password from 218.26.11.11
Nov 30 17:48:49 ip-172-31-27-153 sshd[23005]: Invalid user password from 218.26.11.11
Nov 30 17:48:51 ip-172-31-27-153 sshd[23007]: Invalid user password from 218.26.11.11
Nov 30 17:48:51 ip-172-31-27-153 sshd[23007]: Invalid user password from 218.26.11.11
Nov 30 17:48:51 ip-172-31-27-153 sshd[23007]: Invalid user password from 218.26.11.11
Nov 30 17:48:51 ip-172-31-27-153 sshd[23007]: Invalid user password from 218.26.11.11
Nov 30 17:48:54 ip-172-31-27-153 sshd[23009]: Invalid user password from 218.26.11.11
Nov 30 17:48:54 ip-172-31-27-153 sshd[23009]: Invalid user password from 218.26.11.11
Nov 30 17:48:54 ip-172-31-27-153 sshd[23009]: Invalid user password from 218.26.11.11
Nov 30 17:48:54 ip-172-31-27-153 sshd[23009]: Invalid user password from 218.26.11.11
Nov 30 17:48:56 ip-172-31-27-153 sshd[23011]: Invalid user password from 218.26.11.11
Nov 30 17:48:56 ip-172-31-27-153 sshd[23011]: Invalid user password from 218.26.11.11
Nov 30 17:48:56 ip-172-31-27-153 sshd[23011]: Invalid user password from 218.26.11.11
Nov 30 17:48:56 ip-172-31-27-153 sshd[23011]: Invalid user password from 218.26.11.11
Nov 30 17:48:59 ip-172-31-27-153 sshd[23013]: Invalid user password from 218.26.11.11
Nov 30 17:48:59 ip-172-31-27-153 sshd[23013]: Invalid user password from 218.26.11.11
```

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

Answer: A

NEW QUESTION 90
Refer to the exhibit.

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



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

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.

Answer: B

NEW QUESTION 92
Which principle is being followed when an analyst gathers information relevant to a security incident to determine the appropriate course of action?

A. decision making
B. rapid response
C. data mining
D. due diligence

Answer: D

NEW QUESTION 94
Which event is a vishing attack?

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

Answer: D

NEW QUESTION 96
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

NEW QUESTION 99
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

Answer: A

NEW QUESTION 102
What is a difference between tampered and untampered disk images?

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

Answer: D

NEW QUESTION 106
A company receptionist received a threatening call referencing stealing assets and did not take any action assuming it was a social engineering attempt. Within 48 hours, multiple assets were breached, affecting the confidentiality of sensitive information. What is the threat actor in this incident?

A. company assets that are threatened
B. customer assets that are threatened
C. perpetrators of the attack
D. victims of the attack

Answer: C

NEW QUESTION 111
Which HTTP header field is used in forensics to identify the type of browser used?

A. referrer
B. host
C. user-agent
D. accept-language

Answer: C

Explanation:
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:12.0) Gecko/20100101 Firefox/12.0 In computing, a user agent is any software, acting on behalf of a user, which "retrieves, renders and facilitates end-user interaction with Web content".[1] A user agent is therefore a special kind of software agent.
https://en.wikipedia.org/wiki/User_agent#User_agent_identification
A user agent is a computer program representing a person, for example, a browser in a Web context. https://developer.mozilla.org/en-US/docs/Glossary/User_agent

NEW QUESTION 114
What is threat hunting?

A. Managing a vulnerability assessment report to mitigate potential threats.
B. Focusing on proactively detecting possible signs of intrusion and compromise.
C. Pursuing competitors and adversaries to infiltrate their system to acquire intelligence data.
D. Attempting to deliberately disrupt servers by altering their availability

Answer: B

NEW QUESTION 116
What is the principle of defense-in-depth?

A. Agentless and agent-based protection for security are used.
B. Several distinct protective layers are involved.
C. Access control models are involved.
D. Authentication, authorization, and accounting mechanisms are used.

Answer: B

NEW QUESTION 117
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?

A. Cross-Site Scripting attack
B. XML External Entitles attack
C. Insecure Deserialization
D. Regular GET requests

Answer: A

NEW QUESTION 119
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

Answer: D

NEW QUESTION 123
Refer to the exhibit.

```
GET /item.php?id=34' or sleep(10)
```

This request was sent to a web application server driven by a database. Which type of web server attack is represented?

A. parameter manipulation
B. heap memory corruption
C. command injection
D. blind SQL injection

Answer: D

NEW QUESTION 128
An employee reports that someone has logged into their system and made unapproved changes, files are out of order, and several documents have been placed in the recycle bin. The security specialist reviewed the system logs, found nothing suspicious, and was not able to determine what occurred. The software is up to date; there are no alerts from antivirus and no failed login attempts. What is causing the lack of data visibility needed to detect the attack?

A. The threat actor used a dictionary-based password attack to obtain credentials.
B. The threat actor gained access to the system by known credentials.
C. The threat actor used the teardrop technique to confuse and crash login services.
D. The threat actor used an unknown vulnerability of the operating system that went undetected.

Answer: C

NEW QUESTION 131
Which open-sourced packet capture tool uses Linux and Mac OS X operating systems?

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

Answer: B

NEW QUESTION 132
What are two social engineering techniques? (Choose two.)

A. privilege escalation
B. DDoS attack
C. phishing
D. man-in-the-middle
E. pharming

Answer: CE

NEW QUESTION 135
An intruder attempted malicious activity and exchanged emails with a user and received corporate information, including email distribution lists. The intruder asked the user to engage with a link in an email. When the fink launched, it infected machines and the intruder was able to access the corporate network.
Which testing method did the intruder use?

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

Answer: A

NEW QUESTION 137
Which data format is the most efficient to build a baseline of traffic seen over an extended period of time?

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

Answer: C

NEW QUESTION 140
Which attack method intercepts traffic on a switched network?

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

Answer: B

Explanation:
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

NEW QUESTION 141
Which security technology allows only a set of pre-approved applications to run on a system?

