

# Cisco

## Exam Questions 200-201

Understanding Cisco Cybersecurity Operations Fundamentals



### NEW QUESTION 1

Refer to the exhibit.

```
# nmap -sV 172.18.104.139

Starting Nmap 7.01 ( https://nmap.org ) at 2020-03-07 11:36 EST
Nmap scan report for 172.18.104.139
Host is up (0.000018s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
25/tcp    open  smtp      Postfix smtpd
110/tcp   open  pop3      Dovecot pop3d
143/tcp   open  imap      Dovecot imapd
Service Info: Host: 172.18.108.139; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

What does the output indicate about the server with the IP address 172.18.104.139?

- A. open ports of a web server
- B. open port of an FTP server
- C. open ports of an email server
- D. running processes of the server

**Answer: C**

### NEW QUESTION 2

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 3

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 4

What is a difference between SIEM and SOAR?

- A. SOAR predicts and prevents security alerts, while SIEM checks attack patterns and applies the mitigation.
- B. SIEM's primary function is to collect and detect anomalies, while SOAR is more focused on security operations automation and response.
- C. SIEM predicts and prevents security alerts, while SOAR checks attack patterns and applies the mitigation.
- D. SOAR's primary function is to collect and detect anomalies, while SIEM is more focused on security operations automation and response.

**Answer: B**

### NEW QUESTION 5

When communicating via TLS, the client initiates the handshake to the server and the server responds back with its certificate for identification. Which information is available on the server certificate?

- A. server name, trusted subordinate CA, and private key
- B. trusted subordinate CA, public key, and cipher suites
- C. trusted CA name, cipher suites, and private key
- D. server name, trusted CA, and public key

**Answer: D**

### NEW QUESTION 6

Which regex matches only on all lowercase letters?

- A. [az]+

- B. [^az]+
- C. az+
- D. a\*z+

**Answer:** A

#### NEW QUESTION 7

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

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

**Answer:** D

#### NEW QUESTION 8

A security specialist notices 100 HTTP GET and POST requests for multiple pages on the web servers. The agent in the requests contains PHP code that, if executed, creates and writes to a new PHP file on the webserver. Which event category is described?

- A. reconnaissance
- B. action on objectives
- C. installation
- D. exploitation

**Answer:** D

#### NEW QUESTION 9

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

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

**Answer:** D

#### Explanation:

\* 3.3.3 Identifying the Attacking Hosts During incident handling, system owners and others sometimes want to or need to identify the attacking host or hosts.

Although this information can be important, incident handlers should generally stay focused on containment, eradication, and recovery.

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>

The response phase, or containment, of incident response, is the point at which the incident response team begins interacting with affected systems and attempts to keep further damage from occurring as a result of the incident.

#### NEW QUESTION 10

How does certificate authority impact a security system?

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

**Answer:** B

#### NEW QUESTION 10

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 13

What makes HTTPS traffic difficult to monitor?

- A. SSL interception
- B. packet header size
- C. signature detection time
- D. encryption

**Answer:** D

#### NEW QUESTION 14

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 19

