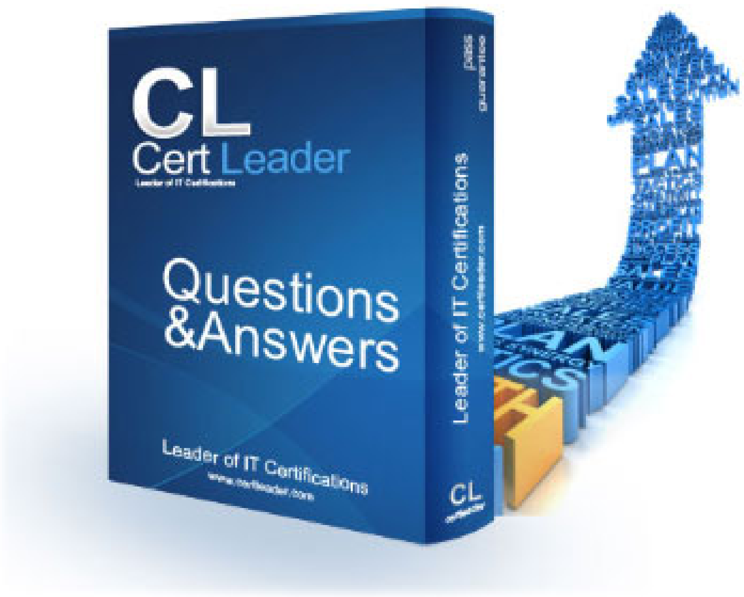
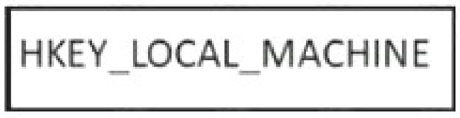
200-201 Dumps

Understanding Cisco Cybersecurity Operations Fundamentals

https://www.certleader.com/200-201-dumps.html



NEW QUESTION 1
Refer to the exhibit.



```
HKEY_LOCAL_MACHINE
```

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 2
What causes events on a Windows system to show Event Code 4625 in the log messages?

A. The system detected an XSS attack
B. Someone is trying a brute force attack on the network
C. Another device is gaining root access to the system
D. A privileged user successfully logged into the system

Answer: B

NEW QUESTION 3
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 4
An analyst received a ticket regarding a degraded processing capability for one of the HR department's servers. On the same day, an engineer noticed a disabled antivirus software and was not able to determine when or why it occurred. According to the NIST Incident Handling Guide, what is the next phase of this investigation?

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

Answer: B

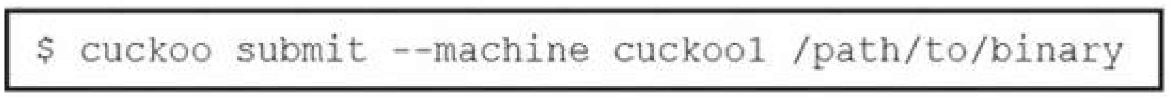
NEW QUESTION 5
What is a difference between inline traffic interrogation and traffic mirroring?

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
Refer to the exhibit.



```
$ cuckoo submit --machine cuckoo1 /path/to/binary
```

Which event is occurring?

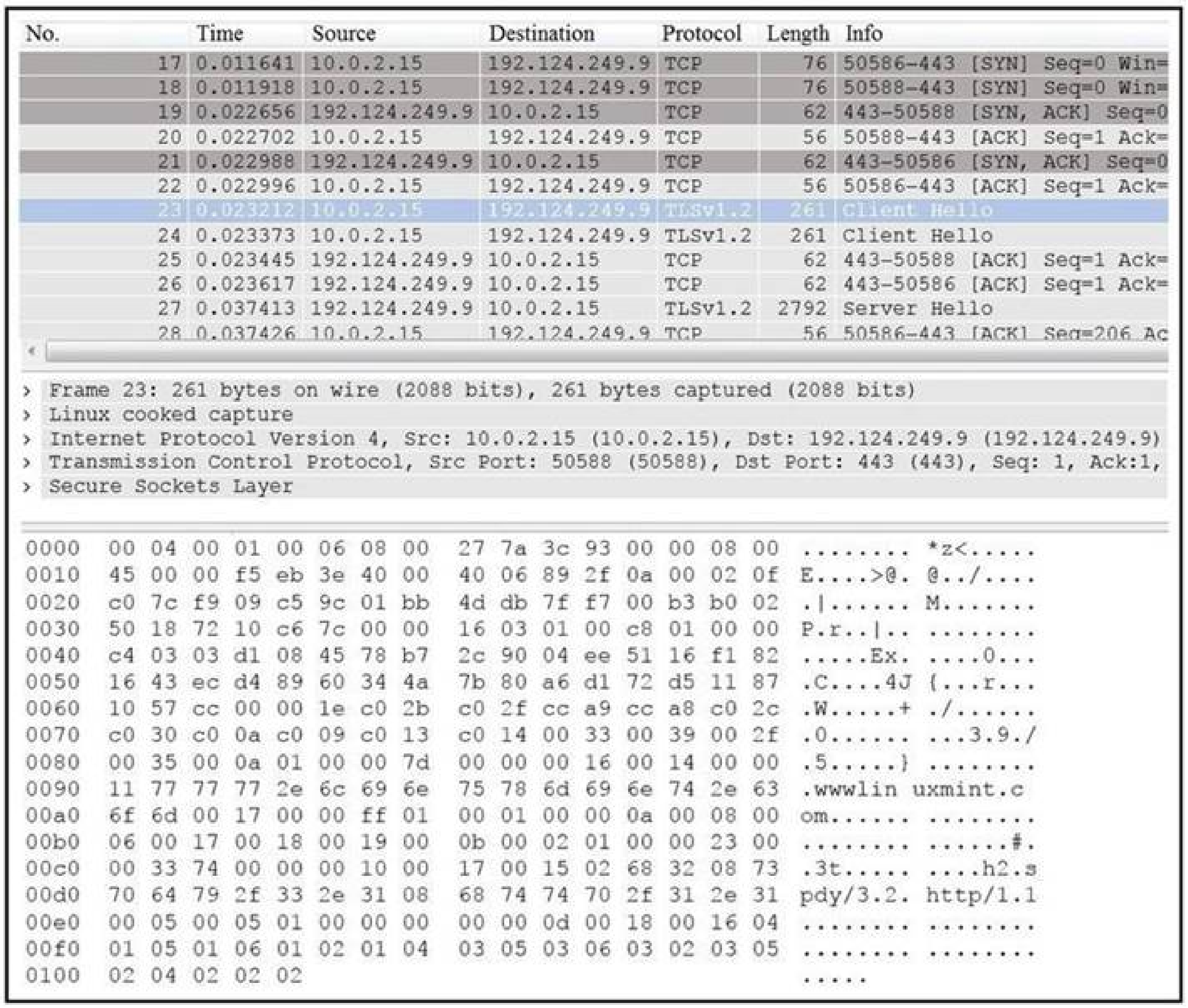
A. A binary named "submit" is running on VM cuckoo1.

B. A binary is being submitted to run on VM cuckoo1
C. A binary on VM cuckoo1 is being submitted for evaluation
D. A URL is being evaluated to see if it has a malicious binary

Answer: B

Explanation:
https://cuckoo.readthedocs.io/en/latest/usage/submit/

NEW QUESTION 7
Refer to the exhibit.

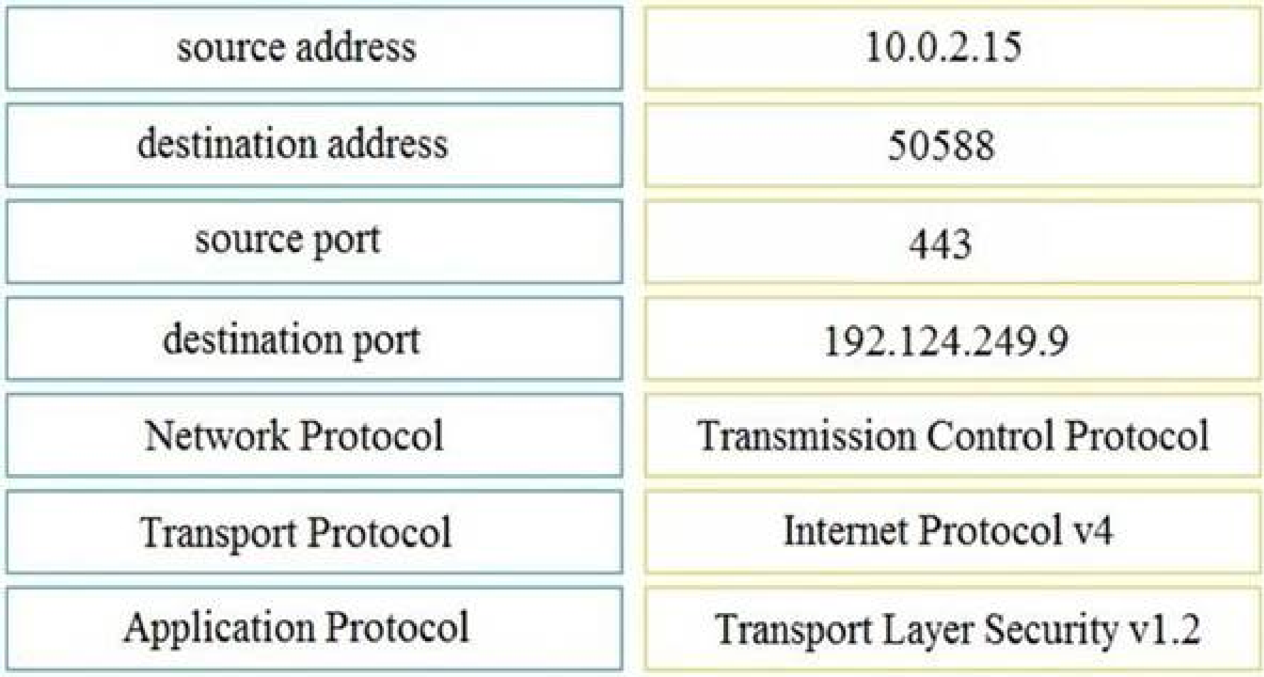


```
No.      Time      Source          Destination     Protocol Length Info
      17 0.011641 10.0.2.15       192.124.249.9   TCP          76 50586-443 [SYN] Seq=0 Win=
      18 0.011918 10.0.2.15       192.124.249.9   TCP          76 50588-443 [SYN] Seq=0 Win=
      19 0.022656 192.124.249.9   10.0.2.15       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  .wwwlin uxmint.c
00a0  6f 6d 00 17 00 00 ff 01  00 01 00 00 0a 00 08 00  om...... ........
00b0  06 00 17 00 18 00 19 00  0b 00 02 01 00 00 23 00  ........ ......#.
00c0  00 33 74 00 00 00 10 00  17 00 15 02 68 32 08 73  .3t..... ....h2.s
00d0  70 64 79 2f 33 2e 31 08  68 74 74 70 2f 31 2e 31  pdy/3.2. http/1.1
00e0  00 05 00 05 01 00 00 00  00 00 0d 00 18 00 16 04  ........ ........
00f0  01 05 01 06 01 02 01 04  03 05 03 06 03 02 03 05  ........ ........
0100  02 04 02 02 02                                    .....
```