A. application-level blacklisting
B. host-based IPS
C. application-level whitelisting
D. antivirus

Answer: C

NEW QUESTION 146
Which technology on a host is used to isolate a running application from other applications?

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

Answer: A

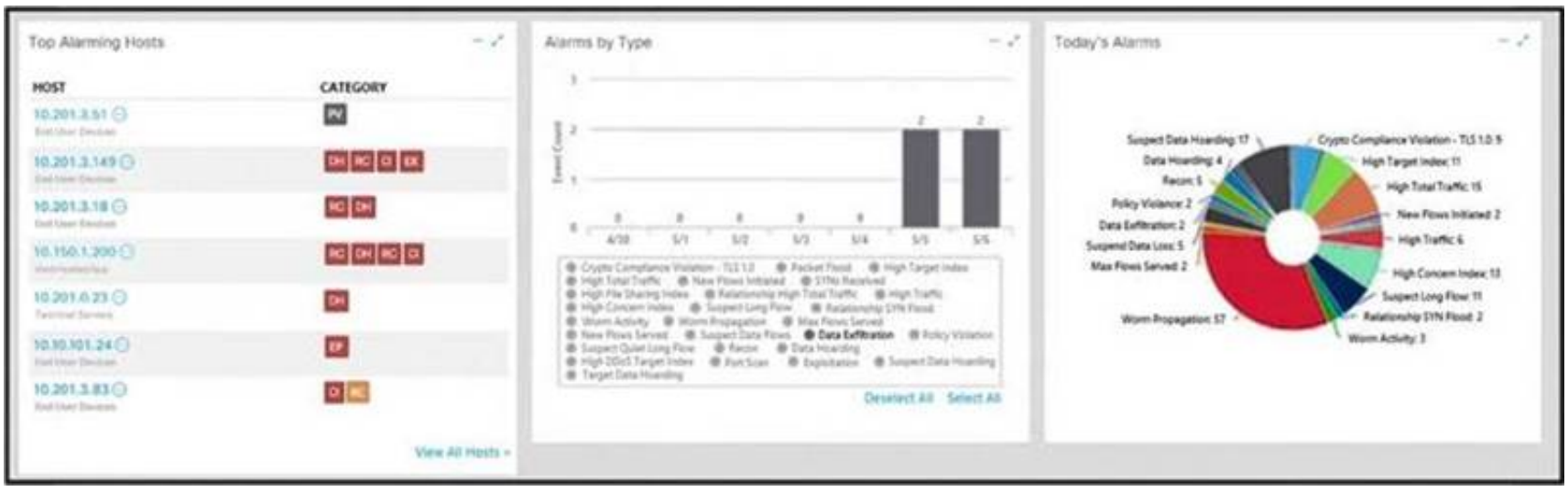
NEW QUESTION 148
Refer to the exhibit.

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.

Answer: B

NEW QUESTION 150
Refer to the exhibit.



What is the potential threat identified in this Stealthwatch dashboard?

A. A policy violation is active for host 10.10.101.24.
B. A host on the network is sending a DDoS attack to another inside host.
C. There are two active data exfiltration alerts.
D. A policy violation is active for host 10.201.3.149.

Answer: C

NEW QUESTION 151
Refer to the exhibit.

```
Mar 6 10:35:34 user sshd[12900]: pam_unix(sshd:auth):authentication failure;
logname= uid=0 euid=0 tty=ssh ruser= rhost=127.0.0.1
Mar 6 10:35:36 user sshd[12900]: Failed password for invalid user not_bill from
127.0.0.1 port 38346 ssh2
```

In which Linux log file is this output found?

A. /var/log/authorization.log
B. /var/log/dmesg
C. var/log/var.log
D. /var/log/auth.log

