Cisco

Exam Questions 200-201

Understanding Cisco Cybersecurity Operations Fundamentals

NEW QUESTION 1
What is a difference between an inline and a tap mode traffic monitoring?

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

Answer: D

NEW QUESTION 2
Which of these describes SOC metrics in relation to security incidents?

A. time it takes to detect the incident
B. time it takes to assess the risks of the incident
C. probability of outage caused by the incident
D. probability of compromise and impact caused by the incident

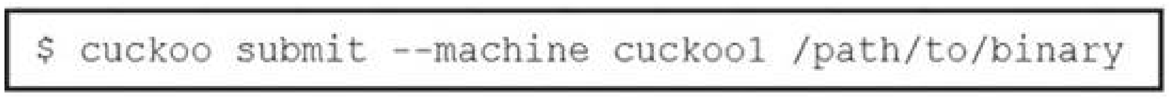
Answer: A

NEW QUESTION 3
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 4
Refer to the exhibit.



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

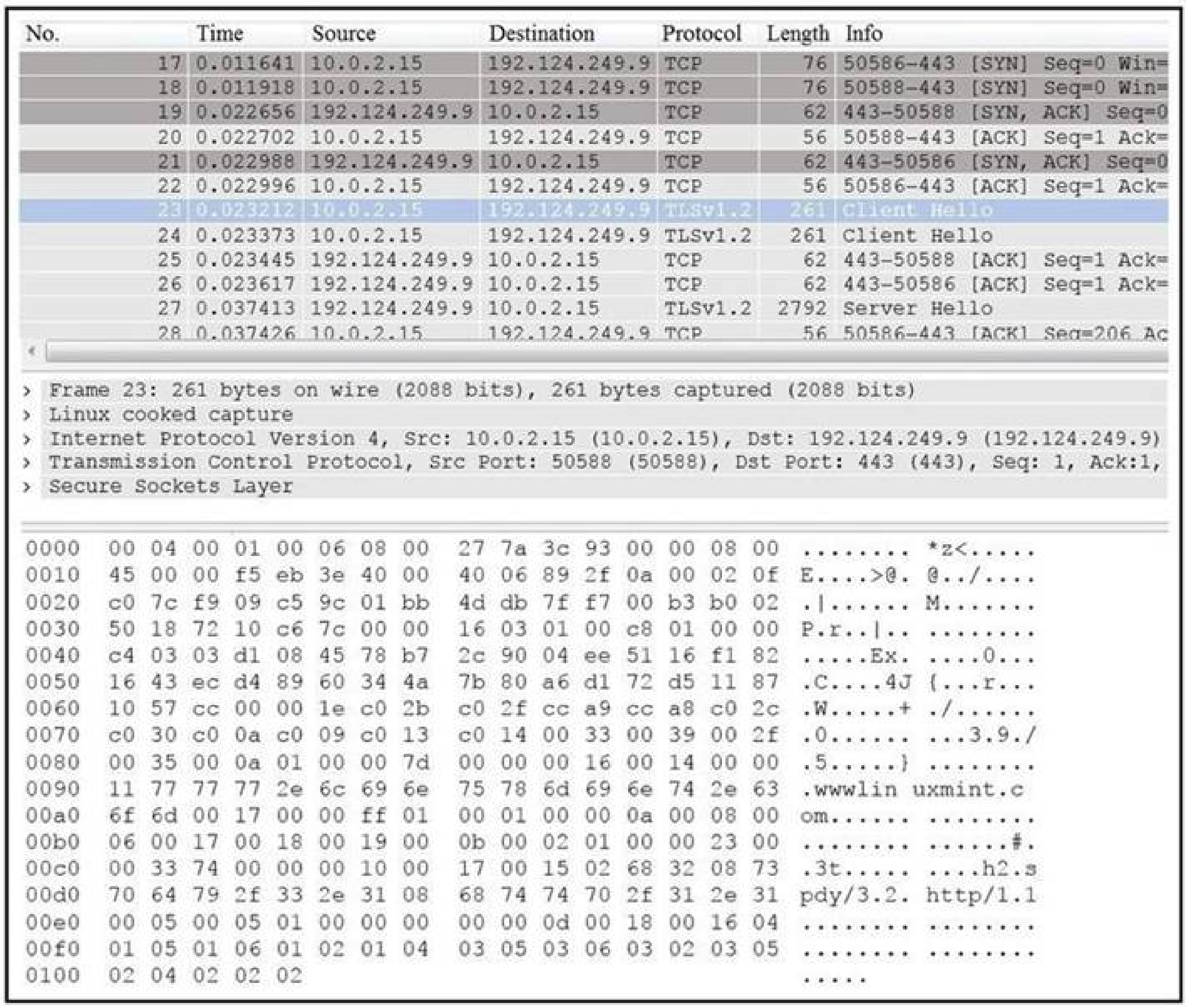
Which event is occurring?