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

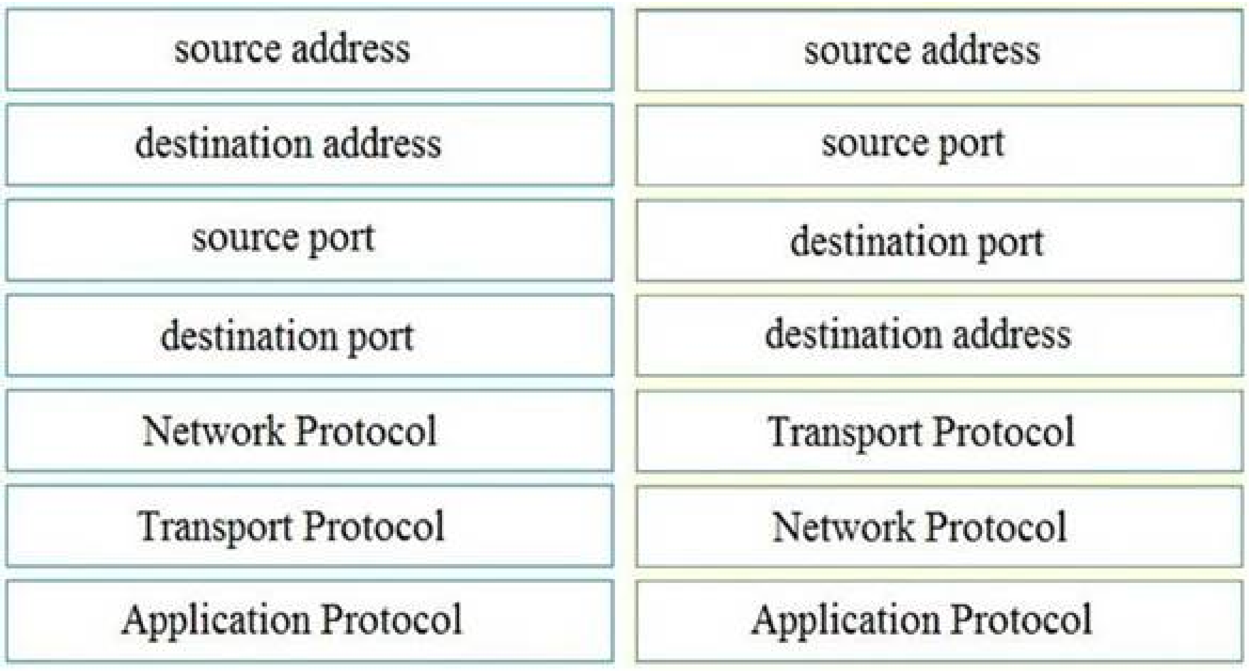


source address	10.0.2.15
destination address	50588
source port	443
destination port	192.124.249.9
Network Protocol	Transmission Control Protocol
Transport Protocol	Internet Protocol v4
Application Protocol	Transport Layer Security v1.2

A. Mastered
B. Not Mastered

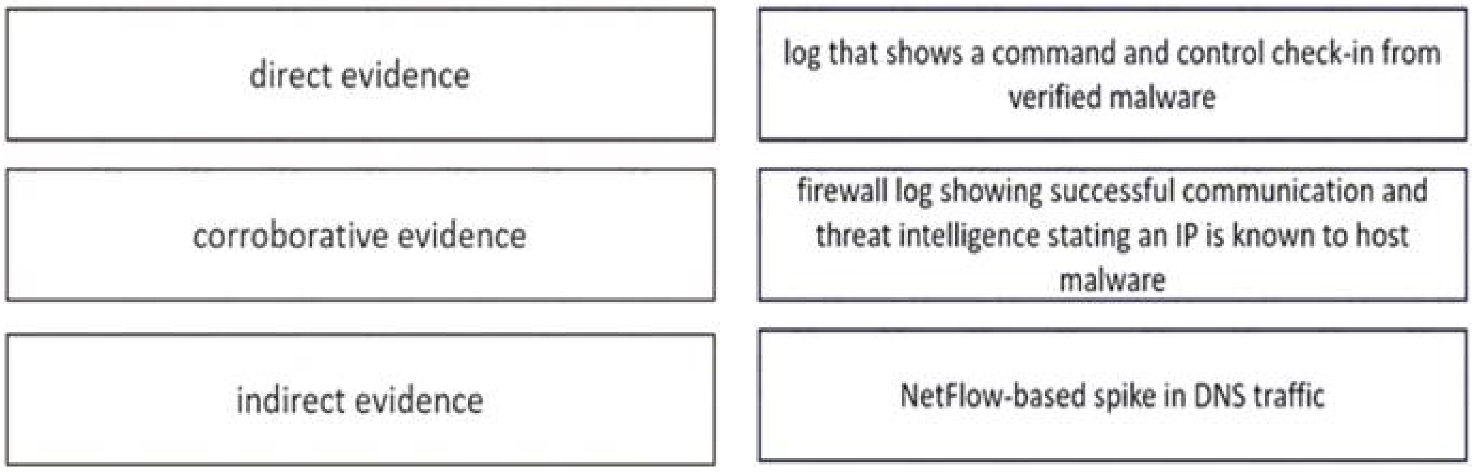
Answer: A

Explanation:



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

NEW QUESTION 8
Drag and drop the type of evidence from the left onto the description of that evidence on the right.



direct evidence	log that shows a command and control check-in from verified malware
corroborative evidence	firewall log showing successful communication and threat intelligence stating an IP is known to host malware
indirect evidence	NetFlow-based spike in DNS traffic

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, application Description automatically generated

NEW QUESTION 9
A system administrator is ensuring that specific registry information is accurate.
Which type of configuration information does the HKEY_LOCAL_MACHINE hive contain?

A. file extension associations
B. hardware, software, and security settings for the system
C. currently logged in users, including folders and control panel settings
D. all users on the system, including visual settings

Answer: B

Explanation:
https://docs.microsoft.com/en-us/troubleshoot/windows-server/performance/windows-registry-advanced-users

NEW QUESTION 10
What describes a buffer overflow attack?

A. injecting new commands into existing buffers
B. fetching data from memory buffer registers
C. overloading a predefined amount of memory
D. suppressing the buffers in a process

Answer: C

NEW QUESTION 10
A company is using several network applications that require high availability and responsiveness, such that milliseconds of latency on network traffic is not acceptable. An engineer needs to analyze the network and identify ways to improve traffic movement to minimize delays. Which information must the engineer obtain for this analysis?

A. total throughput on the interface of the router and NetFlow records
B. output of routing protocol authentication failures and ports used
C. running processes on the applications and their total network usage

D. deep packet captures of each application flow and duration

Answer: C

NEW QUESTION 14
Which action should be taken if the system is overwhelmed with alerts when false positives and false negatives are compared?

A. Modify the settings of the intrusion detection system.
B. Design criteria for reviewing alerts.
C. Redefine signature rules.
D. Adjust the alerts schedule.

Answer: A

Explanation:
Traditional intrusion detection system (IDS) and intrusion prevention system (IPS) devices need to be tuned to avoid false positives and false negatives. Next-generation IPSs do not need the same level of tuning compared to traditional IPSs. Also, you can obtain much deeper reports and functionality, including advanced malware protection and retrospective analysis to see what happened after an attack took place. Ref: Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide

NEW 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.

Answer: A

NEW QUESTION 20
What is the impact of false positive alerts on business compared to true positive?

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

Answer: C

NEW QUESTION 22
Which artifact is used to uniquely identify a detected file?