Answer: D

NEW QUESTION 156
An analyst discovers that a legitimate security alert has been dismissed. Which signature caused this impact on network traffic?

A. true negative
B. false negative
C. false positive
D. true positive

Answer: B

Explanation:
A false negative occurs when the security system (usually a WAF) fails to identify a threat. It produces a “negative” outcome (meaning that no threat has been observed), even though a threat exists.

NEW QUESTION 159
What is obtained using NetFlow?

A. session data
B. application logs
C. network downtime report
D. full packet capture

Answer: A

NEW QUESTION 163
Drag and drop the technology on the left onto the data type the technology provides on the right.

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

tcpdump	web content filtering
web content filtering	tcpdump
traditional stateful firewall	NetFlow
NetFlow	traditional stateful firewall

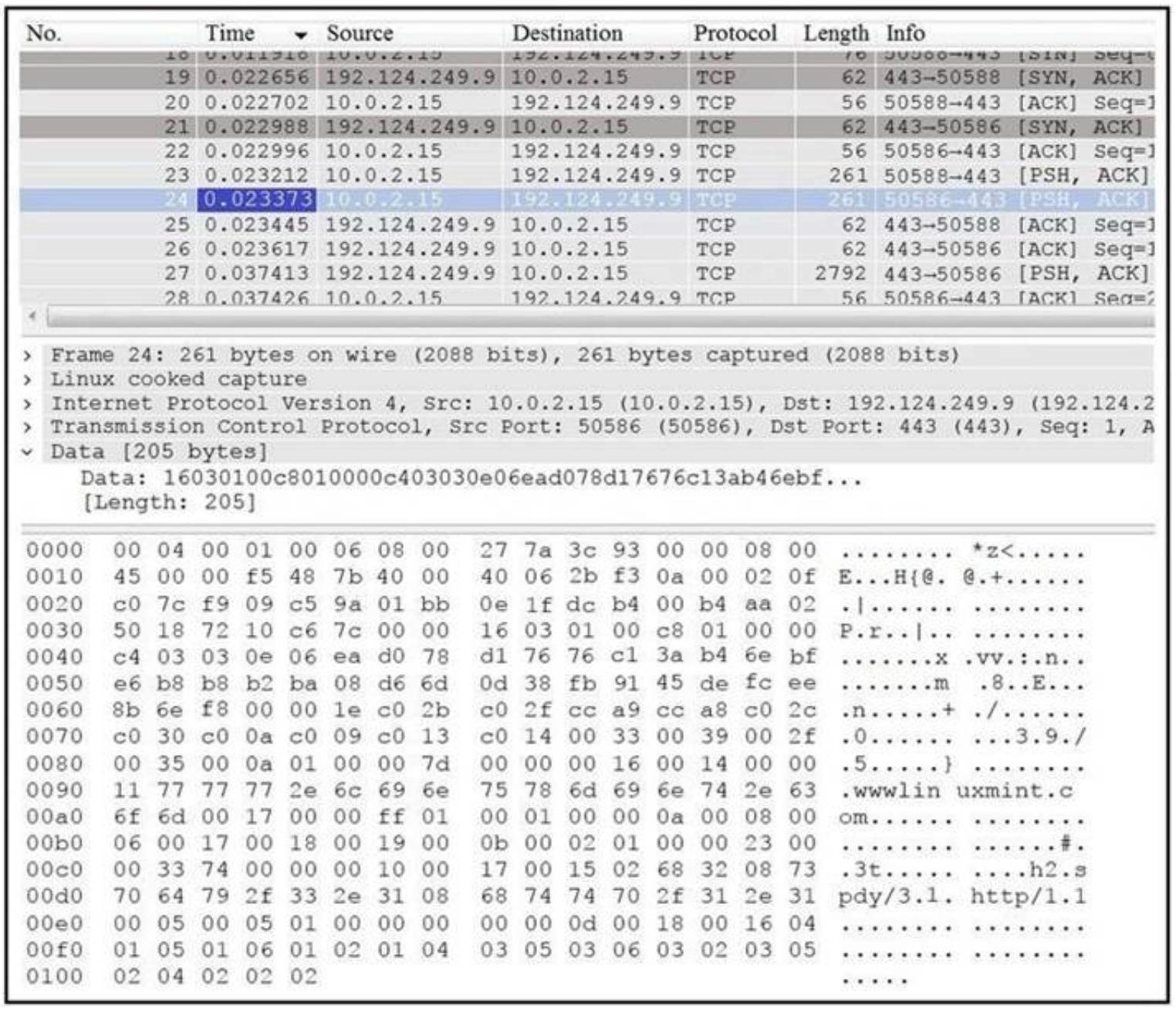
NEW QUESTION 165

Which utility blocks a host portscan?

A. HIDS
B. sandboxing
C. host-based firewall
D. antimalware

Answer: C

NEW QUESTION 168
Refer to the exhibit.

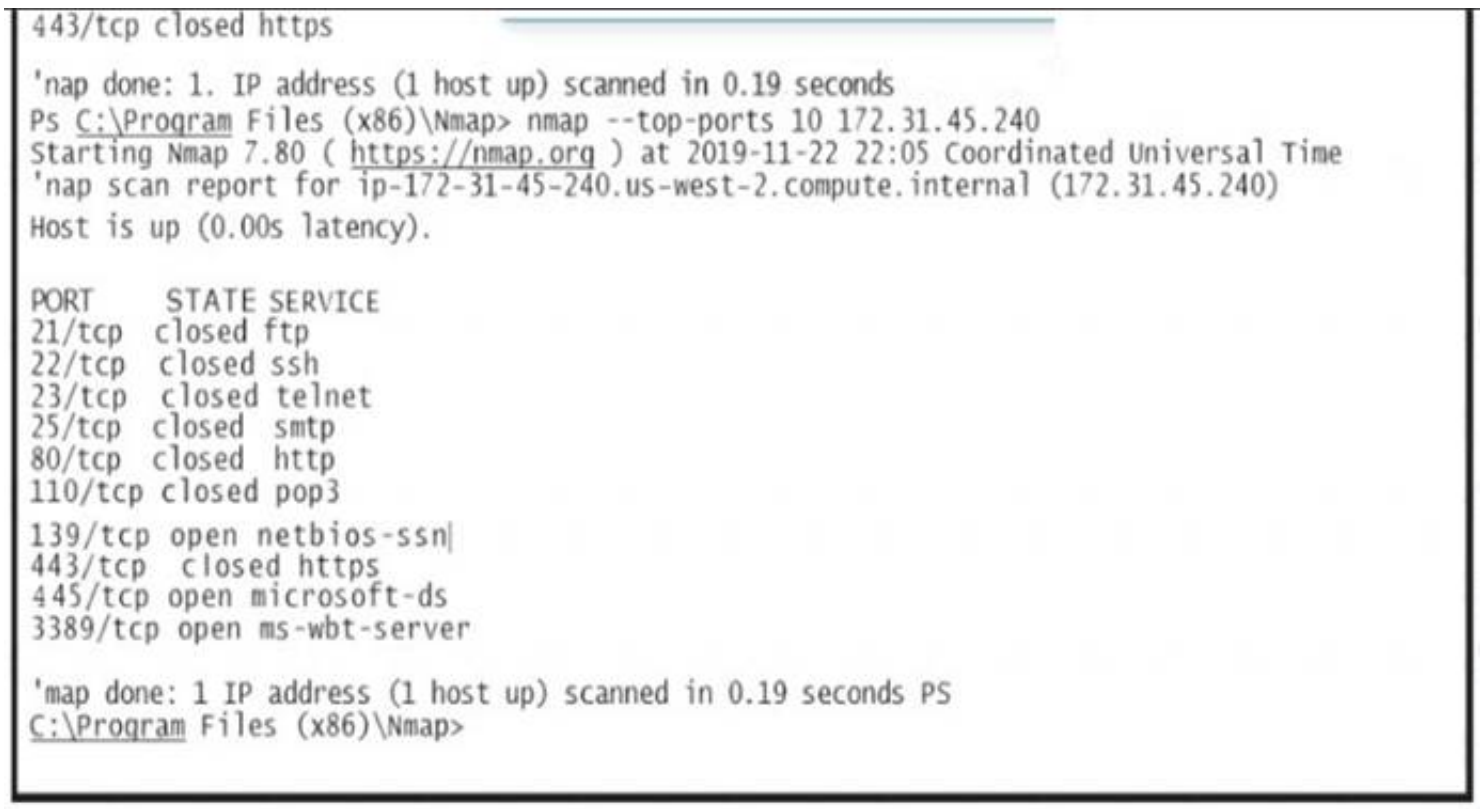


Which application protocol is in this PCAP file?