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 5
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. ....0...
0050  16 43 ec d4 89 60 34 4a  7b 80 a6 d1 72 d5 11 87   .C....4J {...r...
0060  10 57 cc 00 00 1e c0 2b  c0 2f cc a9 cc a8 c0 2c   .W.....+ ./......
0070  c0 30 c0 0a c0 09 c0 13  c0 14 00 33 00 39 00 2f   .0...... ...3.9./
0080  00 35 00 0a 01 00 00 7d  00 00 00 16 00 14 00 00   .5.....} ........
0090  11 77 77 77 2e 6c 69 6e  75 78 6d 69 6e 74 2e 63   .wwwlin uxmint.c
00a0  6f 6d 00 17 00 00 ff 01  00 01 00 00 0a 00 08 00   om...... ........
00b0  06 00 17 00 18 00 19 00  0b 00 02 01 00 00 23 00   ........ ......#.
00c0  00 33 74 00 00 00 10 00  17 00 15 02 68 32 08 73   .3t..... ....h2.s
00d0  70 64 79 2f 33 2e 31 08  68 74 74 70 2f 31 2e 31   pdy/3.2. http/1.1
00e0  00 05 00 05 01 00 00 00  00 00 0d 00 18 00 16 04   ........ ........
00f0  01 05 01 06 01 02 01 04  03 05 03 06 03 02 03 05   ........ ........
0100  02 04 02 02 02                                     .....
```

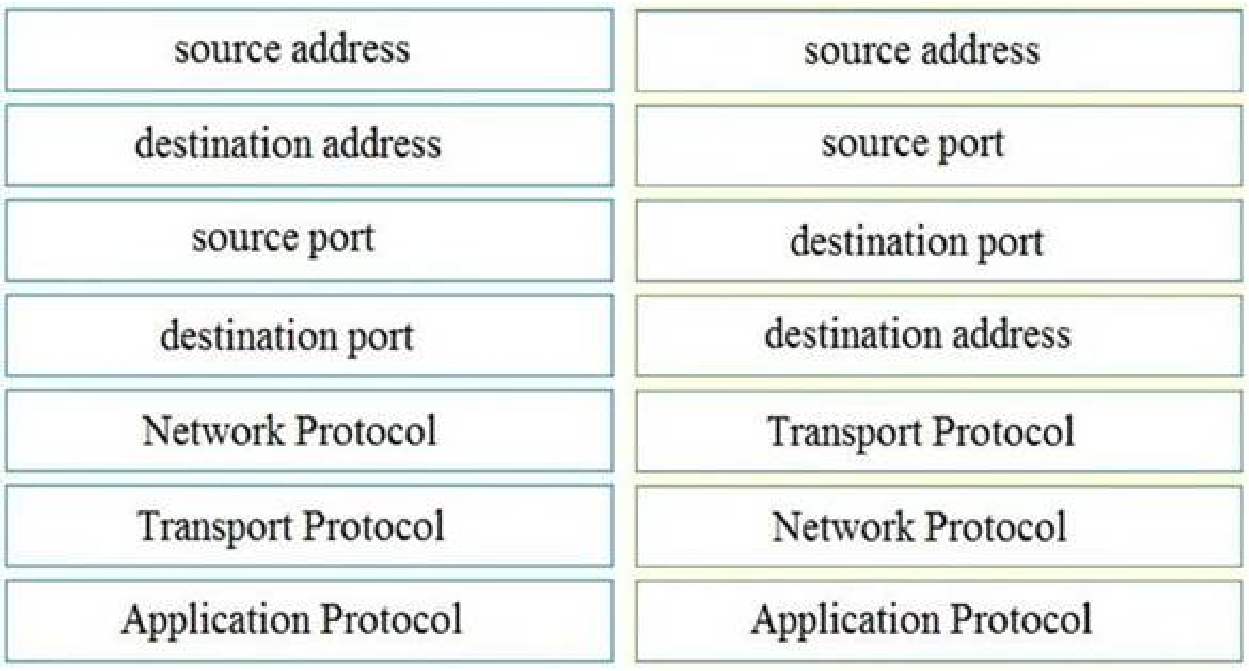
Drag and drop the element name from the left onto the correct piece of the PCAP file on the right.

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 6
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 7
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 8
A security engineer has a video of a suspect entering a data center that was captured on the same day that files in the same data center were transferred to a competitor.
Which type of evidence is this?

A. best evidence
B. prima facie evidence
C. indirect evidence
D. physical evidence

Answer: C

Explanation:
There are three general types of evidence:
--> Best evidence: can be presented in court in the original form (for example, an exact copy of a hard disk drive).
--> Corroborating evidence: tends to support a theory or an assumption deduced by some initial evidence. This corroborating evidence confirms the proposition.
--> Indirect or circumstantial evidence: extrapolation to a conclusion of fact (such as fingerprints, DNA evidence, and so on).

NEW QUESTION 9
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

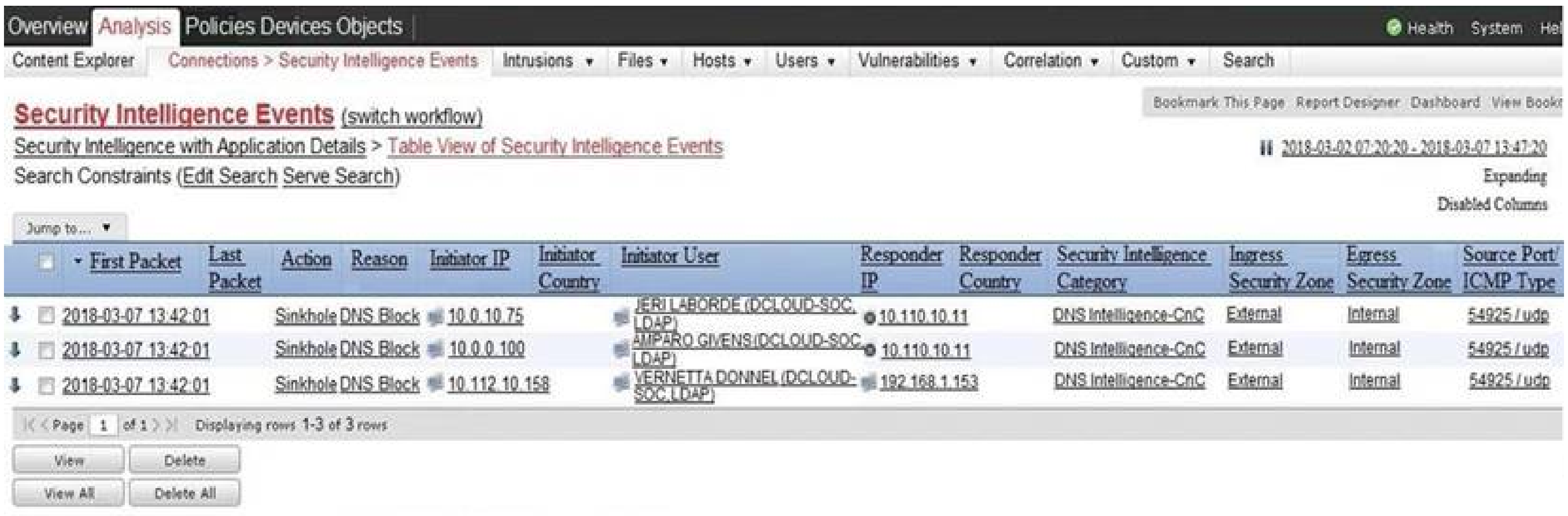
NEW QUESTION 10

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 10
Refer to the exhibit.



Security Intelligence Events (switch workflow)
Security Intelligence with Application Details > Table View of Security Intelligence Events
Search Constraints (Edit Search Serve Search)

2018-03-02 07:20:20 - 2018-03-07 13:47:20
Expanding
Disabled Columns

	☐	First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Initiator User	Responder IP	Responder Country	Security Intelligence Category	Ingress Security Zone	Egress Security Zone	Source Port/ ICMP Type
⬇	☐	2018-03-07 13:42:01		Sinkhole	DNS Block	10.0.10.75		JERI LABORDE (DCLOUD-SOC, LDAP)	10.110.10.11		DNS Intelligence-CnC	External	Internal	54925 / udp
⬇	☐	2018-03-07 13:42:01		Sinkhole	DNS Block	10.0.0.100		AMPARO GIVENS(DCLOUD-SOC, LDAP)	10.110.10.11		DNS Intelligence-CnC	External	Internal	54925 / udp
⬇	☐	2018-03-07 13:42:01		Sinkhole	DNS Block	10.112.10.158		VERNETTA DONNEL (DCLOUD-SOC LDAP)	192.168.1.153		DNS Intelligence-CnC	External	Internal	54925 / udp

Page 1 of 1 Displaying rows 1-3 of 3 rows

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

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

Answer: DE

NEW QUESTION 12
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 14
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 18
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

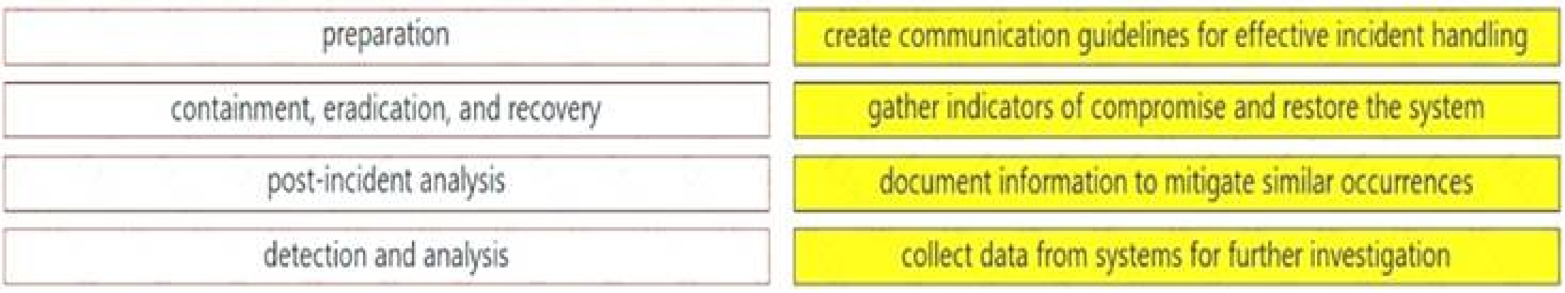
Answer: B

NEW QUESTION 19
Which event is user interaction?

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

Answer: D

NEW QUESTION 23
Drag and drop the elements from the left into the correct order for incident handling on the right.

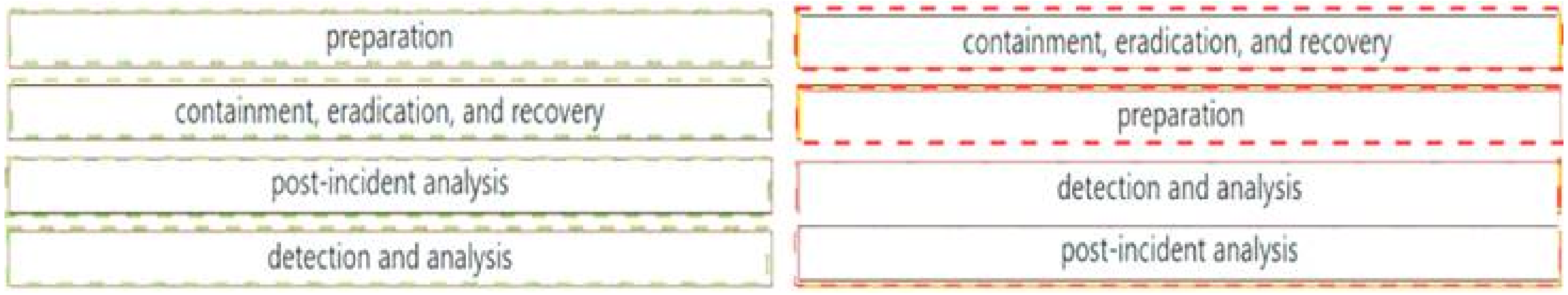


preparation	create communication guidelines for effective incident handling
containment, eradication, and recovery	gather indicators of compromise and restore the system
post-incident analysis	document information to mitigate similar occurrences
detection and analysis	collect data from systems for further investigation

A. Mastered
B. Not Mastered

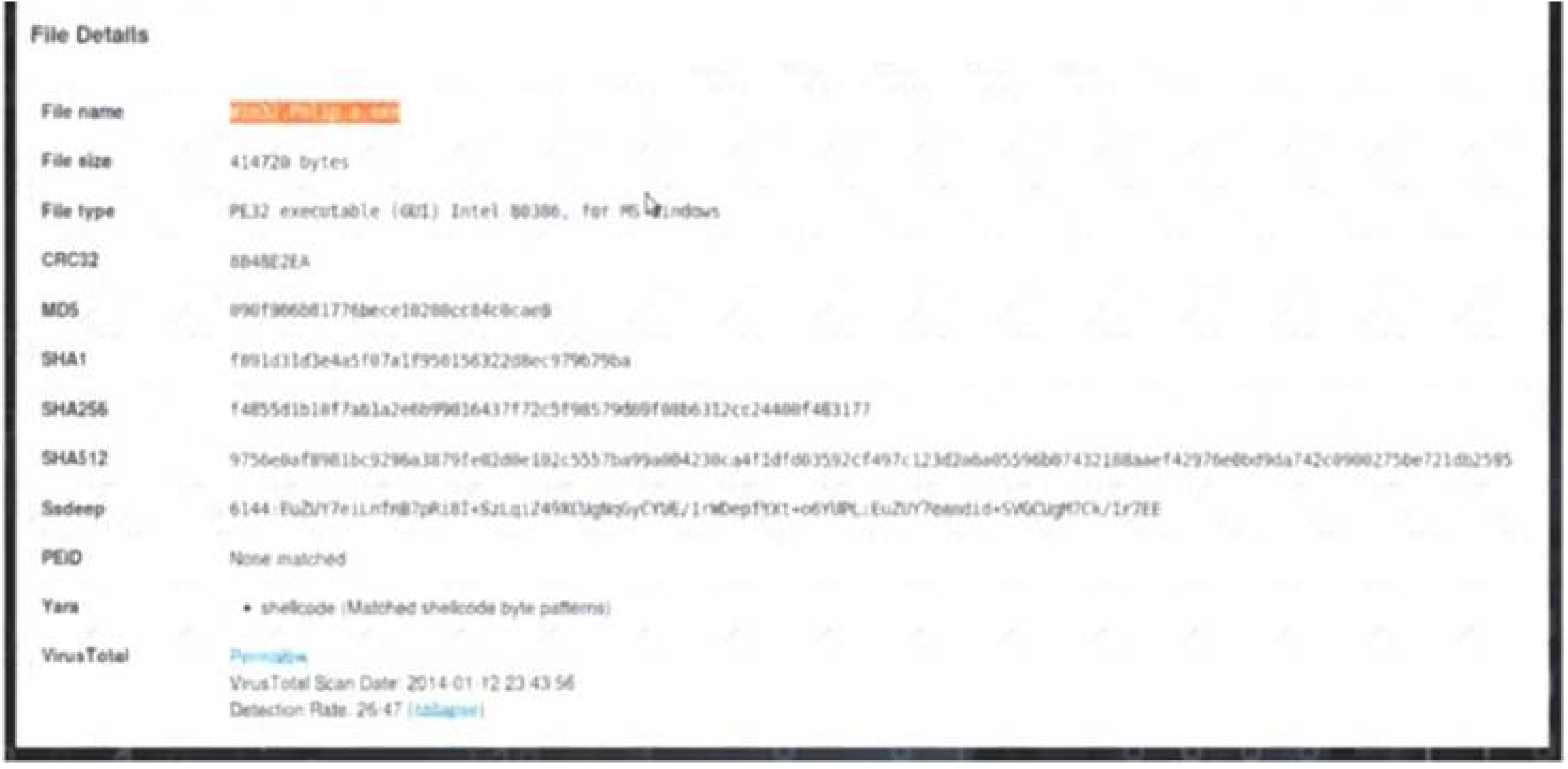
Answer: A

Explanation:



preparation	containment, eradication, and recovery
containment, eradication, and recovery	preparation
post-incident analysis	detection and analysis
detection and analysis	post-incident analysis

NEW QUESTION 24
A malicious file has been identified in a sandbox analysis tool.



File Details

File name	[illegible]
File size	414720 bytes
File type	PE32 executable (GUI) Intel 80386, for MS Windows
CRC32	8B48E2EA
MD5	090f9066b81776bece18288cc84c8cae9
SHA1	f891d31d3e4a5f07a1f950156322d8ec979b79ba