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

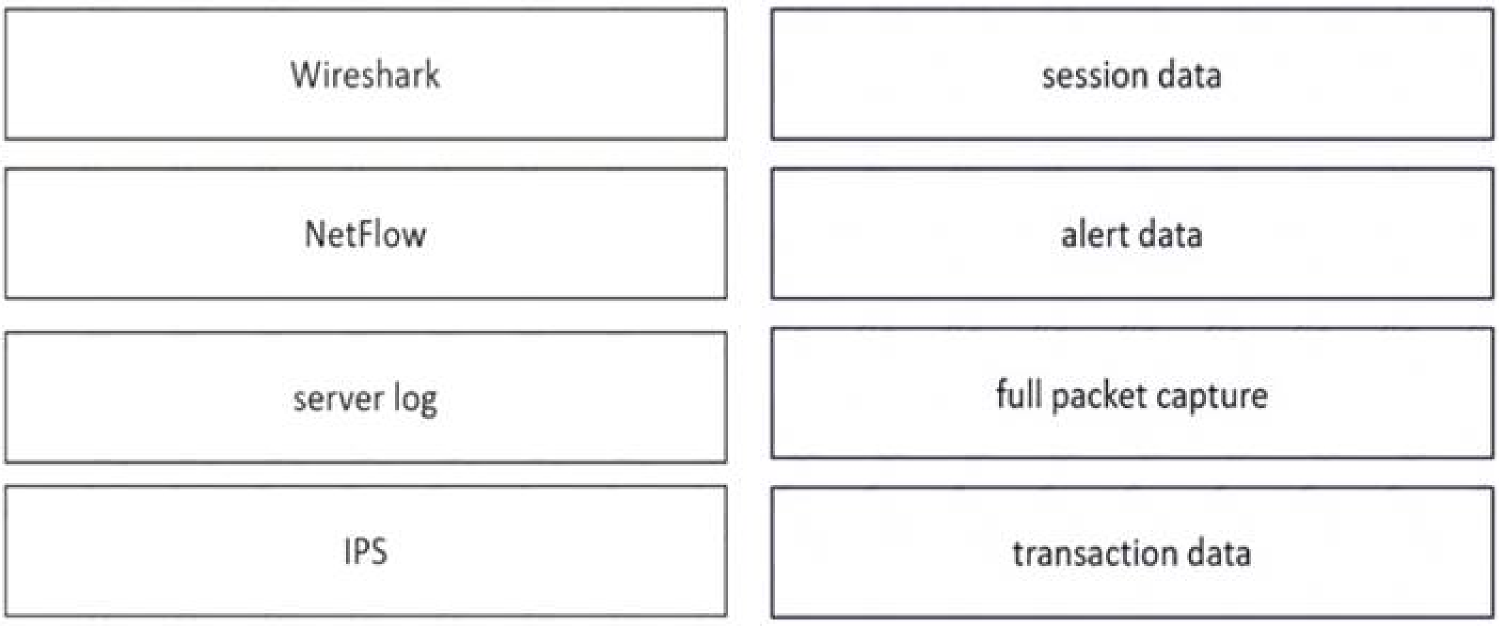
Answer: D

NEW QUESTION 27
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 30
Drag and drop the data source from the left onto the data type on the right.

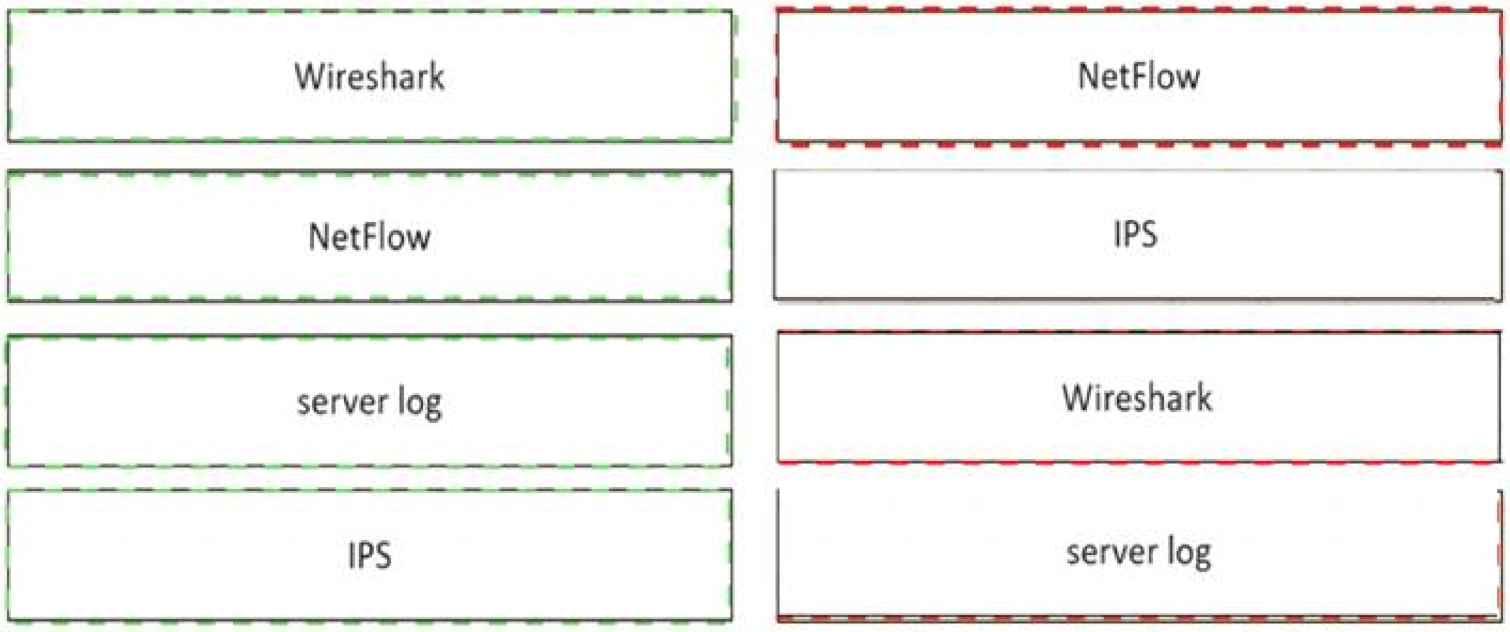


Wireshark	session data
NetFlow	alert data
server log	full packet capture
IPS	transaction data

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Wireshark	NetFlow
NetFlow	IPS
server log	Wireshark
IPS	server log

NEW QUESTION 34
An engineer is investigating a case of the unauthorized usage of the “Tcpdump” tool. The analysis revealed that a malicious insider attempted to sniff traffic on a specific interface. What type of information did the malicious insider attempt to obtain?

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

Answer: C

NEW QUESTION 39
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

Answer: B

NEW QUESTION 41
One of the objectives of information security is to protect the CIA of information and systems. What does CIA mean in this context?

A. confidentiality, identity, and authorization
B. confidentiality, integrity, and authorization
C. confidentiality, identity, and availability
D. confidentiality, integrity, and availability

Answer: D

NEW QUESTION 45

What does cyber attribution identify in an investigation?

A. cause of an attack
B. exploit of an attack
C. vulnerabilities exploited
D. threat actors of an attack

Answer: D

Explanation:
https://www.techtarget.com/searchsecurity/definition/cyber-attribution

NEW QUESTION 48
Which security principle is violated by running all processes as root or administrator?

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

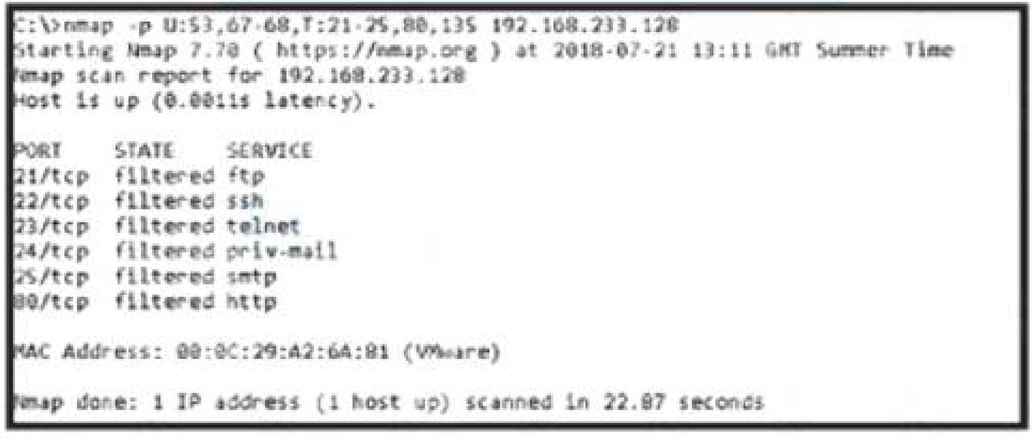
Answer: A

NEW QUESTION 51
Which evasion technique is a function of ransomware?

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

Answer: B

NEW QUESTION 53
Refer to the exhibit.