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 20

Why is HTTPS traffic difficult to screen?

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

**Answer:** B

#### NEW QUESTION 23

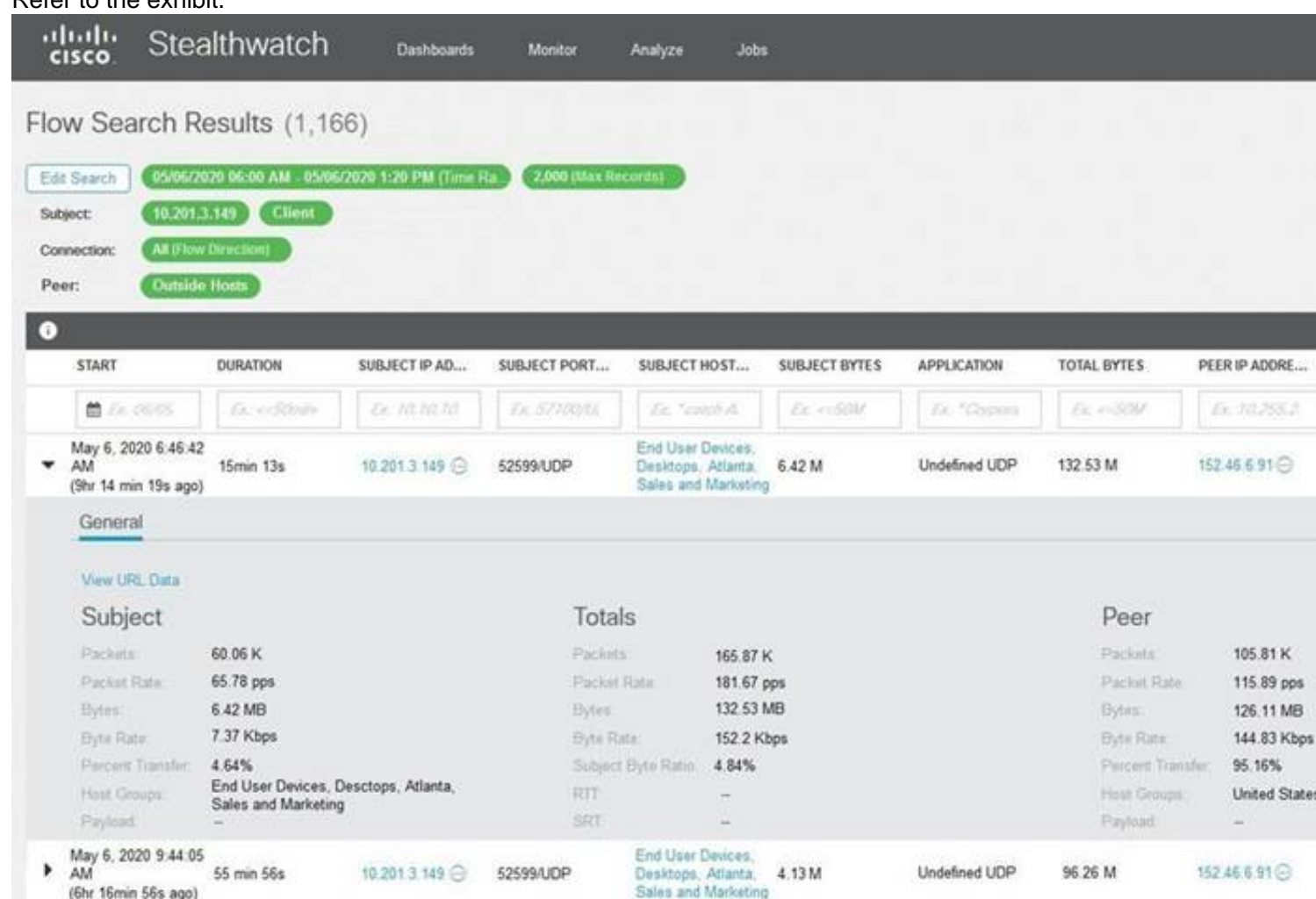
An engineer needs to configure network systems to detect command and control communications by decrypting ingress and egress perimeter traffic and allowing network security devices to detect malicious outbound communications. Which technology should be used to accomplish the task?

- A. digital certificates
- B. static IP addresses
- C. signatures
- D. cipher suite

**Answer:** A

## NEW QUESTION 24

Refer to the exhibit.



The screenshot shows the Cisco Stealthwatch interface. At the top, there's a navigation bar with 'Dashboards', 'Monitor', 'Analyze', and 'Jobs'. Below it, the 'Flow Search Results' section shows 1,166 results. The search filters are: Subject: 10.201.3.149 (Client), Connection: All (Flow Direction), Peer: Outside Hosts. The search criteria bar shows: 05/06/2020 06:00 AM - 05/06/2020 1:20 PM (Time Ra...), 2,000 (Max Records). Below the filters, there's a table of search results. The first result is for May 6, 2020 6:46:42 AM (9hr 14 min 19s ago), with a duration of 15min 13s, subject IP 10.201.3.149, subject port 52599/UDP, subject host 'End User Devices, Desktops, Atlanta, Sales and Marketing', subject bytes 6.42 M, application 'Undefined UDP', total bytes 132.53 M, and peer IP 152.46.6.91. Below the table, there's a 'General' tab with a 'View URL Data' link. The 'General' tab shows three columns: Subject, Totals, and Peer. The Subject column shows: Packets: 60.06 K, Packet Rate: 65.78 pps, Bytes: 6.42 MB, Byte Rate: 7.37 Kbps, Percent Transfer: 4.64%, Host Groups: End User Devices, Desktops, Atlanta, Sales and Marketing, Payload: -. The Totals column shows: Packets: 165.87 K, Packet Rate: 181.67 pps, Bytes: 132.53 MB, Byte Rate: 152.2 Kbps, Subject Byte Ratio: 4.84%, RTT: --, SRT: --. The Peer column shows: Packets: 105.81 K, Packet Rate: 115.89 pps, Bytes: 126.11 MB, Byte Rate: 144.83 Kbps, Percent Transfer: 95.16%, Host Groups: United States, Payload: --.

What is the potential threat identified in this Stealthwatch dashboard?

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

**Answer: D**

## NEW QUESTION 26

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

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

**Answer: A**

## NEW QUESTION 27

An automotive company provides new types of engines and special brakes for rally sports cars. The company has a database of inventions and patents for their engines and technical information Customers can access the database through the company's website after they register and identify themselves. Which type of protected data is accessed by customers?

- A. IP data
- B. PII data
- C. PSI data
- D. PHI data

**Answer: B**

## NEW QUESTION 31

Which two elements are assets in the role of attribution in an investigation? (Choose two.)

- A. context
- B. session
- C. laptop
- D. firewall logs
- E. threat actor

**Answer: CD**

### Explanation:

The following are some factors that are used during attribution in an investigation: Assets, Threat actor, Indicators of Compromise (IoCs), Indicators of Attack (IoAs), Chain of custody Asset: This factor identifies which assets were compromised by a threat actor or hacker. An example of an asset can be an organization's domain controller (DC) that runs Active Directory Domain Services (AD DS). AD is a service that allows an administrator to manage user accounts, user groups, and policies across a Microsoft Windows environment. Keep in mind that an asset is anything that has value to an organization; it can be something physical, digital, or even people. Cisco Certified CyberOps Associate 200-201 Certification Guide