SHA256	f4855d1b18f7ab1a2e6b99816437f72c5f98579d89f08b6312cc24400f483177
SHA512	9756e0af8981bc9296a3879fe82d0e102c5557ba99a804230ca4f1dfd03592cf497c123d2a6a05596b07432188aaef42976e0bd9da742c09002750e721db2595
Ssdeep	6144:EuZUY7eiLnfnB7pRi8I+SzLqiZ49XOUgNqGyCYUE/1rWDepfYXt+o6YUPL:EuZUY7eandid+SVGCUgM7Ck/1r7EE
PEiD	None matched
Yara	• shellcode (Matched shellcode byte patterns)
VirusTotal	Permalink VirusTotal Scan Date: 2014-01-12 23:43:56 Detection Rate: 26/47 (collapse)

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

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

Answer: D

NEW QUESTION 27
An engineer needs to fetch logs from a proxy server and generate actual events according to the data received. Which technology should the engineer use to accomplish this task?

A. Firepower
B. Email Security Appliance
C. Web Security Appliance
D. Stealthwatch

Answer: C

NEW QUESTION 28
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

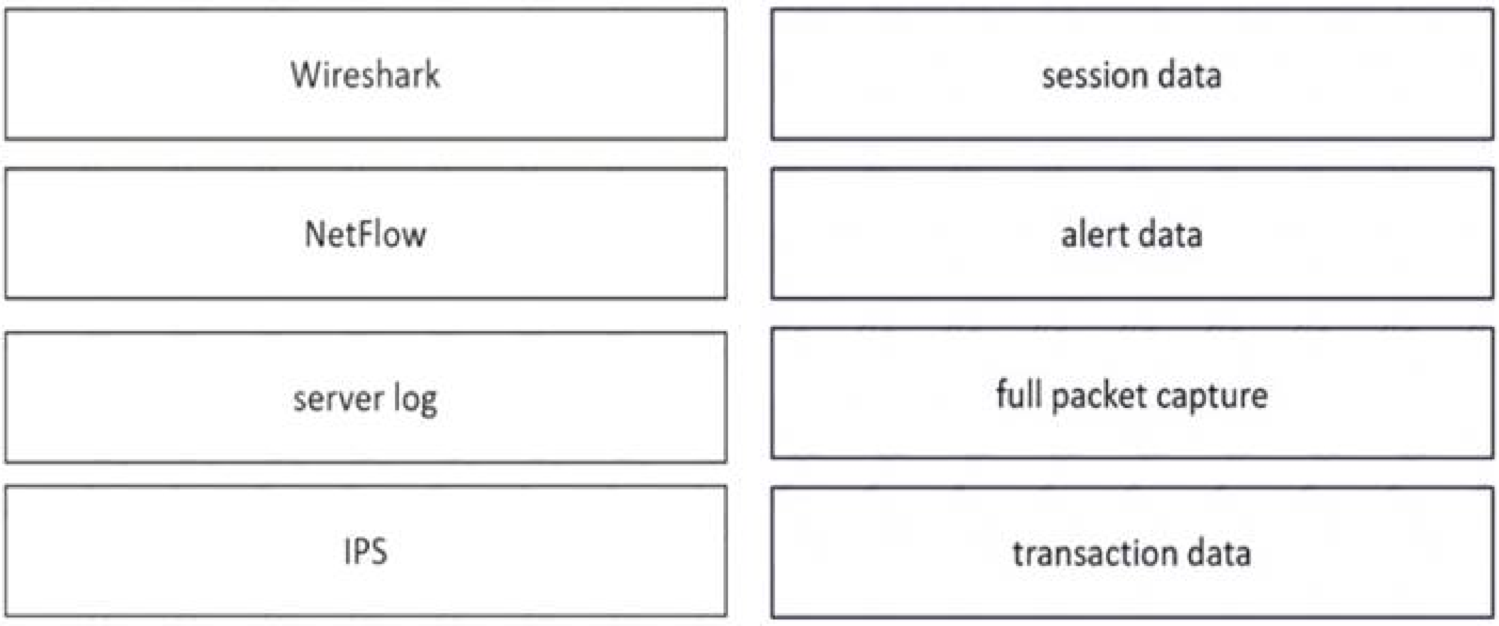
NEW QUESTION 32
What is a benefit of agent-based protection when compared to agentless protection?

A. It lowers maintenance costs
B. It provides a centralized platform
C. It collects and detects all traffic locally
D. It manages numerous devices simultaneously

Answer: C

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

NEW QUESTION 34
Drag and drop the data source from the left onto the data type on the right.

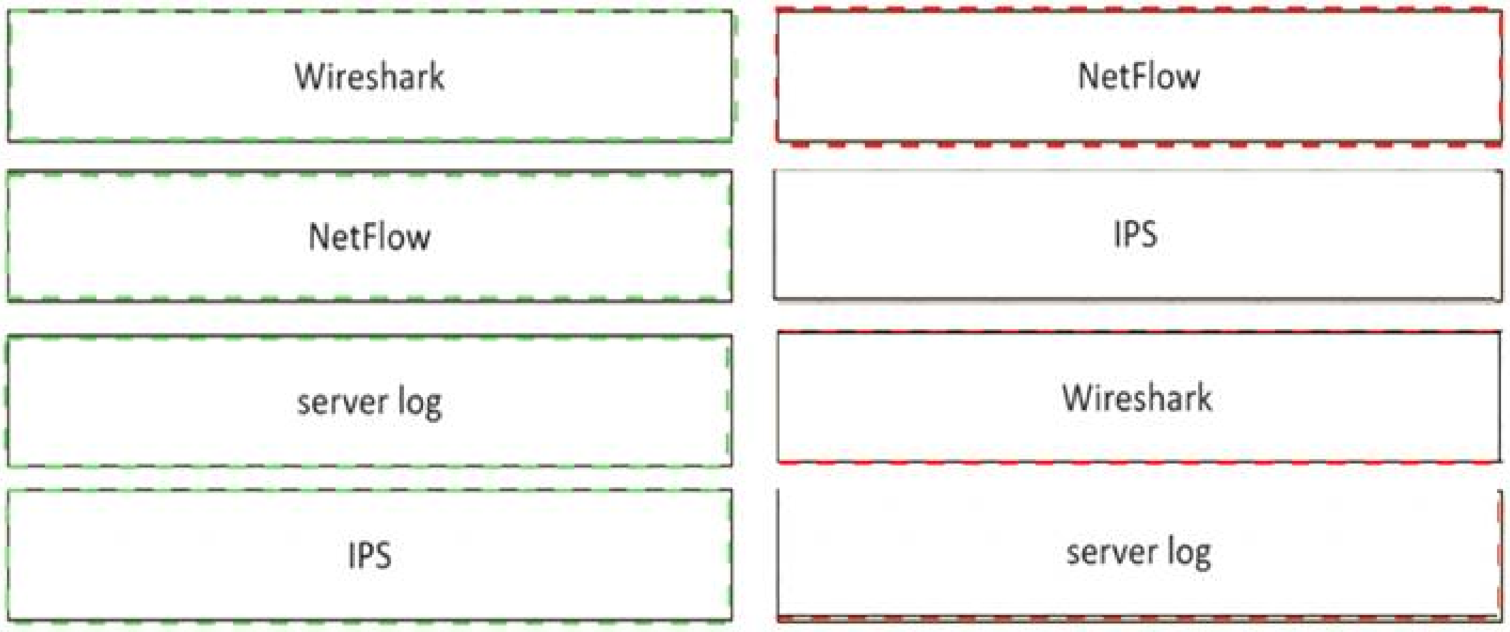


Wireshark	session data
NetFlow	alert data
server log	full packet capture
IPS	transaction data

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Wireshark	NetFlow
NetFlow	IPS
server log	Wireshark
IPS	server log

NEW QUESTION 39
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 42

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 47
Which evasion technique is a function of ransomware?

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

Answer: B

NEW QUESTION 48
An engineer runs a suspicious file in a sandbox analysis tool to see the outcome. The analysis report shows that outbound callouts were made post infection. Which two pieces of information from the analysis report are needed to investigate the callouts? (Choose two.)

A. signatures
B. host IP addresses
C. file size
D. dropped files
E. domain names

Answer: BE

NEW QUESTION 49
Which data type is necessary to get information about source/destination ports?

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

Answer: B

Explanation:
Session data provides information about the five tuples; source IP address/port number, destination IP address/port number and the protocol
What is Connectivity Data? According to IBM - Connectivity data defines how entities are connected in the network. It includes connections between different devices, and VLAN-related connections within the same
device https://www.ibm.com/docs/en/networkmanager/4.2.0?topic=relationships-connectivity-data

NEW QUESTION 53
Which category relates to improper use or disclosure of PII data?

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

Answer: C

NEW QUESTION 54
An analyst is investigating an incident in a SOC environment. Which method is used to identify a session from a group of logs?

A. sequence numbers
B. IP identifier
C. 5-tuple
D. timestamps

Answer: C

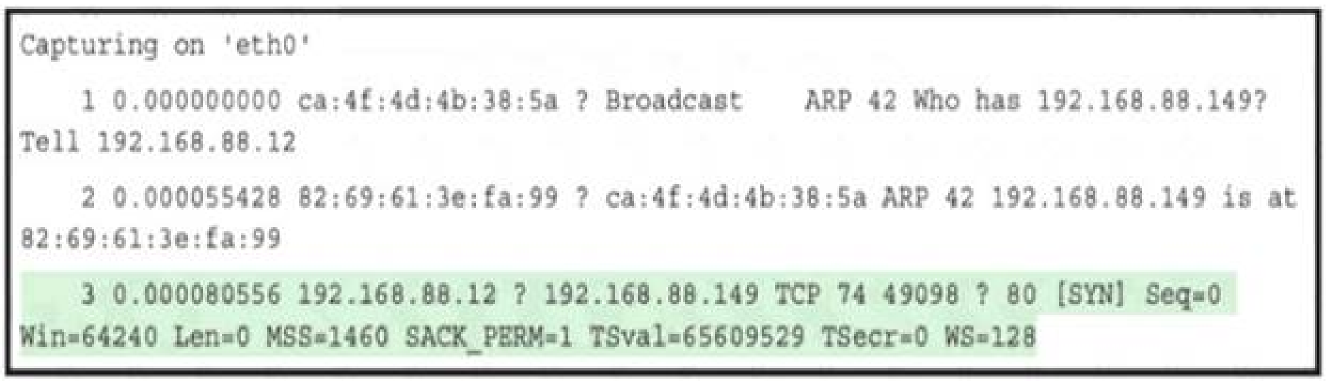
NEW QUESTION 56
A security analyst notices a sudden surge of incoming traffic and detects unknown packets from unknown senders After further investigation, the analyst learns that customers claim that they cannot access company servers According to NIST SP800-61, in which phase of the incident response process is the analyst?

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

Answer:

B

NEW QUESTION 61
Refer to the exhibit.



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

What must be interpreted from this packet capture?

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

Answer: B

NEW QUESTION 63
Which metric should be used when evaluating the effectiveness and scope of a Security Operations Center?

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

Answer: C

NEW QUESTION 66
Which two elements of the incident response process are stated in NIST SP 800-61 r2? (Choose two.)

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

Answer: AB

NEW QUESTION 70
How does an attacker observe network traffic exchanged between two users?

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

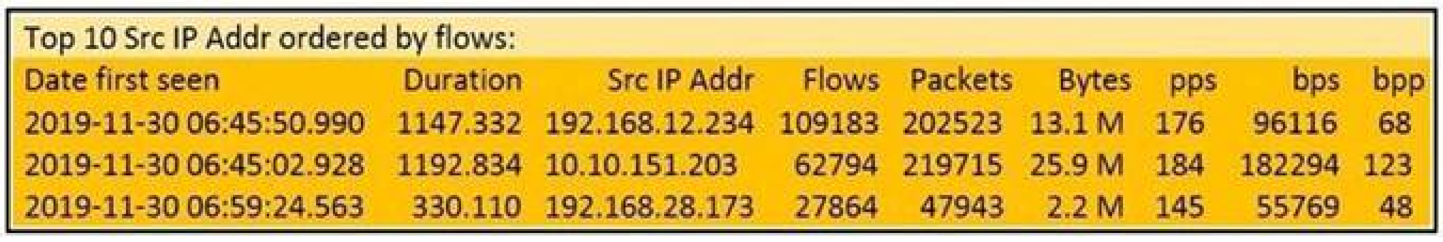
Answer: B

NEW QUESTION 73
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 74
Refer to the exhibit.



Top 10 Src IP Addr ordered by flows:

Date first seen	Duration	Src IP Addr	Flows	Packets	Bytes	pps	bps	bpp
2019-11-30 06:45:50.990	1147.332	192.168.12.234	109183	202523	13.1 M	176	96116	68
2019-11-30 06:45:02.928	1192.834	10.10.151.203	62794	219715	25.9 M	184	182294	123