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

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

MAC Address: 00:0C:29:A2:6A:81 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 22.87 seconds
```

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

A. Identified a firewall device preventing the 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 57
What is the practice of giving employees only those permissions necessary to perform their specific role within an organization?

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

Answer: A

NEW QUESTION 61
Which process is used when IPS events are removed to improve data integrity?

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

Answer: B

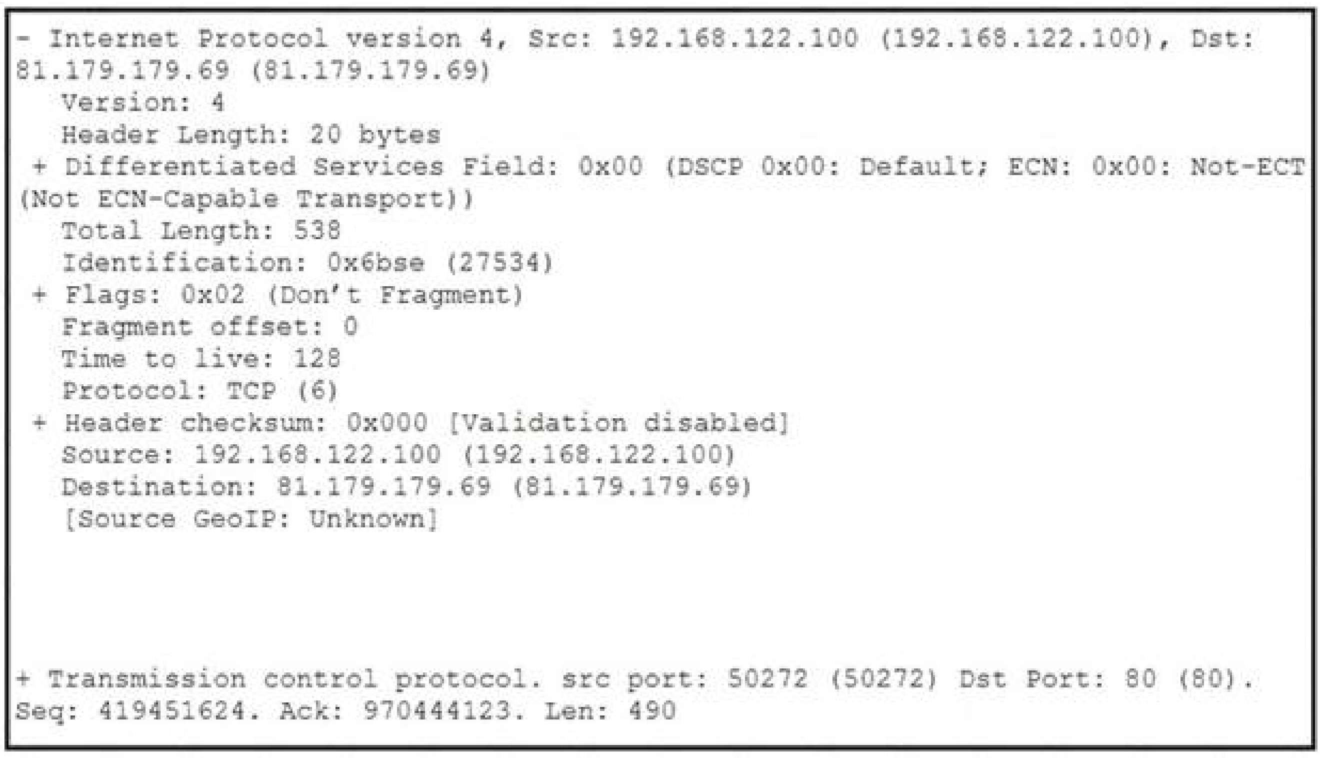
NEW QUESTION 63

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

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

Answer: B

NEW QUESTION 66
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 68
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 70
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

Answer: B

NEW QUESTION 72
At which layer is deep packet inspection investigated on a firewall?

A. internet
B. transport
C. application
D. data link

Answer: C

Explanation:
Deep packet inspection is a form of packet filtering usually carried out as a function of your firewall. It is applied at the Open Systems Interconnection's application layer. Deep packet inspection evaluates the contents of a packet that is going through a checkpoint.

NEW QUESTION 76

Which system monitors local system operation and local network access for violations of a security policy?

A. host-based intrusion detection
B. systems-based sandboxing
C. host-based firewall
D. antivirus

Answer: A

Explanation:
HIDS is capable of monitoring the internals of a computing system as well as the network packets on its network interfaces. Host-based firewall is a piece of software running on a single Host that can restrict incoming and outgoing Network activity for that host only.

NEW QUESTION 77
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 79
An engineer is analyzing a recent breach where confidential documents were altered and stolen by the receptionist Further analysis shows that the threat actor connected an externa USB device to bypass security restrictions and steal data The engineer could not find an external USB device Which piece of information must an engineer use for attribution in an investigation?

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

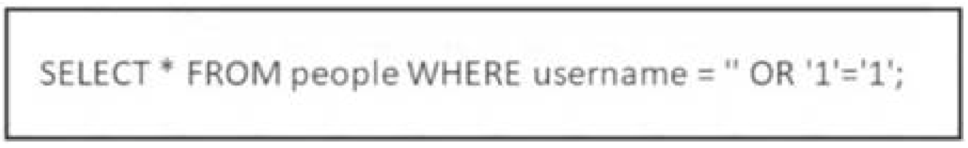
Answer: C

NEW QUESTION 84
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.

Answer: C

NEW QUESTION 86
Refer to the exhibit.



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

Which type of attack is being executed?

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

Answer: A

NEW QUESTION 90
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

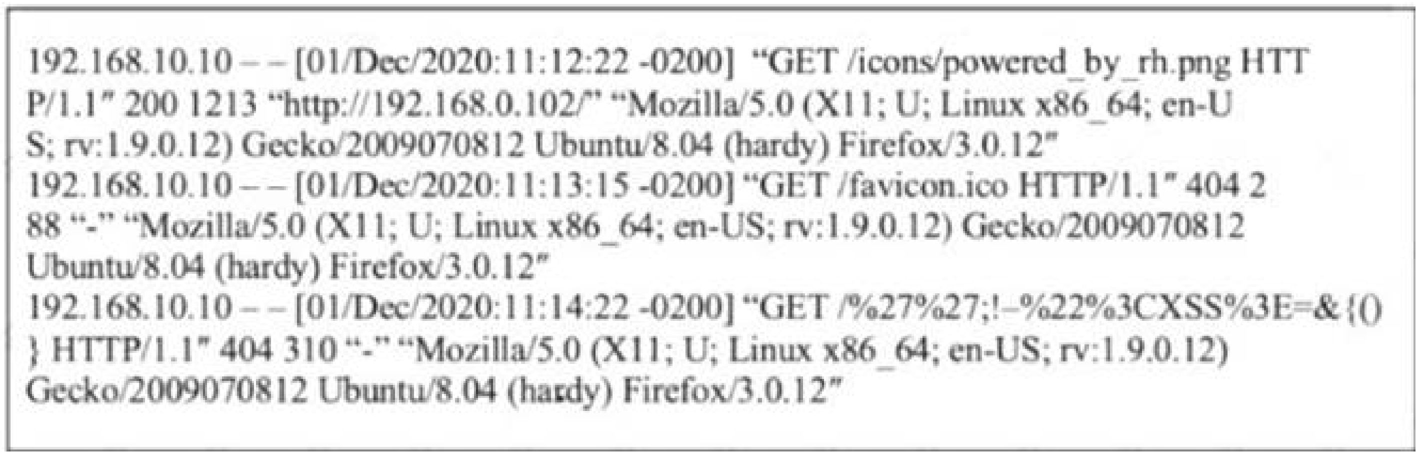
NEW QUESTION 92
Which are two denial-of-service attacks? (Choose two.)

A. TCP connections

B. ping of death
C. man-in-the-middle
D. code-red
E. UDP flooding

Answer: BE

NEW QUESTION 97
Refer to the exhibit.



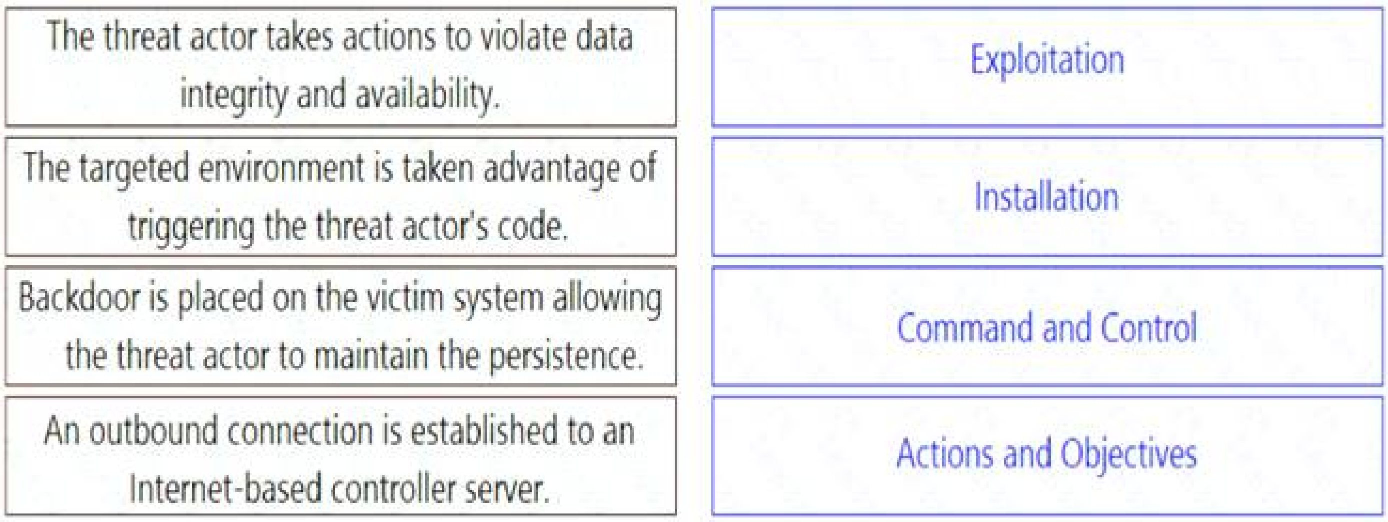
```
192.168.10.10 – – [01/Dec/2020:11:12:22 -0200]  "GET /icons/powered_by_rh.png HTT
P/1.1" 200 1213 "http://192.168.0.102/" "Mozilla/5.0 (X11; U; Linux x86_64; en-U
S; rv:1.9.0.12) Gecko/2009070812 Ubuntu/8.04 (hardy) Firefox/3.0.12"
192.168.10.10 – – [01/Dec/2020:11:13:15 -0200] "GET /favicon.ico 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 98
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.



The threat actor takes actions to violate data integrity and availability.	Exploitation
The targeted environment is taken advantage of triggering the threat actor's code.	Installation
Backdoor is placed on the victim system allowing the threat actor to maintain the persistence.	Command and Control
An outbound connection is established to an Internet-based controller server.	Actions and Objectives

A. Mastered
B. Not Mastered

Answer: A

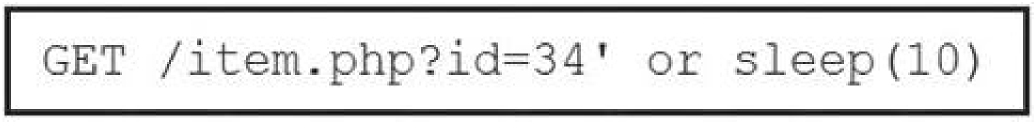
Explanation:
Exploitation - The targeted Environment is taken advantage of triggering the threat actor's code Installation - Backdoor is placed on the victim system allowing the threat actor to maintain the persistence. Command and Control - An outbound connection is established to an Internet-based controller server. Actions and Objectives - The threat actor takes actions to violate data integrity and availability

NEW QUESTION 100
What is the difference between inline traffic interrogation (TAPS) and traffic mirroring (SPAN)?