### NEW QUESTION 36

Refer to the exhibit.

TCP	10.114.248.74:80	216.36.50.65:60973	TIME_WAIT
TCP	10.114.248.74:80	216.36.50.65:60974	TIME_WAIT
TCP	10.114.248.74:80	216.36.50.65:60975	TIME_WAIT
TCP	10.114.248.74:80	216.36.50.65:60976	TIME_WAIT
TCP	10.114.248.74:80	216.36.50.65:60977	TIME_WAIT
TCP	10.114.248.74:80	216.36.50.65:60978	TIME_WAIT
TCP	10.114.248.74:80	216.36.50.65:60979	TIME_WAIT
TCP	10.114.248.74:80	216.36.50.65:60980	TIME_WAIT
TCP	10.114.248.74:80	216.36.50.65:60981	TIME_WAIT
TCP	10.114.248.74:80	216.36.50.65:60983	TIME_WAIT
TCP	10.114.248.74:80	216.36.50.65:60984	TIME_WAIT
TCP	10.114.248.74:80	216.36.50.65:60985	TIME_WAIT
TCP	10.114.248.74:80	216.36.50.65:60986	TIME_WAIT
TCP	10.114.248.74:80	216.36.50.65:60987	TIME_WAIT
TCP	10.114.248.74:80	216.36.50.65:60988	TIME_WAIT
TCP	10.114.248.74:80	216.36.50.65:60989	TIME_WAIT
TCP	10.114.248.74:80	216.36.50.65:60990	TIME_WAIT
TCP	10.114.248.74:80	216.36.50.65:60992	TIME_WAIT
TCP	10.114.248.74:80	216.36.50.65:60993	TIME_WAIT
TCP	10.114.248.74:80	216.36.50.65:60994	TIME_WAIT
TCP	10.114.248.74:80	216.36.50.65:60995	TIME_WAIT
TCP	10.114.248.74:80	216.36.50.65:60996	TIME_WAIT
TCP	10.114.248.74:80	216.36.50.65:60997	TIME_WAIT
TCP	10.114.248.74:80	216.36.50.65:60998	TIME_WAIT
TCP	10.114.248.74:80	216.36.50.65:60999	TIME_WAIT

An engineer received a ticket about a slowed-down web application. The engineer runs the `#netstat -an` command. How must the engineer interpret the results?

- A. The web application is receiving a common, legitimate traffic.
- B. The engineer must gather more data.
- C. The web application server is under a denial-of-service attack.
- D. The server is under a man-in-the-middle attack between the web application and its database.

**Answer: C**

### NEW QUESTION 40

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

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

**Answer: A**

#### Explanation:

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

### NEW QUESTION 44

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

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

**Answer: C**

#### Explanation:

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

### NEW QUESTION 46

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 47

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 49

Refer to the exhibit.

No.	Time	Source	Destination	Protocol	Length	Info
27336	245.7615440	192.168.154.129	192.168.154.131	FTP	79	Request: USER bjones
27337	245.7615820	192.168.154.129	192.168.154.131	FTP	79	Request: USER bjones
27338	245.7616210	192.168.154.129	192.168.154.131	FTP	79	Request: USER bjones
27340	245.7616680	192.168.154.129	192.168.154.131	FTP	80	Request: PASS binkley
27343	245.7617170	192.168.154.129	192.168.154.131	FTP	84	Request: PASS bloomcounty
27344	245.7617400	192.168.154.131	192.168.154.129	FTP	100	Response: 331 Please specify the password.
27345	245.7617580	192.168.154.129	192.168.154.131	FTP	78	Request: PASS brown
27346	245.7617890	192.168.154.131	192.168.154.129	FTP	100	Response: 331 Please specify the password.
27347	245.7618140	192.168.154.129	192.168.154.131	FTP	78	Request: PASS bloom
27348	245.7618360	192.168.154.131	192.168.154.129	FTP	100	Response: 331 Please specify the password.
27349	245.7618550	192.168.154.129	192.168.154.131	FTP	80	Request: PASS blondie
27350	245.7618920	192.168.154.129	192.168.154.131	FTP	77	Request: PASS capp
27351	245.7653470	192.168.154.129	192.168.154.131	FTP	79	Request: PASS caucas
27352	245.7692450	192.168.154.129	192.168.154.131	FTP	80	Request: PASS cerebus
27353	245.7693080	192.168.154.129	192.168.154.131	FTP	81	Request: PASS catwoman
27355	245.7771480	192.168.154.131	192.168.154.129	FTP	88	Response: 530 Login incorrect.
27356	245.7772040	192.168.154.131	192.168.154.129	FTP	88	Response: 530 Login incorrect.