A. SSH
B. TCP
C. TLS
D. HTTP

Answer: D

NEW QUESTION 171
Refer to the exhibit.



What does this output indicate?

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

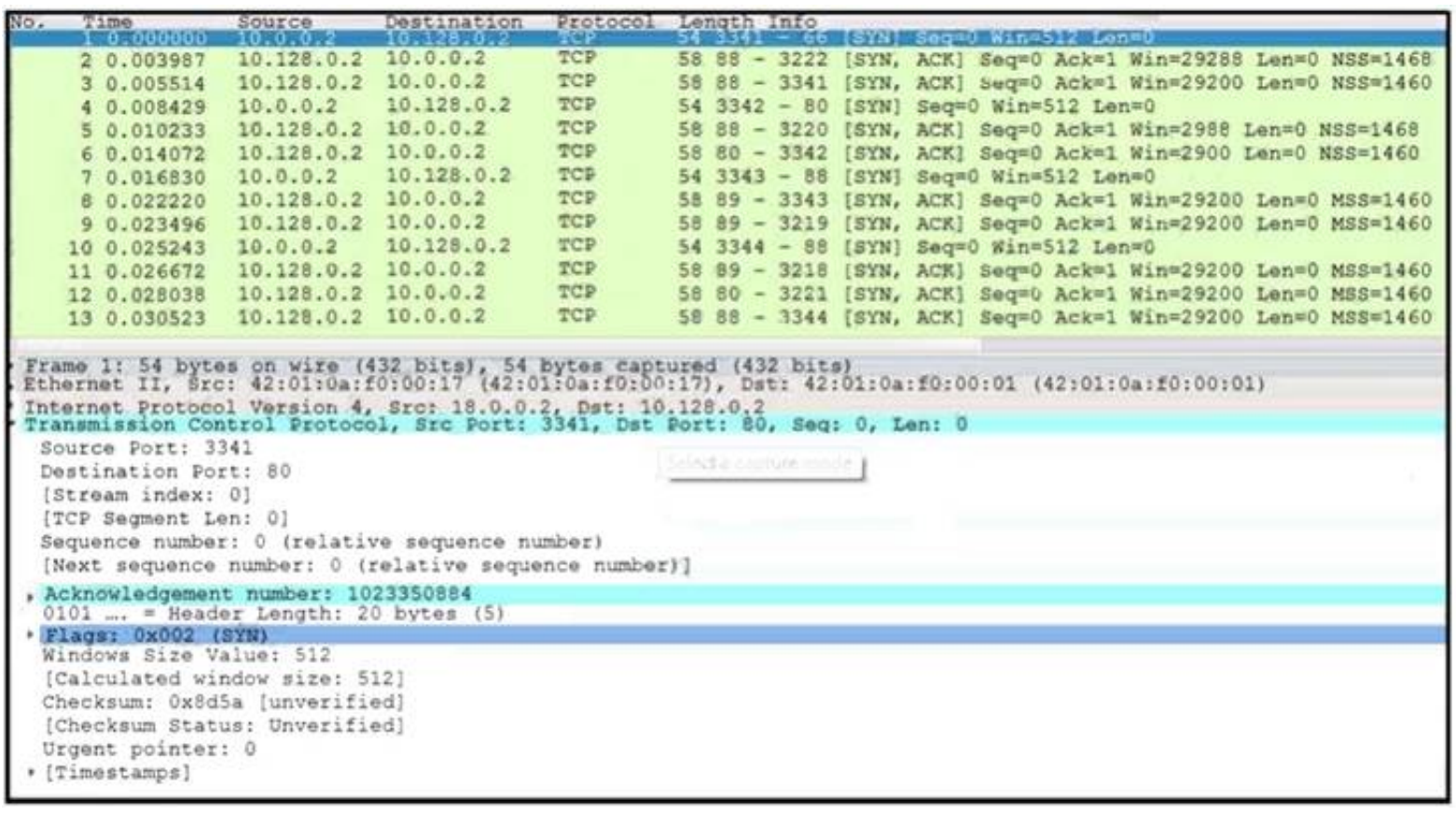
Answer: D

NEW QUESTION 174
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

Answer: B

NEW QUESTION 177
Refer to the exhibit.

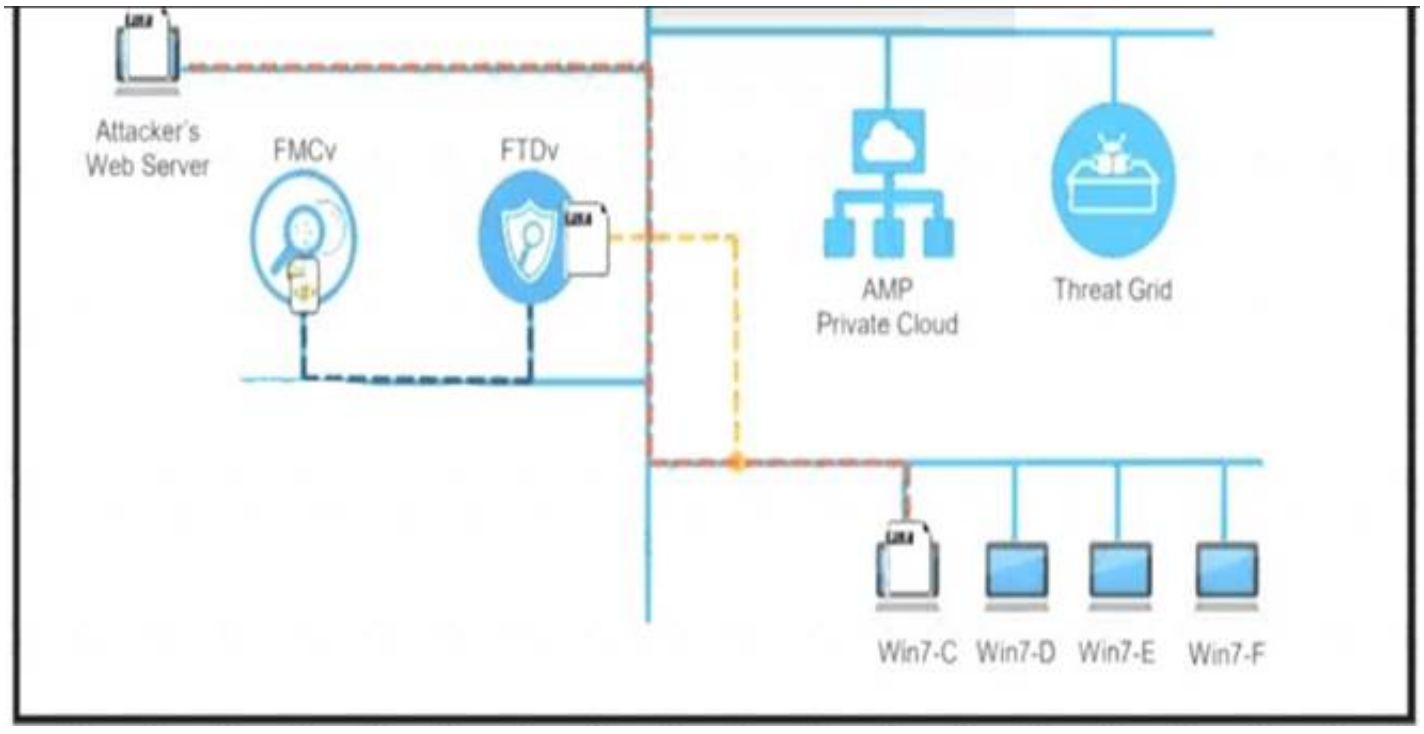


What is occurring in this network traffic?