2019-11-30 06:59:24.563	330.110	192.168.28.173	27864	47943	2.2 M	145	55769	48

What information is depicted?

A. IIS data

B. NetFlow data
C. network discovery event
D. IPS event data

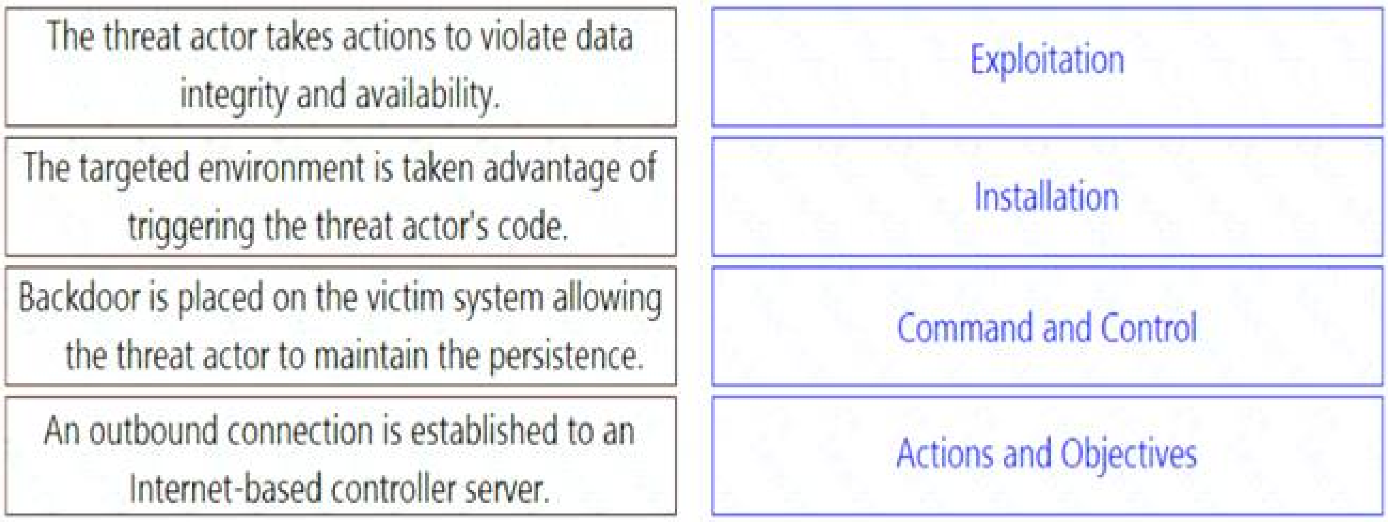
Answer: B

NEW QUESTION 75
An engineer receives a security alert that traffic with a known TOR exit node has occurred on the network. What is the impact of this traffic?

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

Answer: D

NEW QUESTION 77
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 79
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.

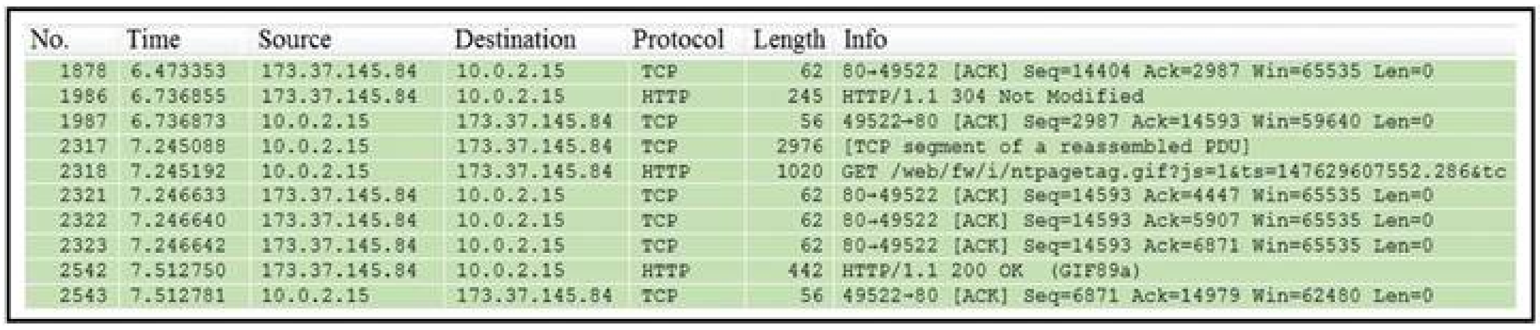
Answer: D

NEW QUESTION 81
A security engineer deploys an enterprise-wide host/endpoint technology for all of the company's corporate PCs. Management requests the engineer to block a selected set of applications on all PCs. Which technology should be used to accomplish this task?

A. application whitelisting/blacklisting
B. network NGFW
C. host-based IDS
D. antivirus/antispyware software

Answer: A

NEW QUESTION 83
Refer to the exhibit.



No.	Time	Source	Destination	Protocol	Length	Info
1878	6.473353	173.37.145.84	10.0.2.15	TCP	62	80→49522 [ACK] Seq=14404 Ack=2987 Win=65535 Len=0
1986	6.736855	173.37.145.84	10.0.2.15	HTTP	245	HTTP/1.1 304 Not Modified
1987	6.736873	10.0.2.15	173.37.145.84	TCP	56	49522→80 [ACK] Seq=2987 Ack=14593 Win=59640 Len=0
2317	7.245088	10.0.2.15	173.37.145.84	TCP	2976	[TCP segment of a reassembled PDU]
2318	7.245192	10.0.2.15	173.37.145.84	HTTP	1020	GET /web/fw/i/ntpagetag.gif?js=1&ts=147629607552.286&tc
2321	7.246633	173.37.145.84	10.0.2.15	TCP	62	80→49522 [ACK] Seq=14593 Ack=4447 Win=65535 Len=0
2322	7.246640	173.37.145.84	10.0.2.15	TCP	62	80→49522 [ACK] Seq=14593 Ack=5907 Win=65535 Len=0
2323	7.246642	173.37.145.84	10.0.2.15	TCP	62	80→49522 [ACK] Seq=14593 Ack=6871 Win=65535 Len=0
2542	7.512750	173.37.145.84	10.0.2.15	HTTP	442	HTTP/1.1 200 OK (GIF89a)
2543	7.512781	10.0.2.15	173.37.145.84	TCP	56	49522→80 [ACK] Seq=6871 Ack=14979 Win=62480 Len=0

Which packet contains a file that is extractable within Wireshark?

A. 2317
B. 1986
C. 2318
D. 2542

Answer: D

NEW QUESTION 84
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

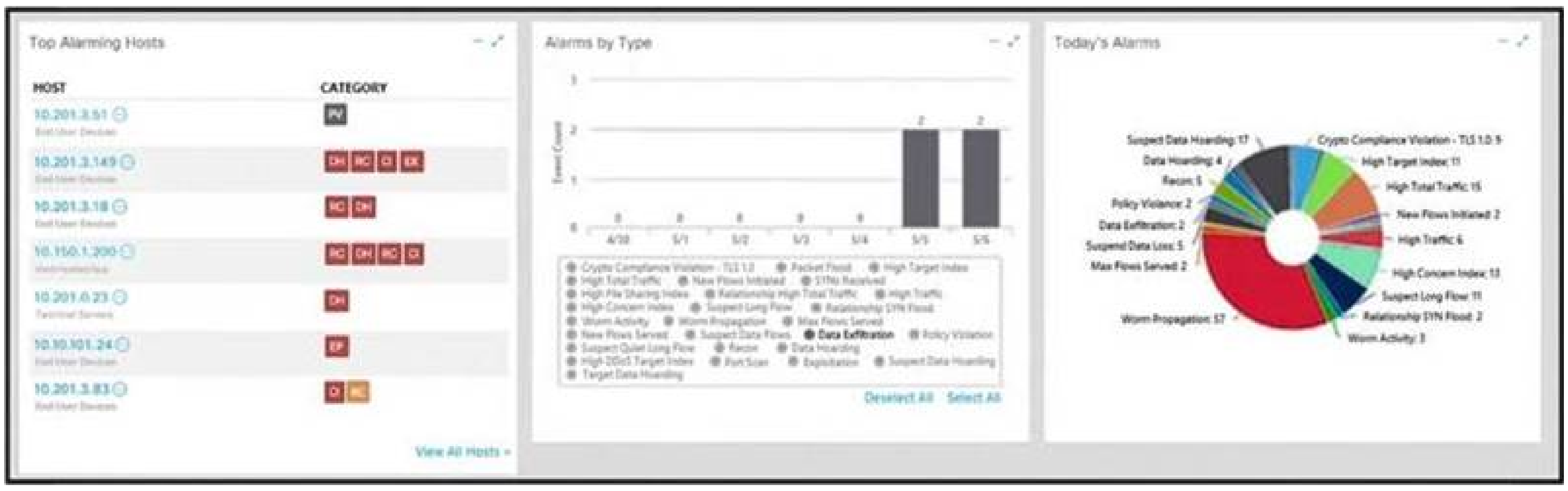
Explanation:
https://explainshell.com/explain?cmd=nmap+-sP

NEW QUESTION 89
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 92
Refer to the exhibit.

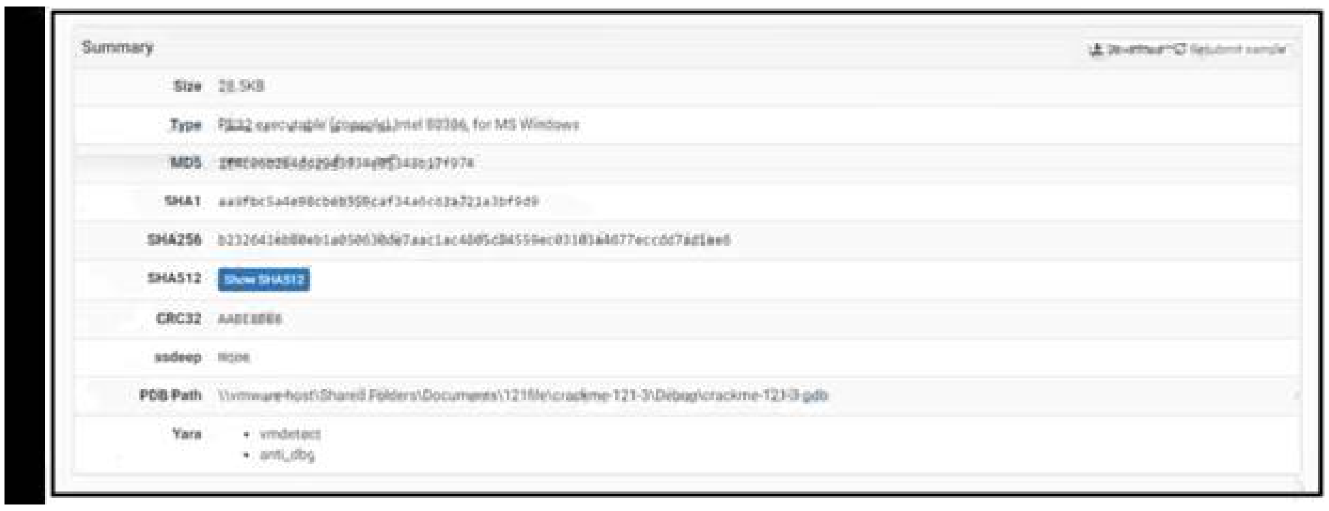


What is the potential threat identified in this Stealthwatch dashboard?

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 93
Refer to the exhibit.


Summary

Download Resubmit sample

Size	28.5KB
Type	PE32 executable (console) Intel 80386, for MS Windows
MD5	2f4c06b2E4dc29d3934a9f343b17f974
SHA1	aa9fbc5a4e98cbeb558caf34a0c83a721a3bf9d9
SHA256	b232641eb80eb1a05063bde7aac1ac4805c84559ec03103a4677eccdd7ad1ee6
SHA512	Show SHA512
CRC32	AABE8BB6
ssdeep	None
PDB Path	\\vmware-host\Shared Folders\Documents\121file\crackme-121-3\Debug\crackme-121-3.pdb
Yara	- vmdetect - anti_dbg

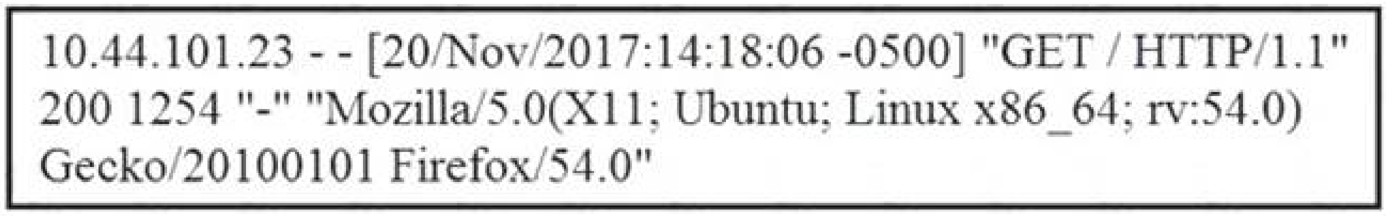
An engineer is reviewing a Cuckoo report of a file. What must the engineer interpret from the report?

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 94
Refer to the exhibit.



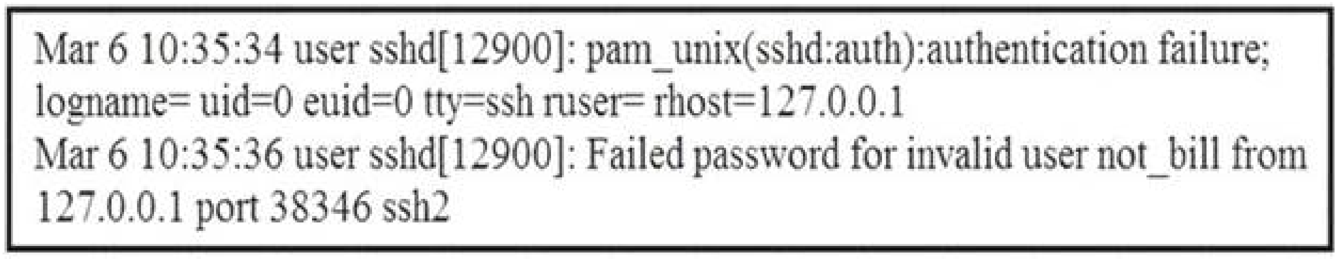
```
10.44.101.23 - - [20/Nov/2017:14:18:06 -0500] "GET / HTTP/1.1"
200 1254 "-" "Mozilla/5.0(X11; Ubuntu; Linux x86_64; rv:54.0)
Gecko/20100101 Firefox/54.0"
```

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 97
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

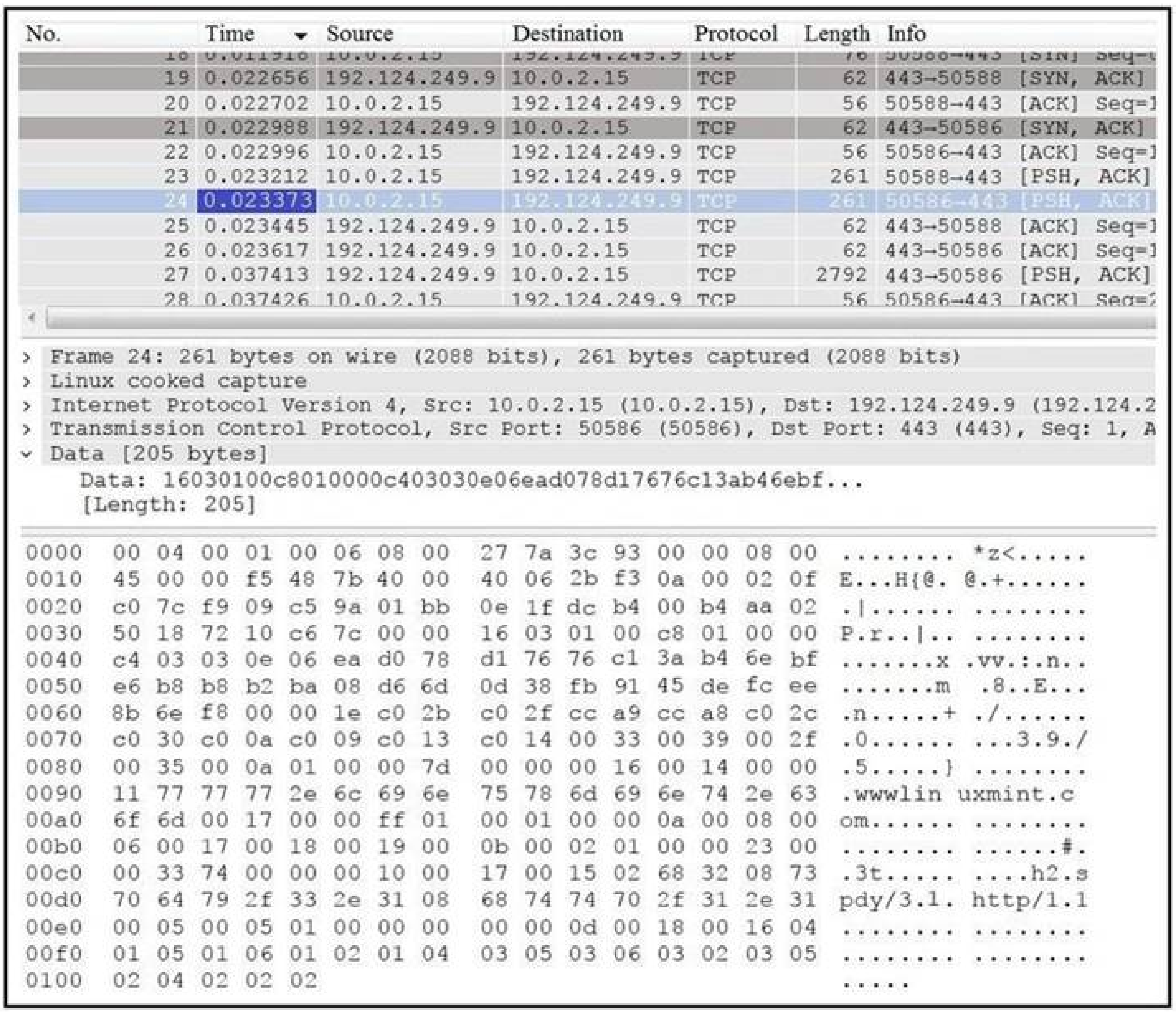
Answer: D

NEW QUESTION 102
Which utility blocks a host portscan?

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

Answer: C

NEW QUESTION 105
Refer to the exhibit.



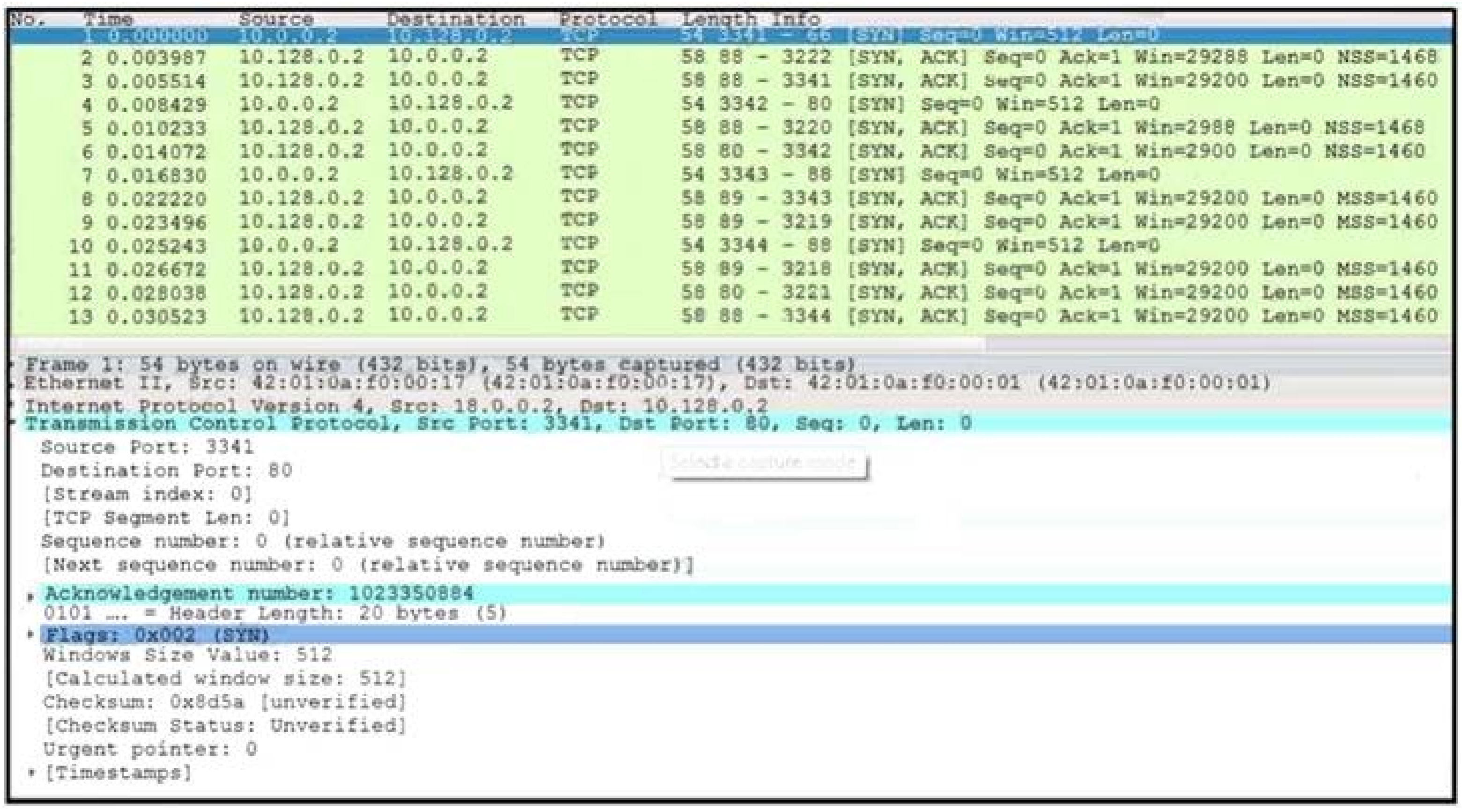
```
No.    Time      Source         Destination    Protocol  Length  Info
   18 0.011918 10.0.2.15      192.124.249.9  TCP         76 50586→443 [SYN] Seq=0
   19 0.022656 192.124.249.9  10.0.2.15      TCP         62 443→50588 [SYN, ACK]
   20 0.022702 10.0.2.15      192.124.249.9  TCP         56 50588→443 [ACK] Seq=1
   21 0.022988 192.124.249.9  10.0.2.15      TCP         62 443→50586 [SYN, ACK]
   22 0.022996 10.0.2.15      192.124.249.9  TCP         56 50586→443 [ACK] Seq=1
   23 0.023212 10.0.2.15      192.124.249.9  TCP        261 50588→443 [PSH, ACK]
   24 0.023373 10.0.2.15      192.124.249.9  TCP        261 50586→443 [PSH, ACK]
   25 0.023445 192.124.249.9  10.0.2.15      TCP         62 443→50588 [ACK] Seq=1
   26 0.023617 192.124.249.9  10.0.2.15      TCP         62 443→50586 [ACK] Seq=1
   27 0.037413 192.124.249.9  10.0.2.15      TCP       2792 443→50586 [PSH, ACK]
   28 0.037426 10.0.2.15      192.124.249.9  TCP         56 50586→443 [ACK] Seq=2