An analyst was given a PCAP file, which is associated with a recent intrusion event in the company FTP server Which display filters should the analyst use to filter the FTP traffic?

- A. dstport == FTP
- B. tcp.port==21
- C. tcpport = FTP
- D. dstport = 21

**Answer: B**

#### NEW QUESTION 54

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 58

What is the difference between mandatory access control (MAC) and discretionary access control (DAC)?

- A. MAC is controlled by the discretion of the owner and DAC is controlled by an administrator
- B. MAC is the strictest of all levels of control and DAC is object-based access
- C. DAC is controlled by the operating system and MAC is controlled by an administrator
- D. DAC is the strictest of all levels of control and MAC is object-based access

**Answer: B**

#### NEW QUESTION 62

Which list identifies the information that the client sends to the server in the negotiation phase of the TLS handshake?

- A. ClientStart, ClientKeyExchange, cipher-suites it supports, and suggested compression methods
- B. ClientStart, TLS versions it supports, cipher-suites it supports, and suggested compression methods
- C. ClientHello, TLS versions it supports, cipher-suites it supports, and suggested compression methods



D. ClientHello, ClientKeyExchange, cipher-suites it supports, and suggested compression methods

Answer: C

NEW QUESTION 65

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

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

Answer: AE

Explanation:

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

NEW QUESTION 67

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 69

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 72

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 75

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 78**

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 82**

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 84**

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 89**

Which information must an organization use to understand the threats currently targeting the organization?

- A. threat intelligence
- B. risk scores
- C. vendor suggestions
- D. vulnerability exposure

**Answer:** A

**NEW QUESTION 93**

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 97**

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 102**

According to the September 2020 threat intelligence feeds a new malware called Egregor was introduced and used in many attacks. Distnbution of Egregor is pnmanly through a Cobalt Strike that has been installed on victim's workstations using RDP exploits Malware exfiltrates the victim's data to a command and control server. The data is used to force victims pay or lose it by publicly releasing it. Which type of attack is described?

- A. malware attack
- B. ransomware attack
- C. whale-phishing
- D. insider threat

Answer: B

**NEW QUESTION 105**

Drag and drop the security concept on the left onto the example of that concept on the right.

Risk Assessment	network is compromised
Vulnerability	lack of an access list
Exploit	configuration review
Threat	leakage of confidential information

- A. Mastered
- B. Not Mastered

Answer: A

**Explanation:**

Risk Assessment	Threat
Vulnerability	Vulnerability
Exploit	Risk Assessment
Threat	Exploit

#### NEW QUESTION 109

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 111

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

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

**Answer: A**

#### Explanation:

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

Ref: Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide

#### NEW QUESTION 115

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 120