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

Answer: D

NEW QUESTION 179
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: B

NEW QUESTION 183
Which regular expression matches "color" and "colour"?

A. colo?ur
B. col[08]+our
C. colou?r
D. col[09]+our

Answer: C

NEW QUESTION 188
How does an SSL certificate impact security between the client and the server?

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

Answer: D

NEW QUESTION 190
What are the two characteristics of the full packet captures? (Choose two.)

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

Answer: CE

NEW QUESTION 195
Refer to the exhibit.

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

Which type of log is displayed?

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

Answer: A

Explanation:
You also see the 5-tuple in IPS events, NetFlow records, and other event data. In fact, on the exam you may need to differentiate between a firewall log versus a traditional IPS or IDS event. One of the things to remember is that traditional IDS and IPS use signatures, so an easy way to differentiate is by looking for a signature ID (SigID). If you see a signature ID, then most definitely the event is a traditional IPS or IDS event.

NEW QUESTION 196
What describes the impact of false-positive alerts compared to false-negative alerts?

A. A false negative is alerting for an XSS attac
B. An engineer investigates the alert and discovers that an XSS attack happened A false positive is when an XSS attack happens and no alert is raised
C. A false negative is a legitimate attack triggering a brute-force aler
D. An engineer investigates the alert and finds out someone intended to break into the system A false positive is when no alert and no attack is occurring
E. A false positive is an event alerting for a brute-force attack An engineer investigates the alert and discovers that a legitimate user entered the wrong credential several times A false negative is when a threat actor tries to brute-force attack a system and no alert is raised.
F. A false positive is an event alerting for an SQL injection attack An engineer investigates the alert and discovers that an attack attempt was blocked by IPS A false negative is when the attack gets detected but succeeds and results in a breach.

Answer: C

NEW QUESTION 197
What are the two differences between stateful and deep packet inspection? (Choose two)

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

Answer: AB

NEW QUESTION 201
How is NetFlow different from traffic mirroring?

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

Answer: A

NEW QUESTION 203
What does an attacker use to determine which network ports are listening on a potential target device?

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

Answer: B

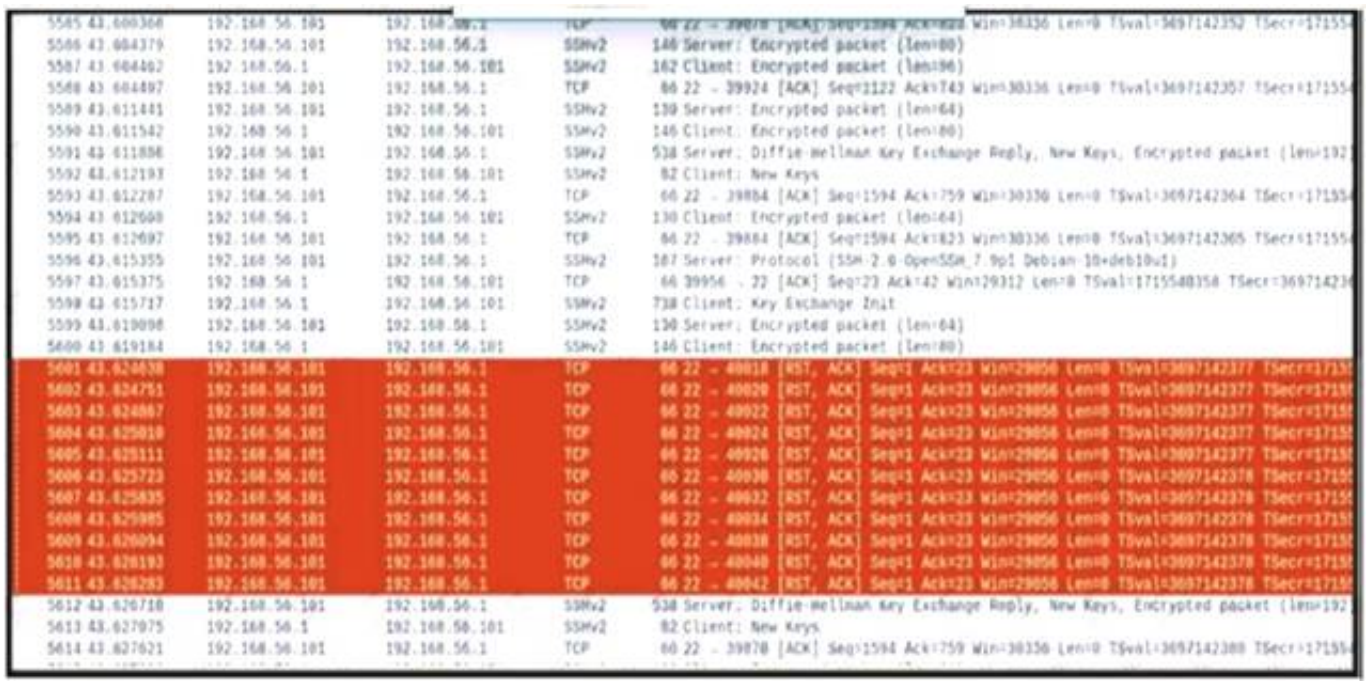
NEW QUESTION 208
What is a difference between tampered and untampered disk images?