A. TAPS interrogation is more complex because traffic mirroring applies additional tags to data and SPAN does not alter integrity and provides full duplex network.
B. SPAN results in more efficient traffic analysis, and TAPS is considerably slower due to latency caused by mirroring.
C. TAPS replicates the traffic to preserve integrity, and SPAN modifies packets before sending them to other analysis tools
D. SPAN ports filter out physical layer errors, making some types of analyses more difficult, and TAPS receives all packets, including physical errors.

Answer: D

NEW QUESTION 105
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 110
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 114
What is a sandbox interprocess communication service?

A. A collection of rules within the sandbox that prevent the communication between sandboxes.
B. A collection of network services that are activated on an interface, allowing for inter-port communication.
C. A collection of interfaces that allow for coordination of activities among processes.
D. A collection of host services that allow for communication between sandboxes.

Answer: C

Explanation:
Inter-process communication (IPC) allows communication between different processes. A process is one or more threads running inside its own, isolated address space. https://docs.legato.io/16_10/basicIPC.html

NEW QUESTION 119
An engineer needs to discover alive hosts within the 192.168.1.0/24 range without triggering intrusive portscan alerts on the IDS device using Nmap. Which command will accomplish this goal?

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

Answer: B

Explanation:
https://explainshell.com/explain?cmd=nmap+-sP

NEW QUESTION 124
Which attack is the network vulnerable to when a stream cipher like RC4 is used twice with the same key?

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

Answer: C

NEW QUESTION 128
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

Answer: C

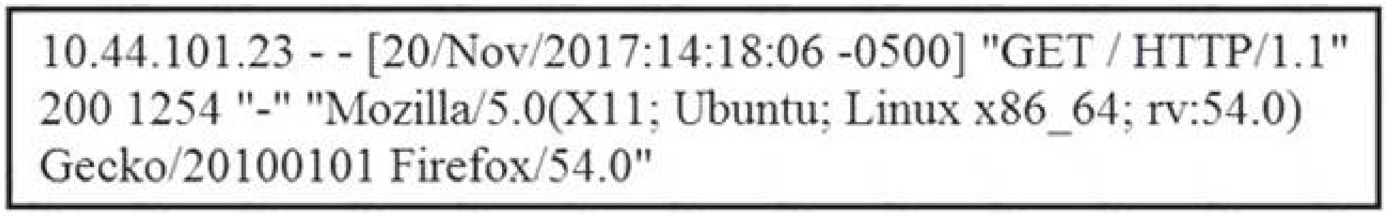
NEW QUESTION 129
Which technology on a host is used to isolate a running application from other applications?

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

Answer: A

NEW QUESTION 134

Refer to the exhibit.



```
10.44.101.23 - - [20/Nov/2017:14:18:06 -0500] "GET / HTTP/1.1"
200 1254 "-" "Mozilla/5.0(X11; Ubuntu; Linux x86_64; rv:54.0)
Gecko/20100101 Firefox/54.0"
```

What does the message indicate?

A. an access attempt was made from the Mosaic web browser
B. a successful access attempt was made to retrieve the password file
C. a successful access attempt was made to retrieve the root of the website
D. a denied access attempt was made to retrieve the password file

Answer: C

NEW QUESTION 136
What is obtained using NetFlow?

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

Answer: A

NEW QUESTION 137
What is the difference between a threat and a risk?

A. Threat represents a potential danger that could take advantage of a weakness in a system
B. Risk represents the known and identified loss or danger in the system
C. Risk represents the nonintentional interaction with uncertainty in the system
D. Threat represents a state of being exposed to an attack or a compromise, either physically or logically.

Answer: A

Explanation:
A threat 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.

NEW QUESTION 142
When trying to evade IDS/IPS devices, which mechanism allows the user to make the data incomprehensible without a specific key, certificate, or password?

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

Answer: C

Explanation:
https://techdifferences.com/difference-between-steganography-and-cryptography.html#:~:text=The%20steganog

NEW QUESTION 147
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 149
What is an attack surface as compared to a vulnerability?

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

Answer: C

Explanation:
An attack surface is the total sum of vulnerabilities that can be exploited to carry out a security attack. Attack surfaces can be physical or digital. The term attack surface is often confused with the term attack vector, but they are not the same thing. The surface is what is being attacked; the vector is the means by which an

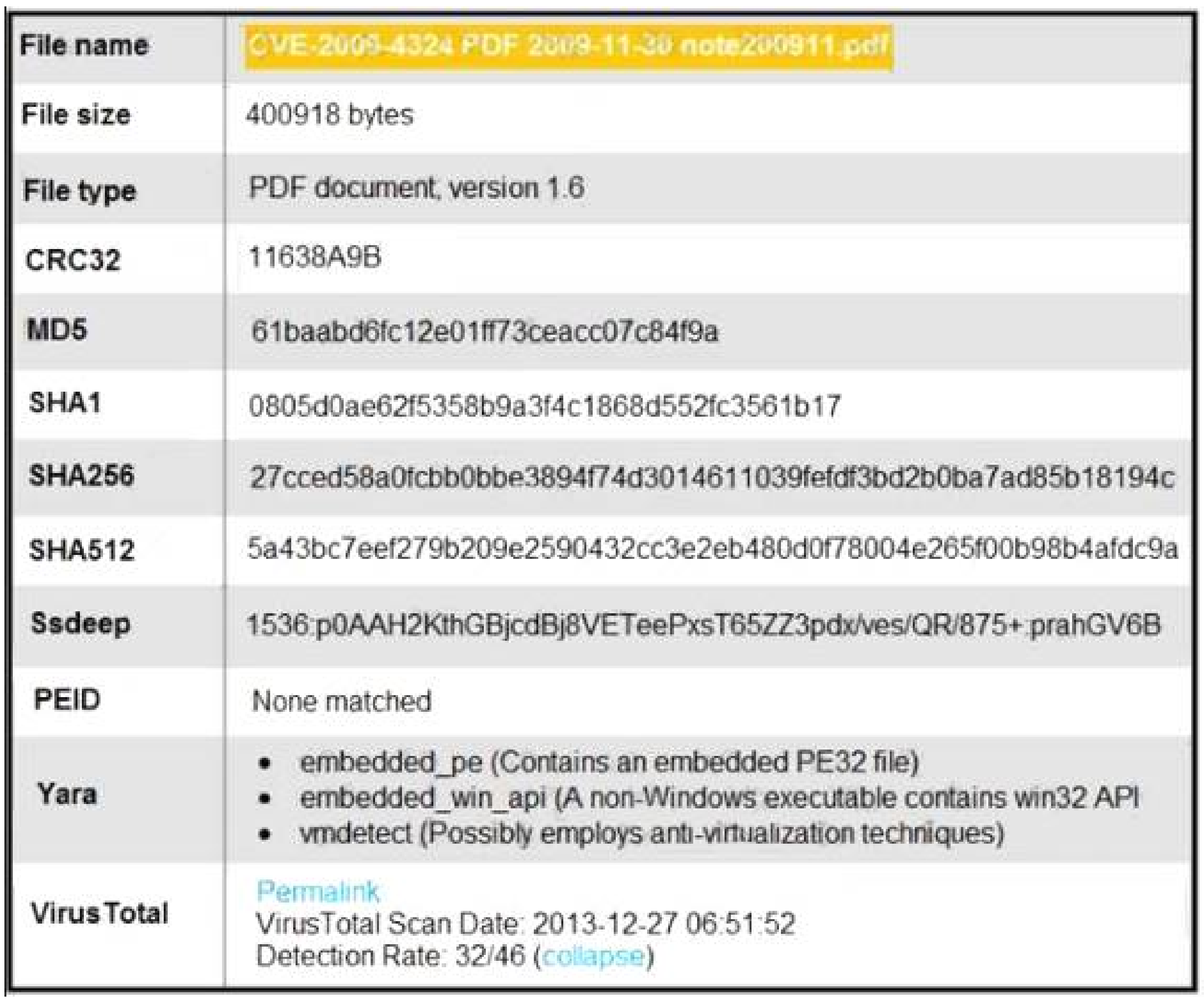
intruder gains access.

NEW QUESTION 154
Which metric in CVSS indicates an attack that takes a destination bank account number and replaces it with a different bank account number?

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

Answer: A

NEW QUESTION 155
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.

Answer: C

NEW QUESTION 158
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 159
What is the virtual address space for a Windows process?

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

Answer: D

NEW QUESTION 160
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 165
Which security principle requires more than one person is required to perform a critical task?

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

Answer: C

NEW QUESTION 169
What is the difference between deep packet inspection and stateful inspection?

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

Answer: D

NEW QUESTION 171
A security incident occurred with the potential of impacting business services. Who performs the attack?