> Frame 24: 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 (192.124.2
> Transmission Control Protocol, Src Port: 50586 (50586), Dst Port: 443 (443), Seq: 1, A
v Data [205 bytes]
    Data: 16030100c8010000c403030e06ead078d17676c13ab46ebf...
    [Length: 205]

0000  00 04 00 01 00 06 08 00  27 7a 3c 93 00 00 08 00   ........ 'z<.....
0010  45 00 00 f5 48 7b 40 00  40 06 2b f3 0a 00 02 0f   E...H{@. @.+.....
0020  c0 7c f9 09 c5 9a 01 bb  0e 1f dc b4 00 b4 aa 02   .|...... ........
0030  50 18 72 10 c6 7c 00 00  16 03 01 00 c8 01 00 00   P.r..|.. ........
0040  c4 03 03 0e 06 ea d0 78  d1 76 76 c1 3a b4 6e bf   .......x .vv.:.n..
0050  e6 b8 b8 b2 ba 08 d6 6d  0d 38 fb 91 45 de fc ee   .......m .8..E...
0060  8b 6e f8 00 00 1e c0 2b  c0 2f cc a9 cc a8 c0 2c   .n.....+ ./......
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/3.1. 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                                     .....
```

Which application protocol is in this PCAP file?

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

Answer: D

NEW QUESTION 110
Refer to the exhibit.