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

Answer: D

Explanation:
The disk image must be intact for forensics analysis. As a cybersecurity professional, you may be given the task of capturing an image of a disk in a forensic manner. Imagine a security incident has occurred on a system and you are required to perform some forensic investigation to determine who and what caused the attack. Additionally, you want to ensure the data that was captured is not tampered with or modified during the creation of a disk image process. Ref: Cisco Certified CyberOps Associate 200-201 Certification Guide

NEW QUESTION 212
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

Answer: C

NEW QUESTION 213
Refer to the exhibit.

What is the potential threat identified in this Stealthwatch dashboard?

A. A policy violation is active for host 10.10.101.24.
B. A host on the network is sending a DDoS attack to another inside host.
C. There are three active data exfiltration alerts.
D. A policy violation is active for host 10.201.3.149.

Answer: C

Explanation:
"EX" = exfiltration And there are three.
Also the "suspect long flow" and "suspect data heading" suggest, for example, DNS exfiltration
https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/management_console/smc_users_guide/SW_6 page 177.

NEW QUESTION 214
Refer to the exhibit.

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

What is depicted in the exhibit?

A. Windows Event logs
B. Apache logs

C. IIS logs
D. UNIX-based syslog

Answer: B

NEW QUESTION 218
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.

Answer: C

NEW QUESTION 222
What is the difference between statistical detection and rule-based detection models?

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

Answer: B

NEW QUESTION 227
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

Answer: B

NEW QUESTION 232
A security expert is working on a copy of the evidence, an ISO file that is saved in CDFS format. Which type of evidence is this file?

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

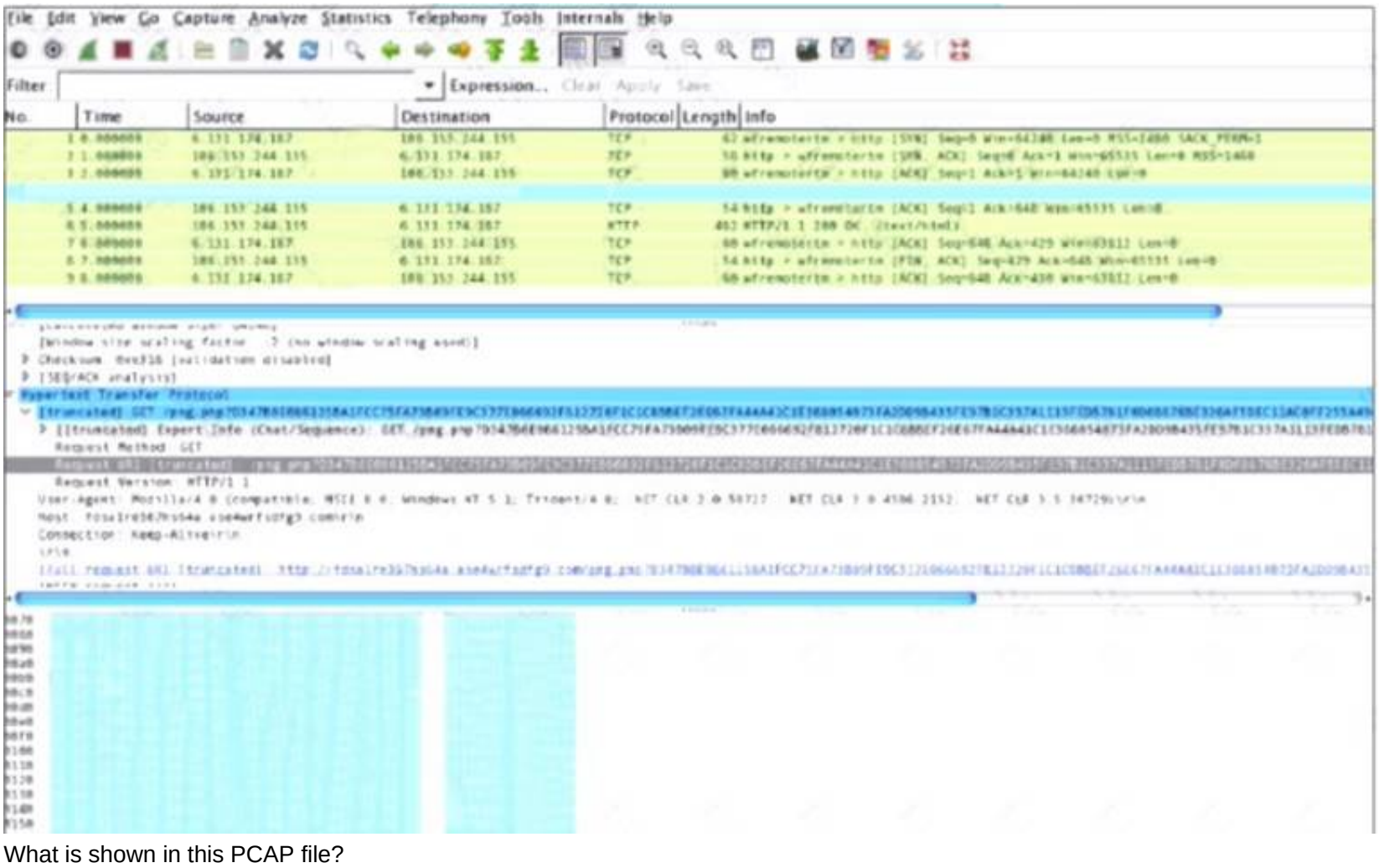
Answer: A

NEW QUESTION 233
What is the relationship between a vulnerability and a threat?

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

Answer: A

NEW QUESTION 234
Refer to the exhibit.



What is shown in this PCAP file?