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: 08:0C: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 port 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 123

Drag and drop the uses on the left onto the type of security system on the right.

ensures protection of individual devices

detects intrusion attempts

monitors host for suspicious activity

monitors incoming traffic and connections

Endpoint

Network

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

ensures protection of individual devices

detects intrusion attempts

monitors host for suspicious activity

monitors incoming traffic and connections

Endpoint

ensures protection of individual devices

monitors incoming traffic and connections

Network

detects intrusion attempts

monitors host for suspicious activity

NEW QUESTION 127

Which technology prevents end-device to end-device IP traceability?

- A. encryption
- B. load balancing
- C. NAT/PAT
- D. tunneling

Answer: C

NEW QUESTION 129

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

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

Answer: D

NEW QUESTION 131

What describes the defense-m-depth principle?

- A. defining precise guidelines for new workstation installations
- B. categorizing critical assets within the organization
- C. isolating guest Wi-Fi from the focal network
- D. implementing alerts for unexpected asset malfunctions

Answer: B

NEW QUESTION 132

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 136**

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 139**

Which type of access control depends on the job function of the user?

- A. discretionary access control
- B. nondiscretionary access control
- C. role-based access control
- D. rule-based access control

**Answer:** C

**NEW QUESTION 141**

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

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

**Answer:** C

**NEW QUESTION 146**

Drag and drop the access control models from the left onto the correct descriptions on the right.

MAC	object owner determines permissions
ABAC	OS determines permissions
RBAC	role of the subject determines permissions
DAC	attributes of the subject determines permissions

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

MAC	DAC
ABAC	MAC
RBAC	RBAC
DAC	ABAC

NEW QUESTION 148

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 149

What is the function of a command and control server?

- A. It enumerates open ports on a network device
- B. It drops secondary payload into malware
- C. It is used to regain control of the network after a compromise
- D. It sends instruction to a compromised system

Answer: D

NEW QUESTION 153

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 156

What is personally identifiable information that must be safeguarded from unauthorized access?

- A. date of birth
- B. driver's license number
- C. gender
- D. zip code

Answer: B

Explanation:

According to the Executive Office of the President, Office of Management and Budget (OMB), and the U.S. Department of Commerce, Office of the Chief Information Officer, PII refers to “information which can be used to distinguish or trace an individual’s identity.”

The following are a few examples:

- An individual’s name
- Social security number
- Biological or personal characteristics, such as an image of distinguishing features, fingerprints, Xrays, voice signature, retina scan, and the geometry of the face
- Date and place of birth
- Mother’s maiden name
- Credit card numbers
- Bank account numbers
- Driver license number
- Address information, such as email addresses or street addresses, and telephone numbers for businesses or personal use
- Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide Omar Santos

NEW QUESTION 161

Refer to the exhibit.