A. malware author
B. threat actor
C. bug bounty hunter
D. direct competitor

Answer: B

NEW QUESTION 174
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

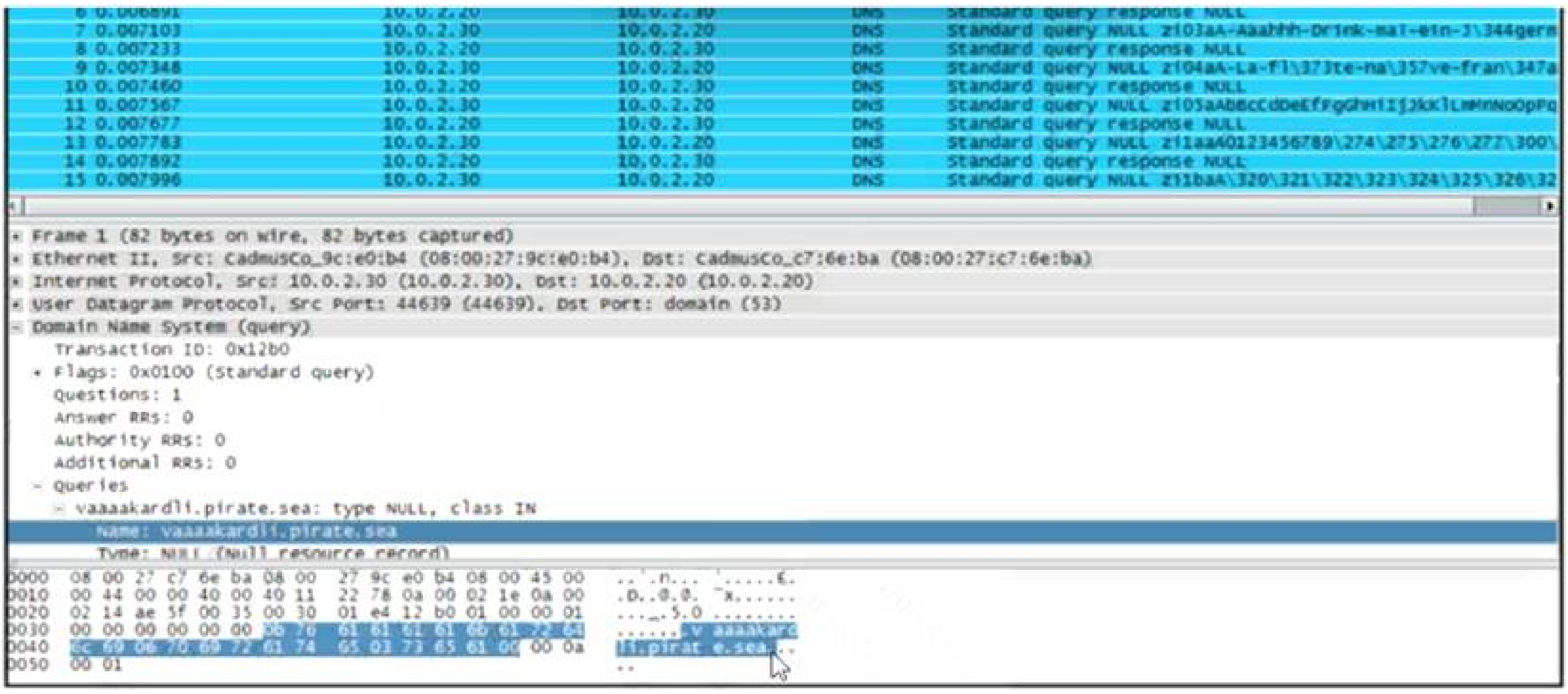
Answer: B

NEW QUESTION 178
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 179
Refer to the exhibit.



```
  6 0.006891   10.0.2.20   10.0.2.30   DNS   Standard query response NULL
  7 0.007103   10.0.2.30   10.0.2.20   DNS   Standard query NULL z103aA-Aaahhh-Drink-mal-ein-J\344germ
  8 0.007233   10.0.2.20   10.0.2.30   DNS   Standard query response NULL
  9 0.007348   10.0.2.30   10.0.2.20   DNS   Standard query NULL z104aA-La-fl\373te-na\357ve-fran\347a
 10 0.007460   10.0.2.20   10.0.2.30   DNS   Standard query response NULL
 11 0.007567   10.0.2.30   10.0.2.20   DNS   Standard query NULL z105aAbBcCdDeEfFgGhHiIjJkKlLmMnNoOpPq
 12 0.007677   10.0.2.20   10.0.2.30   DNS   Standard query response NULL
 13 0.007783   10.0.2.30   10.0.2.20   DNS   Standard query NULL z11aa40123456789\274\275\276\277\300\
 14 0.007892   10.0.2.20   10.0.2.30   DNS   Standard query response NULL
 15 0.007996   10.0.2.30   10.0.2.20   DNS   Standard query NULL z11baA\320\321\322\323\324\325\326\32

+ Frame 1 (82 bytes on wire, 82 bytes captured)
+ Ethernet II, Src: CadmusCo_9c:e0:b4 (08:00:27:9c:e0:b4), Dst: CadmusCo_c7:6e:ba (08:00:27:c7:6e:ba)
+ Internet Protocol, Src: 10.0.2.30 (10.0.2.30), Dst: 10.0.2.20 (10.0.2.20)
+ User Datagram Protocol, Src Port: 44639 (44639), Dst Port: domain (53)
- Domain Name System (query)
    Transaction ID: 0x12b0
  + Flags: 0x0100 (Standard query)
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  - Queries
    - vaaaakardli.pirate.sea: type NULL, class IN
        Name: vaaaakardli.pirate.sea
        Type: NULL (Null resource record)

0000  08 00 27 c7 6e ba 08 00  27 9c e0 b4 08 00 45 00   ..'.n... '.....E.
0010  00 44 00 00 40 00 40 11  22 78 0a 00 02 1e 0a 00   .D..@.@. "x......
0020  02 14 ae 5f 00 35 00 30  01 e4 12 b0 01 00 00 01   ..._.5.0 ........
0030  00 00 00 00 00 00 06 76  61 61 61 61 6b 61 72 64   .......v aaaakard
0040  6c 69 06 70 69 72 61 74  65 03 73 65 61 00 00 0a   li.pirat e.sea...
0050  00 01                                              ..
```

What is occurring?

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

Answer: D

NEW QUESTION 182
Which filter allows an engineer to filter traffic in Wireshark to further analyze the PCAP file by only showing the traffic for LAN 10.11.x.x, between workstations and servers without the Internet?

A. src=10.11.0.0/16 and dst=10.11.0.0/16
B. ip.src==10.11.0.0/16 and ip.dst==10.11.0.0/16
C. ip.src=10.11.0.0/16 and ip.dst=10.11.0.0/16
D. src==10.11.0.0/16 and dst==10.11.0.0/16

Answer: B

NEW QUESTION 186
What is an incident response plan?

A. an organizational approach to events that could lead to asset loss or disruption of operations
B. an organizational approach to security management to ensure a service lifecycle and continuous improvements
C. an organizational approach to disaster recovery and timely restoration of operational services
D. an organizational approach to system backup and data archiving aligned to regulations

Answer: C

NEW QUESTION 190
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 193
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

Answer: B

NEW QUESTION 194
Which action prevents buffer overflow attacks?

A. variable randomization
B. using web based applications

C. input sanitization
D. using a Linux operating system

Answer: C

NEW QUESTION 196
In a SOC environment, what is a vulnerability management metric?

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

Answer: C

NEW QUESTION 197
Which type of data collection requires the largest amount of storage space?

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

Answer: D

NEW QUESTION 199
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})

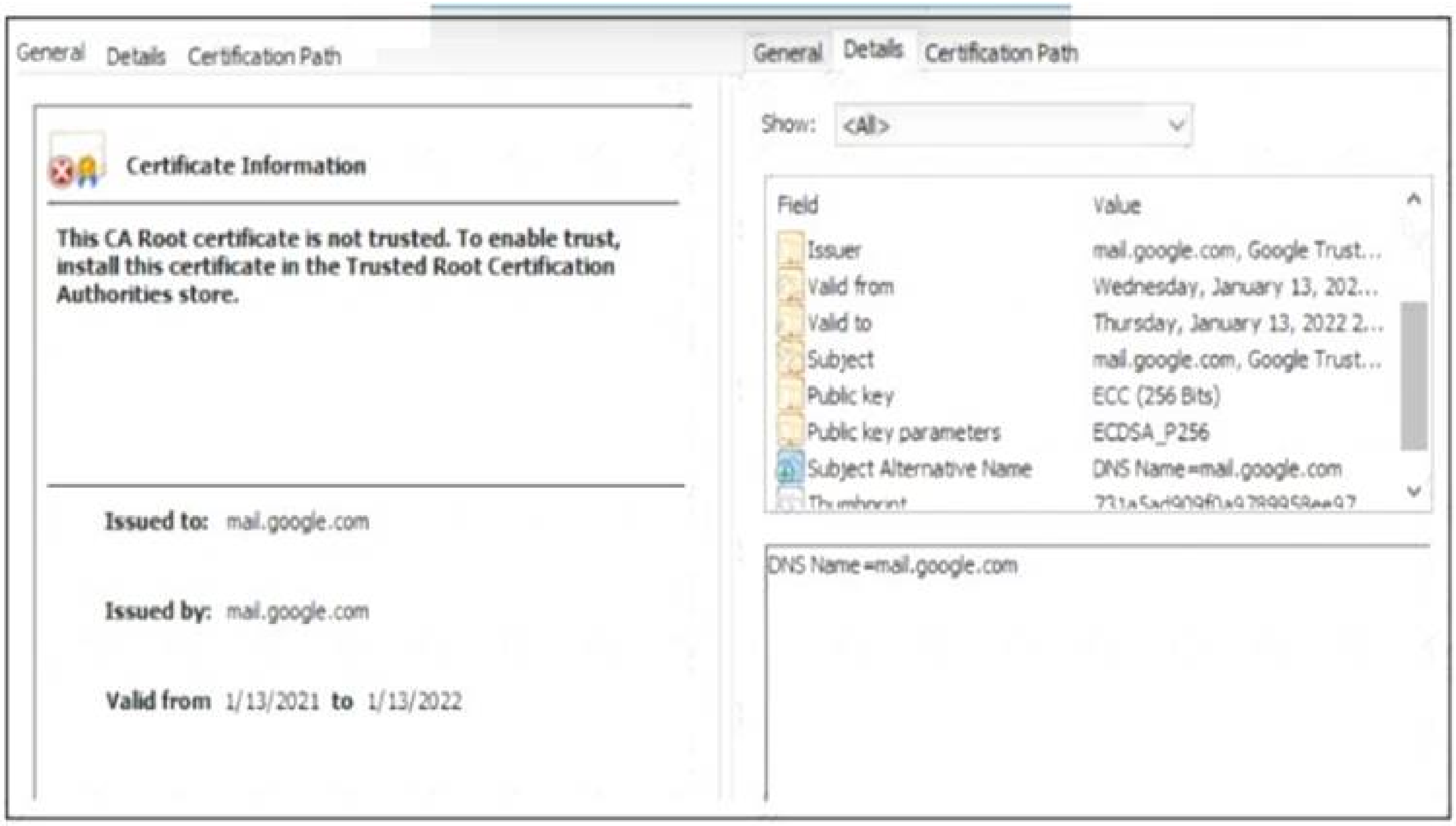
Answer: A

NEW QUESTION 204
What is the impact of encryption?