```
No.  Time       Source       Destination  Protocol  Length Info
   1 0.000000   10.0.0.2     10.128.0.2   TCP       54 3341 - 66 [SYN] Seq=0 Win=512 Len=0
   2 0.003987   10.128.0.2   10.0.0.2     TCP       58 88 - 3222 [SYN, ACK] Seq=0 Ack=1 Win=29288 Len=0 NSS=1468
   3 0.005514   10.128.0.2   10.0.0.2     TCP       58 88 - 3341 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 NSS=1460
   4 0.008429   10.0.0.2     10.128.0.2   TCP       54 3342 - 80 [SYN] Seq=0 Win=512 Len=0
   5 0.010233   10.128.0.2   10.0.0.2     TCP       58 88 - 3220 [SYN, ACK] Seq=0 Ack=1 Win=2988 Len=0 NSS=1468
   6 0.014072   10.128.0.2   10.0.0.2     TCP       58 80 - 3342 [SYN, ACK] Seq=0 Ack=1 Win=2900 Len=0 NSS=1460
   7 0.016830   10.0.0.2     10.128.0.2   TCP       54 3343 - 88 [SYN] Seq=0 Win=512 Len=0
   8 0.022220   10.128.0.2   10.0.0.2     TCP       58 89 - 3343 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
   9 0.023496   10.128.0.2   10.0.0.2     TCP       58 89 - 3219 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
  10 0.025243   10.0.0.2     10.128.0.2   TCP       54 3344 - 88 [SYN] Seq=0 Win=512 Len=0
  11 0.026672   10.128.0.2   10.0.0.2     TCP       58 89 - 3218 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
  12 0.028038   10.128.0.2   10.0.0.2     TCP       58 80 - 3221 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
  13 0.030523   10.128.0.2   10.0.0.2     TCP       58 88 - 3344 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460

Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
Ethernet II, Src: 42:01:0a:f0:00:17 (42:01:0a:f0:00:17), Dst: 42:01:0a:f0:00:01 (42:01:0a:f0:00:01)
Internet Protocol Version 4, Src: 18.0.0.2, Dst: 10.128.0.2
Transmission Control Protocol, Src Port: 3341, Dst Port: 80, Seq: 0, Len: 0
  Source Port: 3341
  Destination Port: 80
  [Stream index: 0]
  [TCP Segment Len: 0]
  Sequence number: 0 (relative sequence number)
  [Next sequence number: 0 (relative sequence number)]
 Acknowledgement number: 1023350884
  0101 .... = Header Length: 20 bytes (5)
 Flags: 0x002 (SYN)
  Windows Size Value: 512
  [Calculated window size: 512]
  Checksum: 0x8d5a [unverified]
  [Checksum Status: Unverified]
  Urgent pointer: 0
 [Timestamps]
```

What is occurring in this network traffic?

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

Answer: D

NEW QUESTION 115
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 117
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 120
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 123
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 125
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

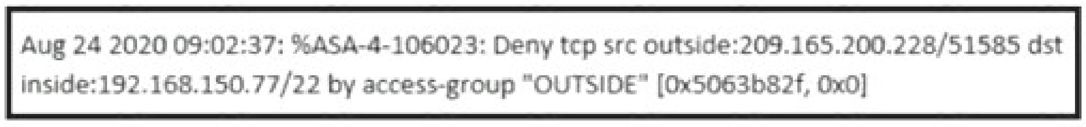
Explanation:
An attack surface is the total sum of vulnerabilities that can be exploited to carry out a security attack. Attack surfaces can be physical or digital. The term attack surface is often confused with the term attack vector, but they are not the same thing. The surface is what is being attacked;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

NEW QUESTION 130
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 134
Refer to the exhibit.



```
Aug 24 2020 09:02:37: %ASA-4-106023: Deny tcp src outside:209.165.200.228/51585 dst
inside:192.168.150.77/22 by access-group "OUTSIDE" [0x5063b82f, 0x0]
```

An analyst received this alert from the Cisco ASA device, and numerous activity logs were produced. How should this type of evidence be categorized?

A. indirect
B. circumstantial
C. corroborative
D. best

Answer: C

Explanation:
Indirect=circumstantail so there is no posibility to match A or B (only one answer is needed in this question). For suer it's not a BEST evidence - this FW data inform only of DROPPED traffic. If smth happend inside network, presented evidence could be used to support other evidences or make our narreation stronger but alone it's mean nothing.

NEW QUESTION 139
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

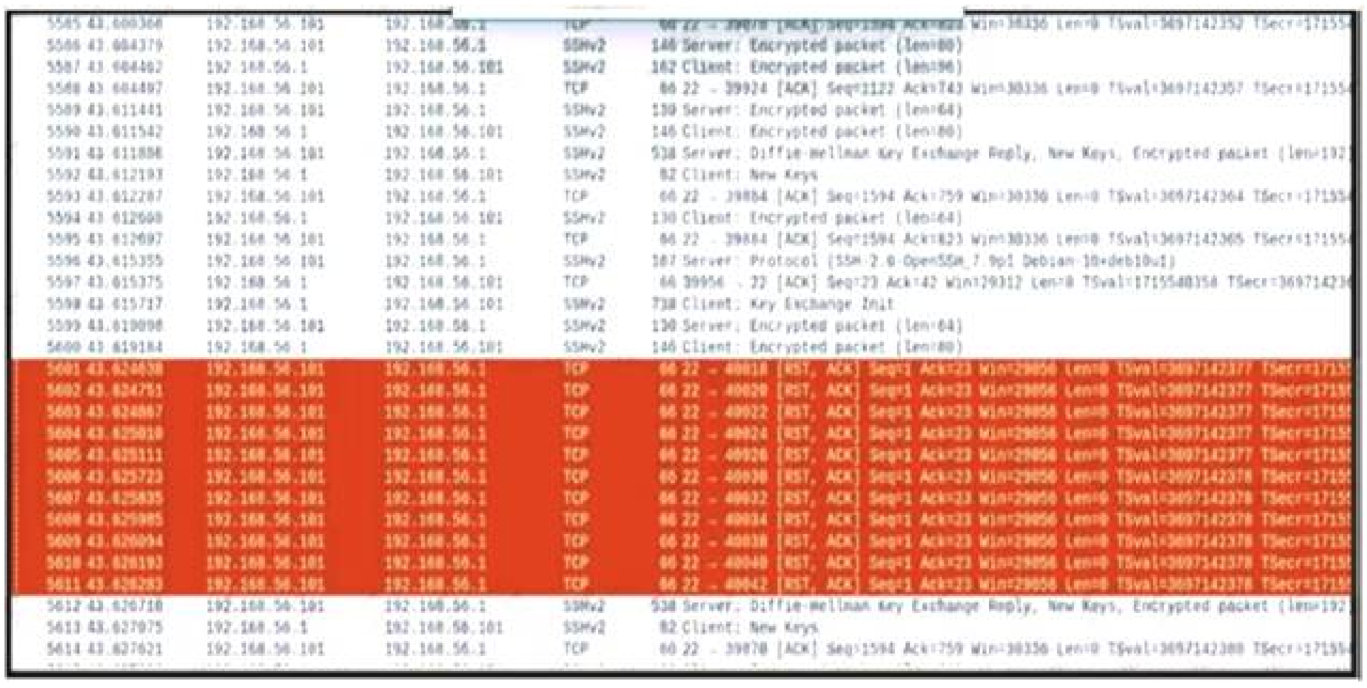
Explanation:
The disk image must be intact for forensics analysis. As a cybersecurity professional, you may be given the task of capturing an image of a disk in a forensic manner. Imagine a security incident has occurred on a system and you are required to perform some forensic investigation to determine 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 142
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, resulting in a potential breach.
B. True positive alerts are blocked by mistake as potential attacks affecting application availability.
C. False positives affect security as no alarm is raised when an attack has taken place, resulting in a potential breach.
D. False positive alerts are blocked by mistake as potential attacks affecting application availability.

Answer: C

NEW QUESTION 146
Refer to the exhibit.