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

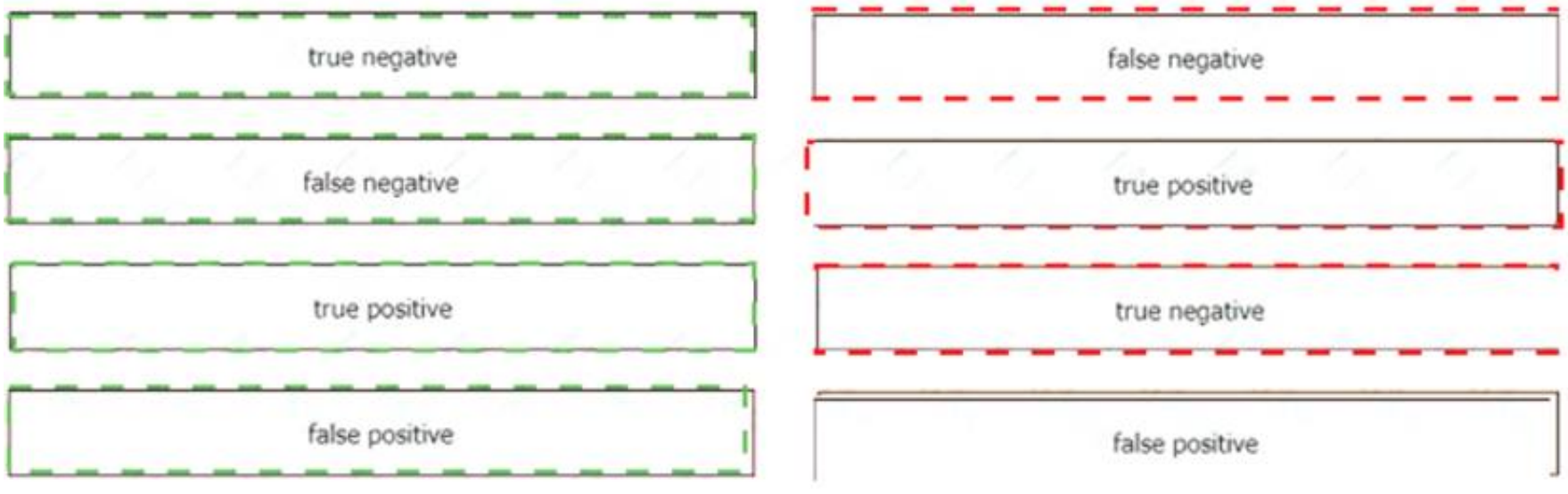
Answer: D

NEW QUESTION 235
Drag and drop the event term from the left onto the description on the right.

A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 240
Which type of attack occurs when an attacker is successful in eavesdropping on a conversation between two IP phones?

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

Answer: D

NEW QUESTION 241
A user received a malicious attachment but did not run it. Which category classifies the intrusion?

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

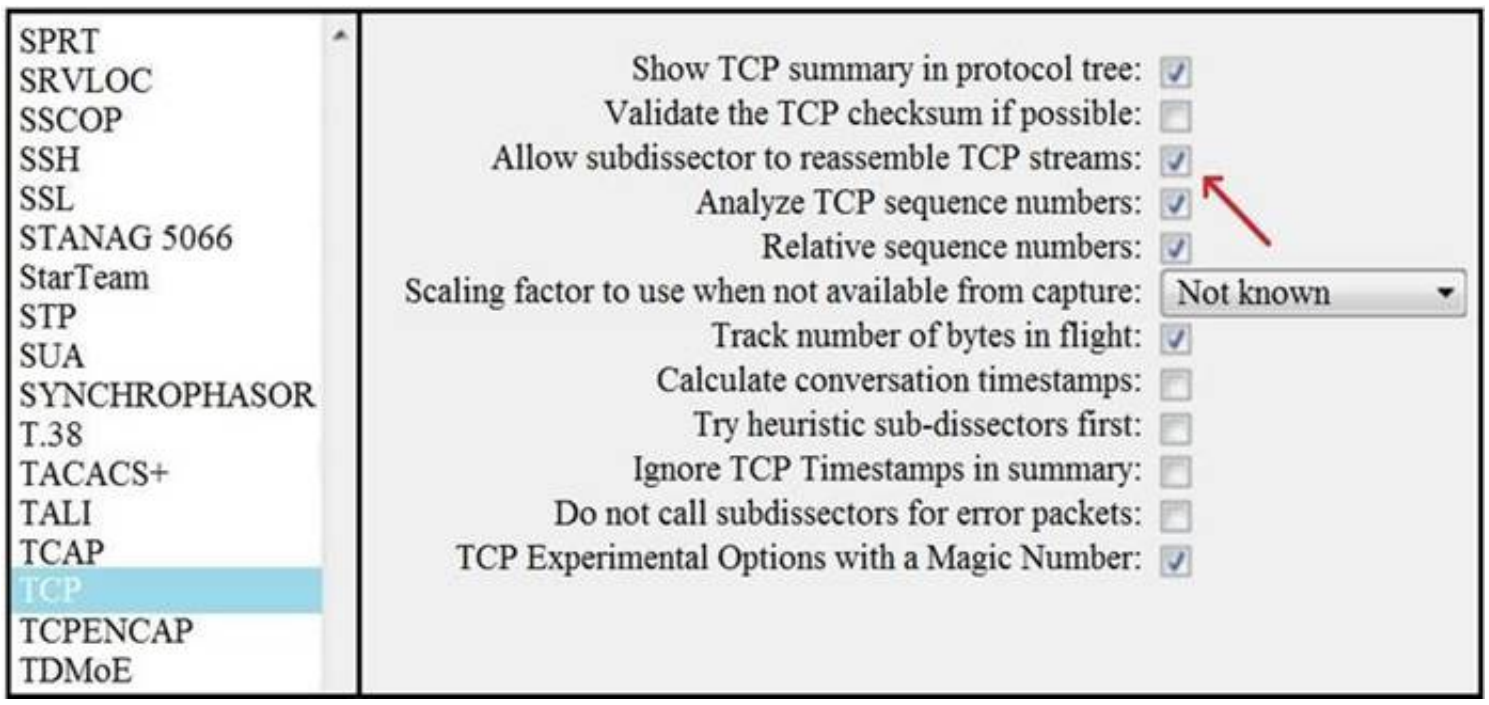
Answer: D

NEW QUESTION 245
How is attacking a vulnerability categorized?