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

Answer: A

NEW QUESTION 207
Refer to the exhibit.



Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: mail.google.com

Issued by: mail.google.com

Valid from 1/13/2021 **to** 1/13/2022

Show: <All>

Field	Value
Issuer	mail.google.com, Google Trust...
Valid from	Wednesday, January 13, 202...
Valid to	Thursday, January 13, 2022 2...
Subject	mail.google.com, Google Trust...
Public key	ECC (256 Bits)
Public key parameters	ECDSA_P256
Subject Alternative Name	DNS Name=mail.google.com
Thumbprint	731a5ad909f0a9789958ee97

DNS Name=mail.google.com

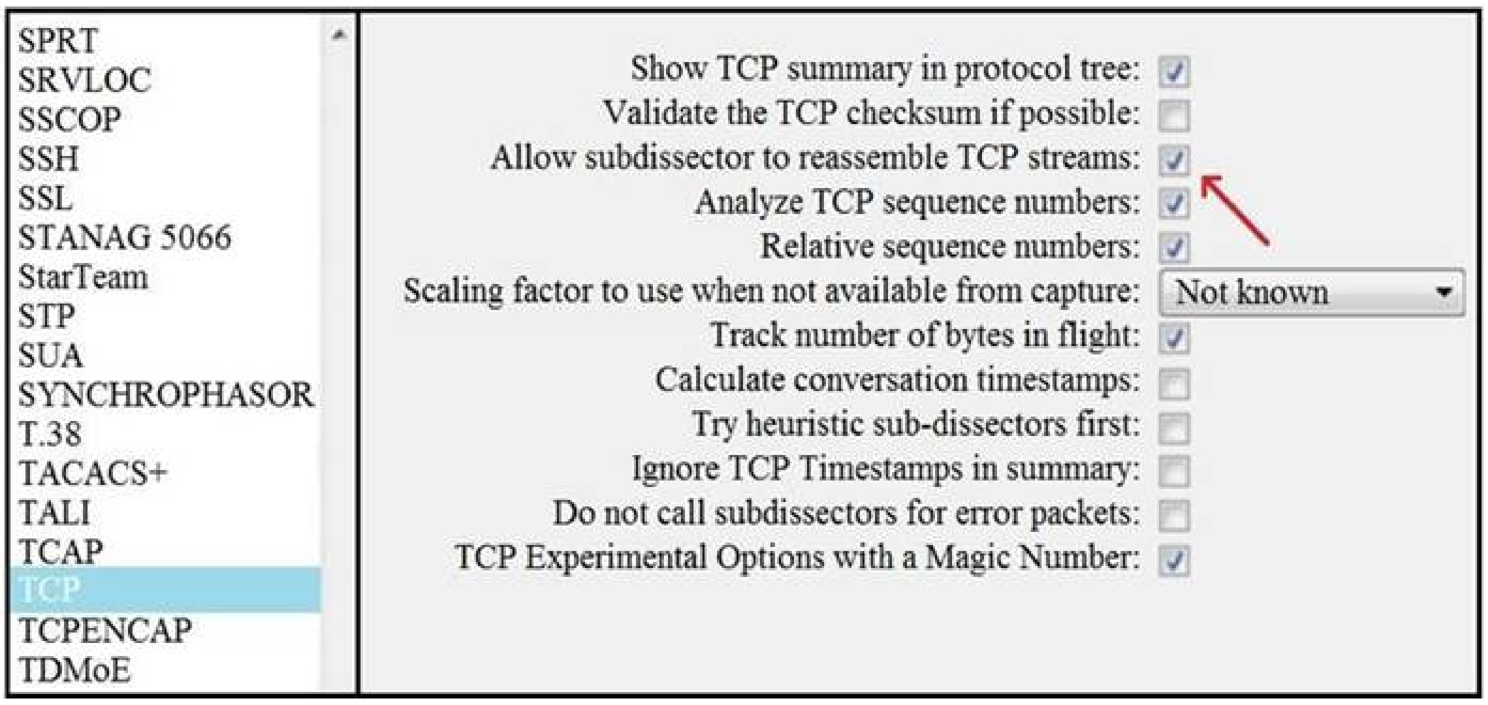
A company employee is connecting to mail google.com from an endpoint device. The website is loaded but with an error. What is occurring?

A. DNS hijacking attack
B. Endpoint local time is invalid.

C. Certificate is not in trusted roots.
D. man-m-the-middle attack

Answer: C

NEW QUESTION 212
Refer to the exhibit.



SPRT
SRVLOC
SSCOP
SSH
SSL
STANAG 5066
StarTeam
STP
SUA
SYNCHROPHASOR
T.38
TACACS+
TALI
TCAP
TCP
TCPENCAP
TDMoE

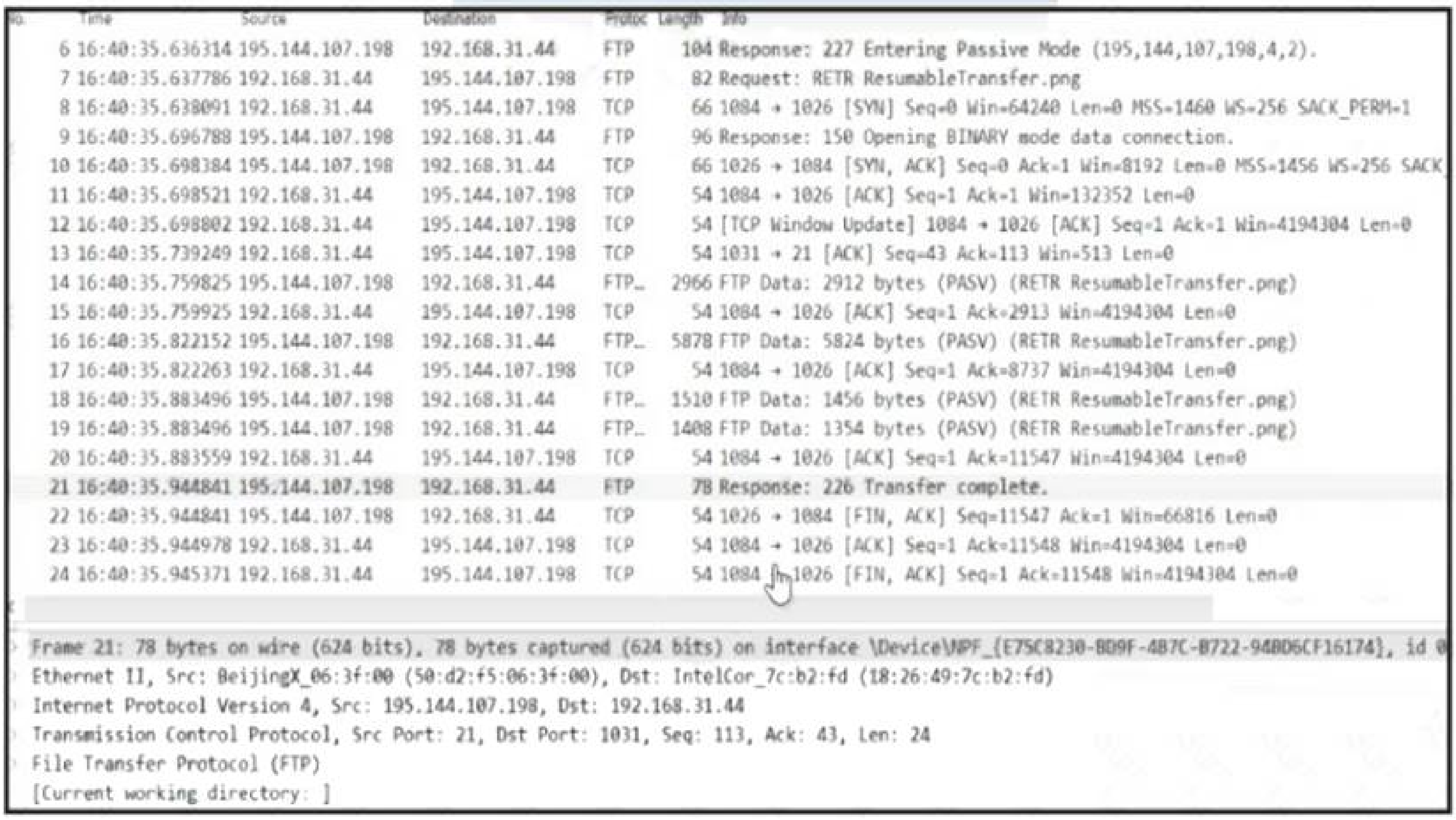
Show TCP summary in protocol tree: ☑
Validate the TCP checksum if possible: ☐
Allow subdissector to reassemble TCP streams: ☑
Analyze TCP sequence numbers: ☑
Relative sequence numbers: ☑
Scaling factor to use when not available from capture: Not known
Track number of bytes in flight: ☑
Calculate conversation timestamps: ☐
Try heuristic sub-dissectors first: ☐
Ignore TCP Timestamps in summary: ☐
Do not call subdissectors for error packets: ☐
TCP Experimental Options with a Magic Number: ☑