```
5585 43.600360   192.168.56.101   192.168.56.1     TCP     66 22 → 39870 [ACK] Seq=1594 Ack=823 Win=30336 Len=0 TSval=3697142352 TSecr=17155
5586 43.604379   192.168.56.101   192.168.56.1     SSHv2  146 Server: Encrypted packet (len=80)
5587 43.604462   192.168.56.1     192.168.56.101   SSHv2  162 Client: Encrypted packet (len=96)
5588 43.604497   192.168.56.101   192.168.56.1     TCP     66 22 → 39924 [ACK] Seq=1122 Ack=743 Win=30336 Len=0 TSval=3697142357 TSecr=17155
5589 43.611441   192.168.56.101   192.168.56.1     SSHv2  130 Server: Encrypted packet (len=64)
5590 43.611542   192.168.56.1     192.168.56.101   SSHv2  146 Client: Encrypted packet (len=80)
5591 43.611886   192.168.56.101   192.168.56.1     SSHv2  538 Server: Diffie-Hellman Key Exchange Reply, New Keys, Encrypted packet (len=192
5592 43.612193   192.168.56.1     192.168.56.101   SSHv2   82 Client: New Keys
5593 43.612287   192.168.56.101   192.168.56.1     TCP     66 22 → 39864 [ACK] Seq=1594 Ack=759 Win=30336 Len=0 TSval=3697142364 TSecr=17155
5594 43.612600   192.168.56.1     192.168.56.101   SSHv2  130 Client: Encrypted packet (len=64)
5595 43.612697   192.168.56.101   192.168.56.1     TCP     66 22 → 39884 [ACK] Seq=1594 Ack=823 Win=30336 Len=0 TSval=3697142365 TSecr=17155
5596 43.615355   192.168.56.101   192.168.56.1     SSHv2  107 Server: Protocol (SSH-2.0-OpenSSH_7.9p1 Debian-10+deb10u1)
5597 43.615375   192.168.56.1     192.168.56.101   TCP     66 39956 → 22 [ACK] Seq=23 Ack=42 Win=29312 Len=0 TSval=1715540358 TSecr=369714236
5598 43.615717   192.168.56.1     192.168.56.101   SSHv2  738 Client: Key Exchange Init
5599 43.619098   192.168.56.101   192.168.56.1     SSHv2  130 Server: Encrypted packet (len=64)
5600 43.619184   192.168.56.1     192.168.56.101   SSHv2  146 Client: Encrypted packet (len=80)
5601 43.624630   192.168.56.101   192.168.56.1     TCP     66 22 → 40018 [RST, ACK] Seq=1 Ack=23 Win=29056 Len=0 TSval=3697142377 TSecr=1715
5602 43.624751   192.168.56.101   192.168.56.1     TCP     66 22 → 40020 [RST, ACK] Seq=1 Ack=23 Win=29056 Len=0 TSval=3697142377 TSecr=1715
5603 43.624867   192.168.56.101   192.168.56.1     TCP     66 22 → 40022 [RST, ACK] Seq=1 Ack=23 Win=29056 Len=0 TSval=3697142377 TSecr=1715
5604 43.625010   192.168.56.101   192.168.56.1     TCP     66 22 → 40024 [RST, ACK] Seq=1 Ack=23 Win=29056 Len=0 TSval=3697142377 TSecr=1715
5605 43.625111   192.168.56.101   192.168.56.1     TCP     66 22 → 40026 [RST, ACK] Seq=1 Ack=23 Win=29056 Len=0 TSval=3697142377 TSecr=1715
5606 43.625723   192.168.56.101   192.168.56.1     TCP     66 22 → 40030 [RST, ACK] Seq=1 Ack=23 Win=29056 Len=0 TSval=3697142378 TSecr=1715
5607 43.625835   192.168.56.101   192.168.56.1     TCP     66 22 → 40032 [RST, ACK] Seq=1 Ack=23 Win=29056 Len=0 TSval=3697142378 TSecr=1715
5608 43.625985   192.168.56.101   192.168.56.1     TCP     66 22 → 40034 [RST, ACK] Seq=1 Ack=23 Win=29056 Len=0 TSval=3697142378 TSecr=1715
5609 43.626094   192.168.56.101   192.168.56.1     TCP     66 22 → 40038 [RST, ACK] Seq=1 Ack=23 Win=29056 Len=0 TSval=3697142378 TSecr=1715
5610 43.626193   192.168.56.101   192.168.56.1     TCP     66 22 → 40040 [RST, ACK] Seq=1 Ack=23 Win=29056 Len=0 TSval=3697142378 TSecr=1715
5611 43.626283   192.168.56.101   192.168.56.1     TCP     66 22 → 40042 [RST, ACK] Seq=1 Ack=23 Win=29056 Len=0 TSval=3697142378 TSecr=1715
5612 43.626710   192.168.56.101   192.168.56.1     SSHv2  538 Server: Diffie-Hellman Key Exchange Reply, New Keys, Encrypted packet (len=192
5613 43.627075   192.168.56.1     192.168.56.101   SSHv2   82 Client: New Keys
5614 43.627621   192.168.56.101   192.168.56.1     TCP     66 22 → 39870 [ACK] Seq=1594 Ack=759 Win=30336 Len=0 TSval=3697142388 TSecr=17155
```

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 147
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 148
At a company party a guest asks questions about the company’s user account format and password complexity. How is this type of conversation classified?

A. Phishing attack
B. Password Revelation Strategy
C. Piggybacking
D. Social Engineering

Answer: D

NEW QUESTION 153
Which type of evidence supports a theory or an assumption that results from initial evidence?

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

Answer: D

Explanation:
Corroborating evidence (or corroboration) is evidence that tends to support a theory or an assumption deduced by some initial evidence. This corroborating evidence confirms the proposition. Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide

NEW QUESTION 155
Which metric in CVSS indicates an attack that takes a destination bank account number and replaces it with a different bank account number?

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

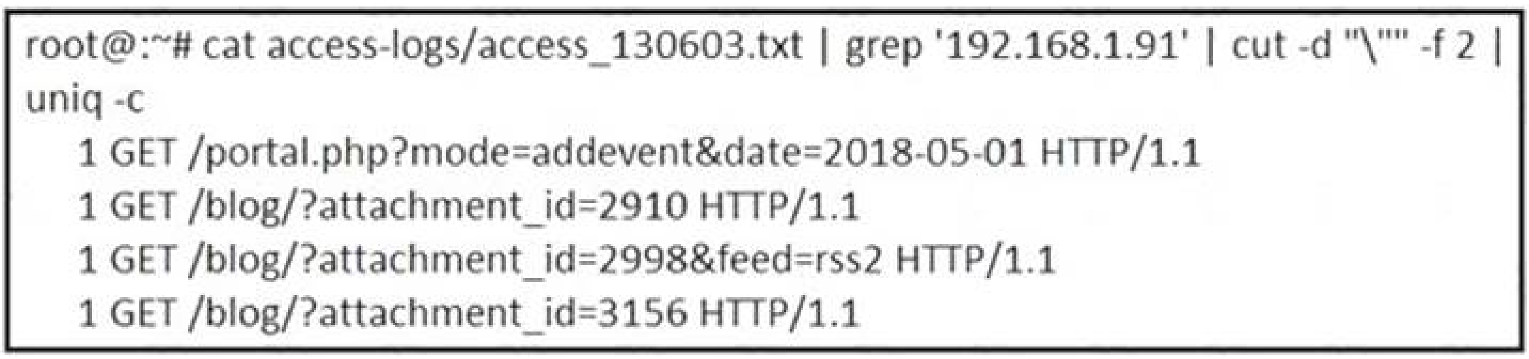
Answer: D

NEW QUESTION 158
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 162
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 163
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 168
Which security monitoring data type requires the largest storage space?

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

Answer: D

NEW QUESTION 169
Which technology should be used to implement a solution that makes routing decisions based on HTTP header, uniform resource identifier, and SSL session ID attributes?

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

Answer: C

Explanation:
Load Balancing: HTTP(S) load balancing is one of the oldest forms of load balancing. This form of load balancing relies on layer 7, which means it operates in the application layer. This allows routing decisions based on attributes like HTTP header, uniform resource identifier, SSL session ID, and HTML form data.
Load balancing applies to layers 4-7 in the seven-layer Open System Interconnection (OSI) model. Its capabilities are: L4. Directing traffic based on network data and transport layer protocols, e.g., IP address and TCP port. L7. Adds content switching to load balancing, allowing routing decisions depending on characteristics such as HTTP header, uniform resource identifier, SSL session ID, and HTML form data. GSLB. Global Server Load Balancing expands L4 and L7 capabilities to servers in different sites

NEW QUESTION 170
An organization has recently adjusted its security stance in response to online threats made by a known hacktivist group.
What is the initial event called in the NIST SP800-61?

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

Answer: B

Explanation:
A precursor is a sign that a cyber-attack is about to occur on a system or network. An indicator is the actual alerts that are generated as an attack is happening. Therefore, as a security professional, it's important to know where you can find both precursor and indicator sources of information.
The following are common sources of precursor and indicator information:

- Security Information and Event Management (SIEM)
- Anti-virus and anti-spam software
- File integrity checking applications/software
- Logs from various sources (operating systems, devices, and applications)
- People who report a security incident https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

NEW QUESTION 175
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 177
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

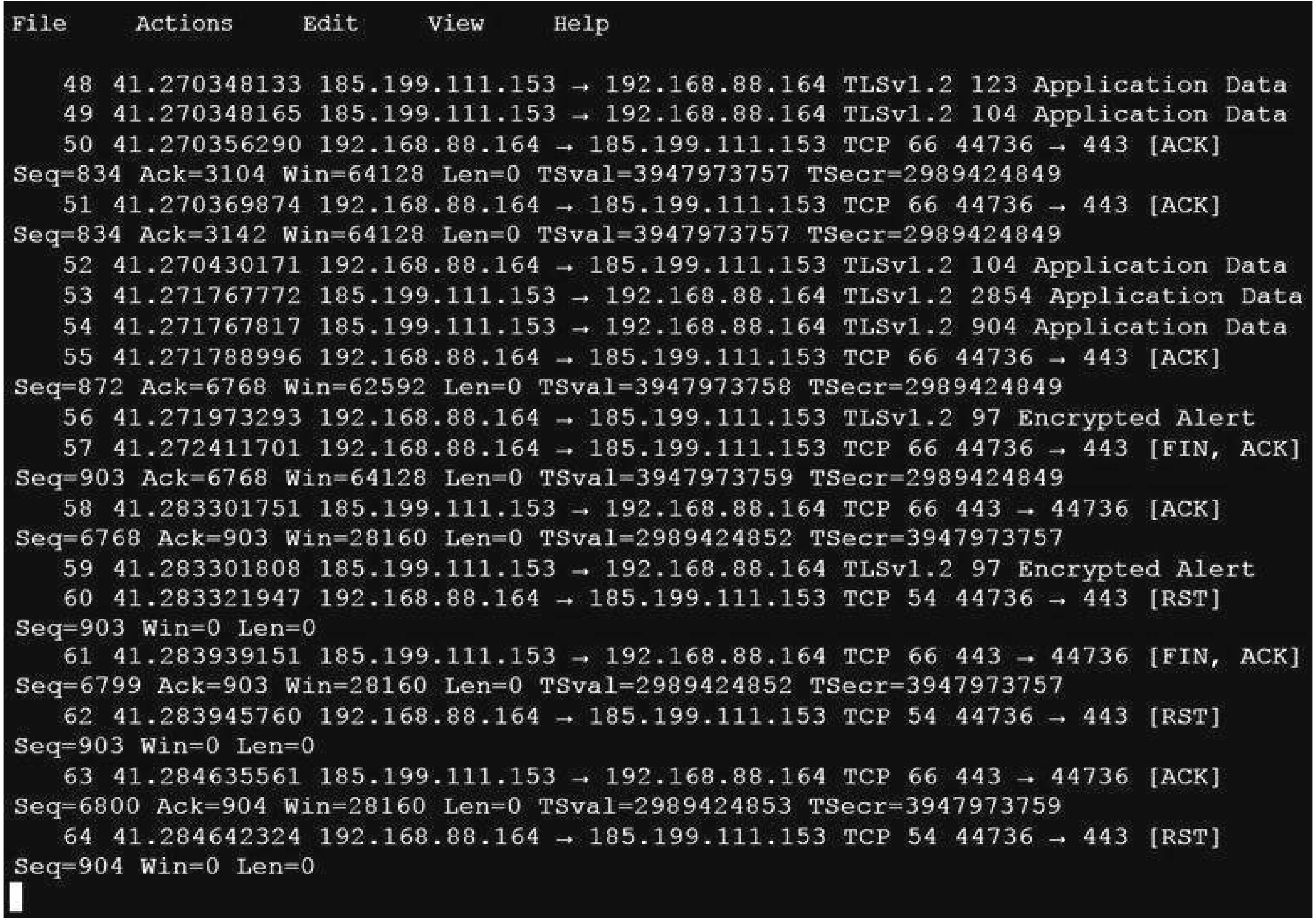
Answer: B

NEW QUESTION 179
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 183
An analyst is investigating a host in the network that appears to be communicating to a command and control server on the Internet. After collecting this packet capture, the analyst cannot determine the technique and payload used for the communication.



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

Which obfuscation technique is the attacker using?

A. Base64 encoding
B. TLS encryption
C. SHA-256 hashing
D. ROT13 encryption

Answer: B

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

NEW QUESTION 187
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 189
What is a description of a social engineering attack?

A. fake offer for free music download to trick the user into providing sensitive data
B. package deliberately sent to the wrong receiver to advertise a new product
C. mistakenly received valuable order destined for another person and hidden on purpose
D. email offering last-minute deals on various vacations around the world with a due date and a counter

Answer: D

NEW QUESTION 193
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
How does a certificate authority impact security?

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

Answer: D

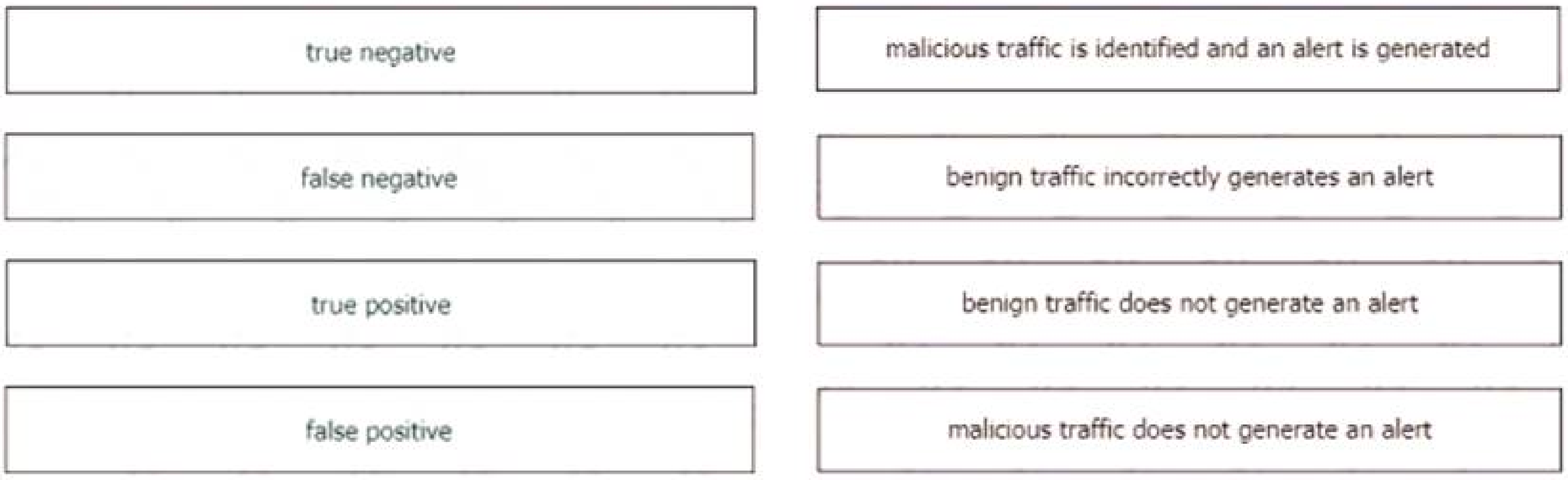
Explanation:
A certificate authority is a computer or entity that creates and issues digital certificates. CA do not "authenticate" it validates. "D" is wrong because The digital certificate validate a user. CA --> DC --> user, server or whatever.

NEW QUESTION 197
Which vulnerability type is used to read, write, or erase information from a database?

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

Answer: D

NEW QUESTION 200
Drag and drop the event term from the left onto the description on the right.

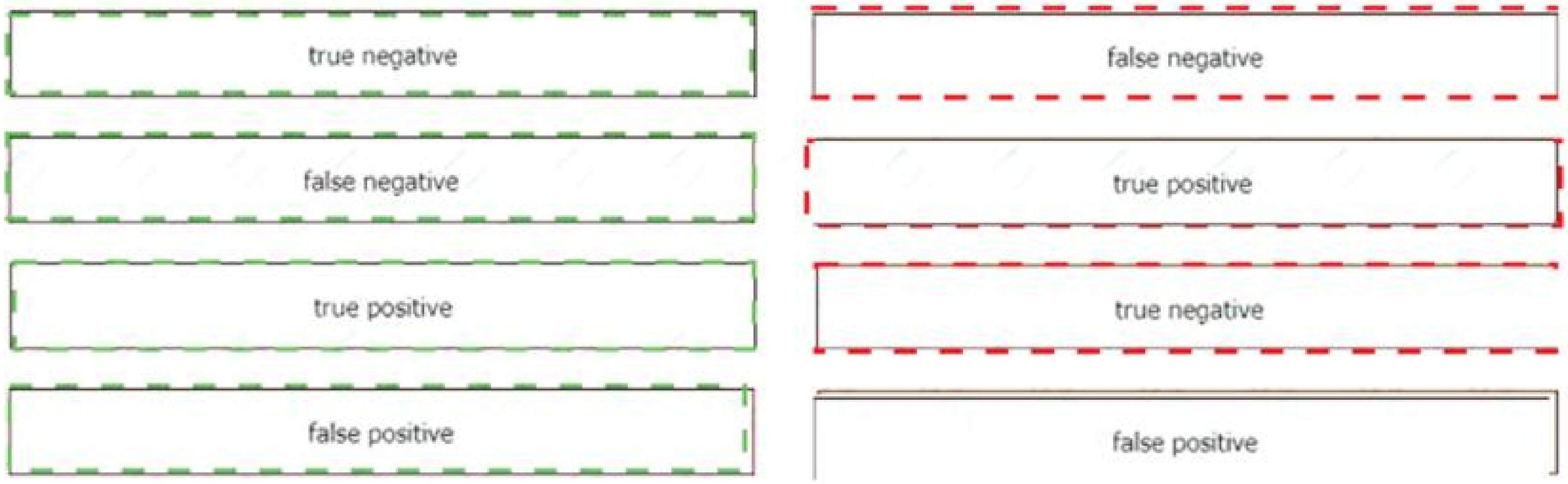


true negative	malicious traffic is identified and an alert is generated
false negative	benign traffic incorrectly generates an alert
true positive	benign traffic does not generate an alert
false positive	malicious traffic does not generate an alert

A. Mastered
B. Not Mastered

Answer: A

Explanation:



true negative	false negative
false negative	true positive
true positive	true negative
false positive	false positive

NEW QUESTION 203
How is attacking a vulnerability categorized?

A. action on objectives

B. delivery
C. exploitation
D. installation

Answer: C

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 208
A threat actor penetrated an organization's network. Using the 5-tuple approach, which data points should the analyst use to isolate the compromised host in a grouped set of logs?

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

Answer: B

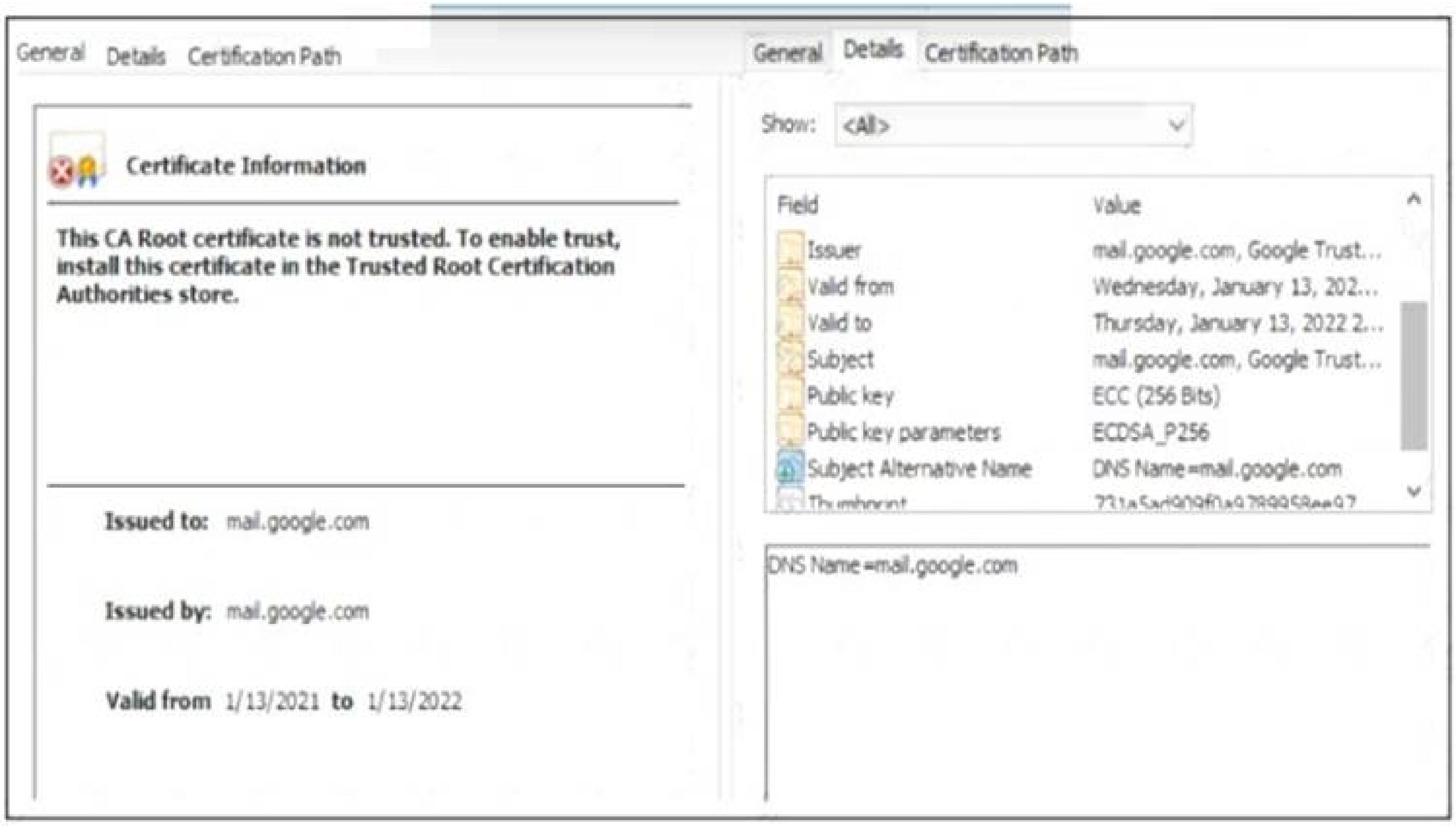
NEW QUESTION 213
Which security model assumes an attacker within and outside of the network and enforces strict verification before connecting to any system or resource within the organization?

A. Biba
B. Object-capability
C. Take-Grant
D. Zero Trust

Answer: D

Explanation:
Zero Trust security is an IT security model that requires strict identity verification for every person and device trying to access resources on a private network, regardless of whether they are sitting within or outside of the network perimeter.

NEW QUESTION 214
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

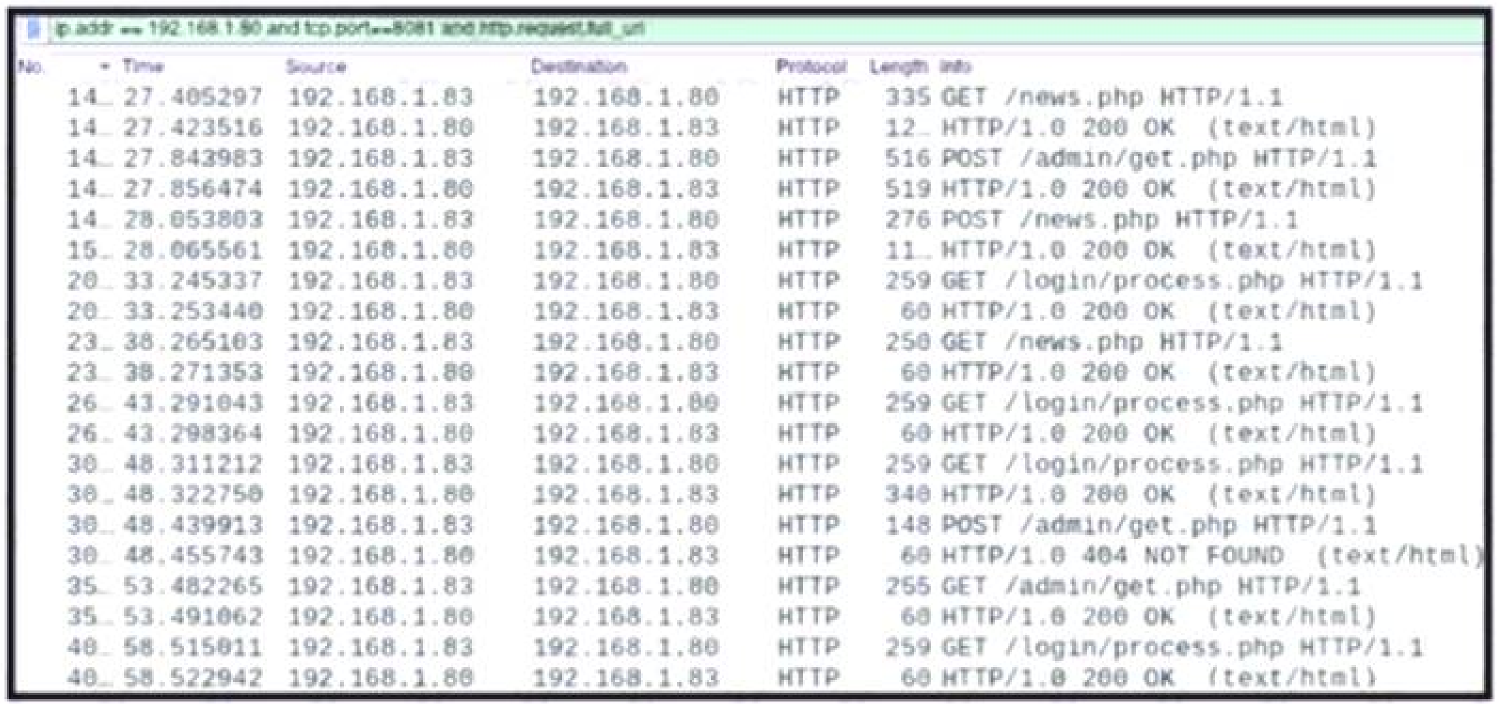
Answer: C

NEW QUESTION 219
What is indicated by an increase in IPv4 traffic carrying protocol 41 ?

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

Answer: D

NEW QUESTION 224
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 229
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 234
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.

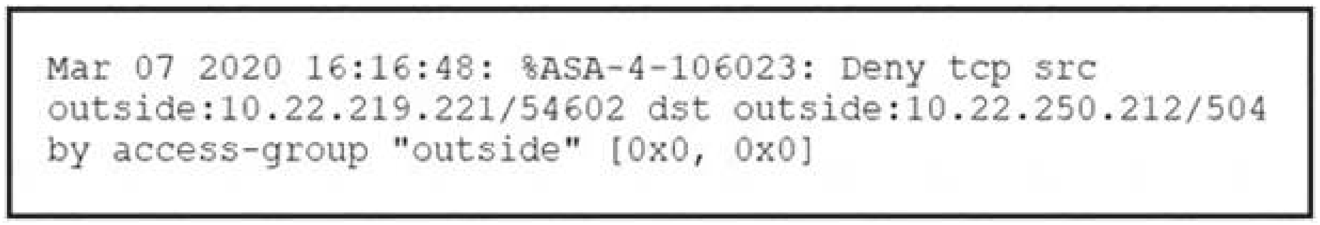
Which component results from this operation?

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 238
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 243
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 248
......