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

Answer: C

NEW QUESTION 248
Refer to the exhibit.



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

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

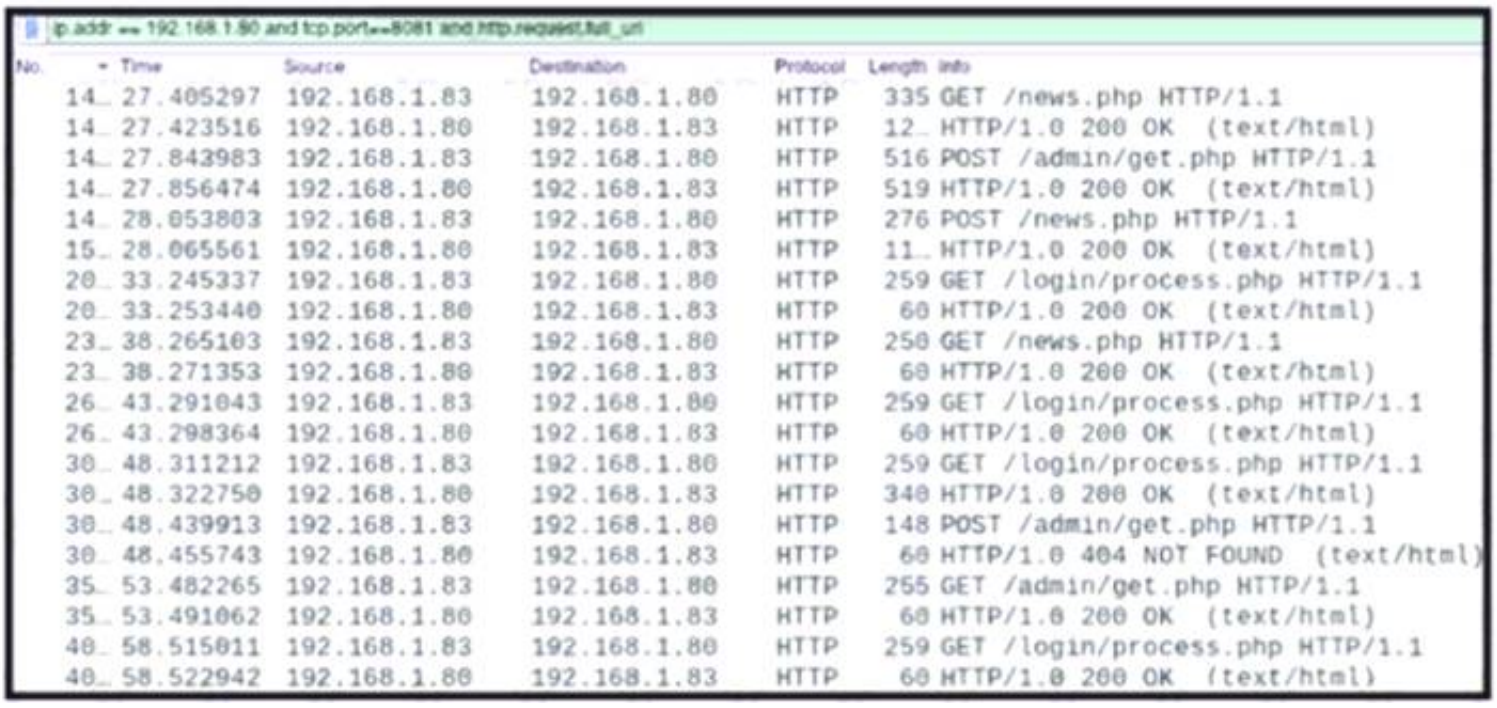
Answer: D

NEW QUESTION 252
Which security technology guarantees the integrity and authenticity of all messages transferred to and from a web application?

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

Answer: B

NEW QUESTION 255
Refer to the exhibit.



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

NEW QUESTION 258
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

Answer: B

NEW QUESTION 262
Refer to the exhibit.

```
Mar 07 2020 16:16:48: %ASA-4-106023: Deny tcp src
outside:10.22.219.221/54602 dst outside:10.22.250.212/504
by access-group "outside" [0x0, 0x0]
```

Which technology generates this log?

A. NetFlow
B. IDS
C. web proxy
D. firewall

Answer: D

NEW QUESTION 267
A developer is working on a project using a Linux tool that enables writing processes to obtain these required results:

- If the process is unsuccessful, a negative value is returned.
- If the process is successful, 0 value is returned to the child process, and the process ID is sent to the parent process.

Which component results from this operation?

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

Answer: D

Explanation:
There are two tasks with specially distinguished process IDs: swapper or sched has process ID 0 and is responsible for paging, and is actually part of the kernel rather than a normal user-mode process. Process ID 1 is usually the init process primarily responsible for starting and shutting down the system. Originally, process ID 1 was not specifically reserved for init by any technical measures: it simply had this ID as a natural consequence of being the first process invoked by the kernel. More recent Unix systems typically have additional kernel components visible as 'processes', in which case PID 1 is actively reserved for the init process to maintain consistency with older systems

NEW QUESTION 270
An employee received an email from a colleague's address asking for the password for the domain controller. The employee noticed a missing letter within the sender's address. What does this incident describe?

A. brute-force attack
B. insider attack
C. shoulder surfing
D. social engineering

Answer: B

NEW QUESTION 272
What is the difference between the rule-based detection when compared to behavioral detection?

A. Rule-Based detection is searching for patterns linked to specific types of attacks, while behavioral is identifying per signature.
B. Rule-Based systems have established patterns that do not change with new data, while behavioral changes.
C. Behavioral systems are predefined patterns from hundreds of users, while Rule-Based only flags potentially abnormal patterns using signatures.
D. Behavioral systems find sequences that match a particular attack signature, while Rule-Based identifies potential attacks.

Answer: D

NEW QUESTION 276
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

200-201 Practice Exam Features:

* 200-201 Questions and Answers Updated Frequently

* 200-201 Practice Questions Verified by Expert Senior Certified Staff

* 200-201 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* 200-201 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year