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 217
Refer to the exhibit.



```
No.  Time             Source           Destination      Protoc Length Info
 6 16:40:35.636314 195.144.107.198 192.168.31.44   FTP    104 Response: 227 Entering Passive Mode (195,144,107,198,4,2).
 7 16:40:35.637786 192.168.31.44   195.144.107.198 FTP     82 Request: RETR ResumableTransfer.png
 8 16:40:35.638091 192.168.31.44   195.144.107.198 TCP     66 1084 → 1026 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 9 16:40:35.696788 195.144.107.198 192.168.31.44   FTP     96 Response: 150 Opening BINARY mode data connection.
10 16:40:35.698384 195.144.107.198 192.168.31.44   TCP     66 1026 → 1084 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1456 WS=256 SACK
11 16:40:35.698521 192.168.31.44   195.144.107.198 TCP     54 1084 → 1026 [ACK] Seq=1 Ack=1 Win=132352 Len=0
12 16:40:35.698802 192.168.31.44   195.144.107.198 TCP     54 [TCP Window Update] 1084 → 1026 [ACK] Seq=1 Ack=1 Win=4194304 Len=0
13 16:40:35.739249 192.168.31.44   195.144.107.198 TCP     54 1031 → 21 [ACK] Seq=43 Ack=113 Win=513 Len=0
14 16:40:35.759825 195.144.107.198 192.168.31.44   FTP…  2966 FTP Data: 2912 bytes (PASV) (RETR ResumableTransfer.png)
15 16:40:35.759925 192.168.31.44   195.144.107.198 TCP     54 1084 → 1026 [ACK] Seq=1 Ack=2913 Win=4194304 Len=0
16 16:40:35.822152 195.144.107.198 192.168.31.44   FTP…  5878 FTP Data: 5824 bytes (PASV) (RETR ResumableTransfer.png)
17 16:40:35.822263 192.168.31.44   195.144.107.198 TCP     54 1084 → 1026 [ACK] Seq=1 Ack=8737 Win=4194304 Len=0
18 16:40:35.883496 195.144.107.198 192.168.31.44   FTP…  1510 FTP Data: 1456 bytes (PASV) (RETR ResumableTransfer.png)
19 16:40:35.883496 195.144.107.198 192.168.31.44   FTP…  1408 FTP Data: 1354 bytes (PASV) (RETR ResumableTransfer.png)
20 16:40:35.883559 192.168.31.44   195.144.107.198 TCP     54 1084 → 1026 [ACK] Seq=1 Ack=11547 Win=4194304 Len=0
21 16:40:35.944841 195.144.107.198 192.168.31.44   FTP     78 Response: 226 Transfer complete.
22 16:40:35.944841 195.144.107.198 192.168.31.44   TCP     54 1026 → 1084 [FIN, ACK] Seq=11547 Ack=1 Win=66816 Len=0
23 16:40:35.944978 192.168.31.44   195.144.107.198 TCP     54 1084 → 1026 [ACK] Seq=1 Ack=11548 Win=4194304 Len=0
24 16:40:35.945371 192.168.31.44   195.144.107.198 TCP     54 1084 → 1026 [FIN, ACK] Seq=1 Ack=11548 Win=4194304 Len=0

Frame 21: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface \Device\NPF_{E75C8230-BD9F-4B7C-B722-94BD6CF16174}, id 0
Ethernet II, Src: BeijingX_06:3f:00 (50:d2:f5:06:3f:00), Dst: IntelCor_7c:b2:fd (18:26:49:7c:b2:fd)
Internet Protocol Version 4, Src: 195.144.107.198, Dst: 192.168.31.44
Transmission Control Protocol, Src Port: 21, Dst Port: 1031, Seq: 113, Ack: 43, Len: 24
File Transfer Protocol (FTP)
[Current working directory: ]
```

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

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

Answer: B

NEW QUESTION 221
What is a difference between signature-based and behavior-based detection?

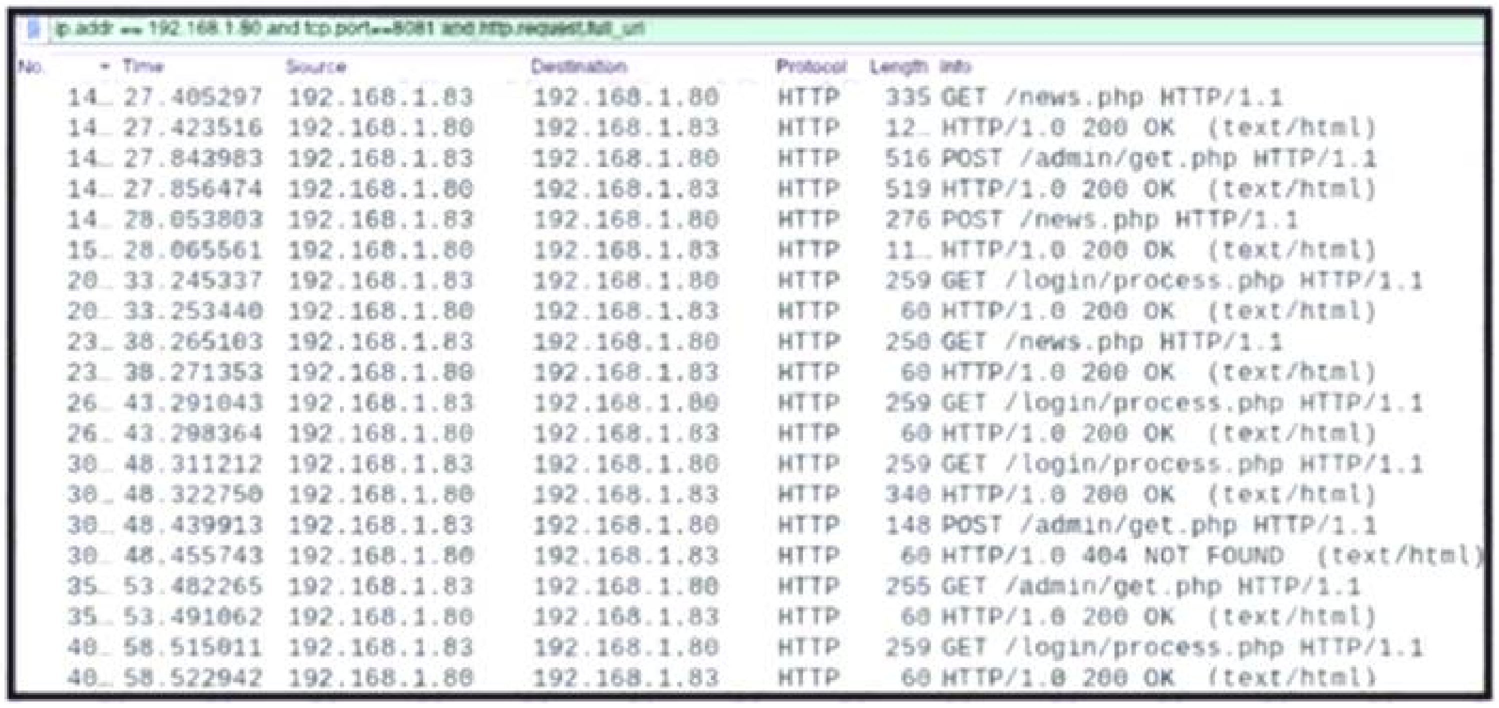
A. Signature-based identifies behaviors that may be linked to attacks, while behavior-based has a predefined set of rules to match before an alert.

B. Behavior-based identifies behaviors that may be linked to attacks, while signature-based has a predefined set of rules to match before an alert.
C. Behavior-based uses a known vulnerability database, while signature-based intelligently summarizes existing data.
D. Signature-based uses a known vulnerability database, while behavior-based intelligently summarizes existing data.

Answer: B

Explanation:
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/what-is-the-difference-between-signature-based-and-behavior-based-ids/

NEW QUESTION 223
Refer to the exhibit.



```
ip.addr == 192.168.1.80 and tcp.port==8081 and http.request.full_uri
No.   Time        Source          Destination     Protocol  Length Info
  14… 27.405297  192.168.1.83    192.168.1.80    HTTP   335 GET /news.php HTTP/1.1
  14… 27.423516  192.168.1.80    192.168.1.83    HTTP   12… HTTP/1.0 200 OK  (text/html)
  14… 27.843983  192.168.1.83    192.168.1.80    HTTP   516 POST /admin/get.php HTTP/1.1
  14… 27.856474  192.168.1.80    192.168.1.83    HTTP   519 HTTP/1.0 200 OK  (text/html)
  14… 28.053803  192.168.1.83    192.168.1.80    HTTP   276 POST /news.php HTTP/1.1
  15… 28.065561  192.168.1.80    192.168.1.83    HTTP   11… HTTP/1.0 200 OK  (text/html)
  20… 33.245337  192.168.1.83    192.168.1.80    HTTP   259 GET /login/process.php HTTP/1.1
  20… 33.253440  192.168.1.80    192.168.1.83    HTTP    60 HTTP/1.0 200 OK  (text/html)
  23… 38.265103  192.168.1.83    192.168.1.80    HTTP   250 GET /news.php HTTP/1.1
  23… 38.271353  192.168.1.80    192.168.1.83    HTTP    60 HTTP/1.0 200 OK  (text/html)
  26… 43.291043  192.168.1.83    192.168.1.80    HTTP   259 GET /login/process.php HTTP/1.1
  26… 43.298364  192.168.1.80    192.168.1.83    HTTP    60 HTTP/1.0 200 OK  (text/html)
  30… 48.311212  192.168.1.83    192.168.1.80    HTTP   259 GET /login/process.php HTTP/1.1
  30… 48.322750  192.168.1.80    192.168.1.83    HTTP   340 HTTP/1.0 200 OK  (text/html)
  30… 48.439913  192.168.1.83    192.168.1.80    HTTP   148 POST /admin/get.php HTTP/1.1
  30… 48.455743  192.168.1.80    192.168.1.83    HTTP    60 HTTP/1.0 404 NOT FOUND  (text/html)
  35… 53.482265  192.168.1.83    192.168.1.80    HTTP   255 GET /admin/get.php HTTP/1.1
  35… 53.491062  192.168.1.80    192.168.1.83    HTTP    60 HTTP/1.0 200 OK  (text/html)
  40… 58.515011  192.168.1.83    192.168.1.80    HTTP   259 GET /login/process.php HTTP/1.1
  40… 58.522942  192.168.1.80    192.168.1.83    HTTP    60 HTTP/1.0 200 OK  (text/html)
```

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

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

Answer: D

NEW QUESTION 224
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 226
Refer to the exhibit.

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

Which kind of attack method is depicted in this string?

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

Answer: A

NEW QUESTION 227
......