```
Capturing on 'eth0'

 1 0.0000000000 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 163

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 164

Refer to the exhibit.

Internet Address	Physical Address	Type
192.168.1.10	d8-a7-56-d7-19-ea	dynamic
192.168.1.67	d8-a7-56-d7-19-ea	dynamic
192.168.1.1	01-00-5e-00-00-16	static

What is occurring in this network?

- A. ARP cache poisoning
- B. DNS cache poisoning
- C. MAC address table overflow
- D. MAC flooding attack

**Answer: A**

#### NEW QUESTION 166

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 170

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 175

Which NIST IR category stakeholder is responsible for coordinating incident response among various business units, minimizing damage, and reporting to regulatory agencies?

- A. CSIRT



- B. PSIRT
- C. public affairs
- D. management

**Answer:** D

**NEW QUESTION 180**

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 181**

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

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

**Answer:** C

**Explanation:**

User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:12.0) Gecko/20100101 Firefox/12.0 In computing, a user agent is any software, acting on behalf of a user, which "retrieves, renders and facilitates end-user interaction with Web content".[1] A user agent is therefore a special kind of software agent.

[https://en.wikipedia.org/wiki/User\\_agent#User\\_agent\\_identification](https://en.wikipedia.org/wiki/User_agent#User_agent_identification)

A user agent is a computer program representing a person, for example, a browser in a Web context. [https://developer.mozilla.org/en-US/docs/Glossary/User\\_agent](https://developer.mozilla.org/en-US/docs/Glossary/User_agent)

**NEW QUESTION 183**

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 external 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 186**

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 188**

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 189**

Refer to the exhibit.

```
192.168.10.10 -- [01/Dec/2020:11:12:22 -0200] "GET /icons/powered_by_rh.png HTTP/1.1" 200 1213 "http://192.168.0.102/" "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/2020:11:13:15 -0200] "GET /favicon.ico HTTP/1.1" 404 288 "-" "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 Entities attack
- C. Insecure Deserialization
- D. Regular GET requests

**Answer:** A

#### NEW QUESTION 194

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

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

**Answer:** C

#### NEW QUESTION 195

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

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

**Answer:** CE

#### NEW QUESTION 200

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 203

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 204

What are two social engineering techniques? (Choose two.)

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

**Answer:** CE

#### NEW QUESTION 205

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

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

**Answer:** A

#### NEW QUESTION 208

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](https://docs.legato.io/16_10/basicIPC.html)

#### NEW QUESTION 210

Which attack method intercepts traffic on a switched network?

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

**Answer:** B

#### Explanation:

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

#### NEW QUESTION 215

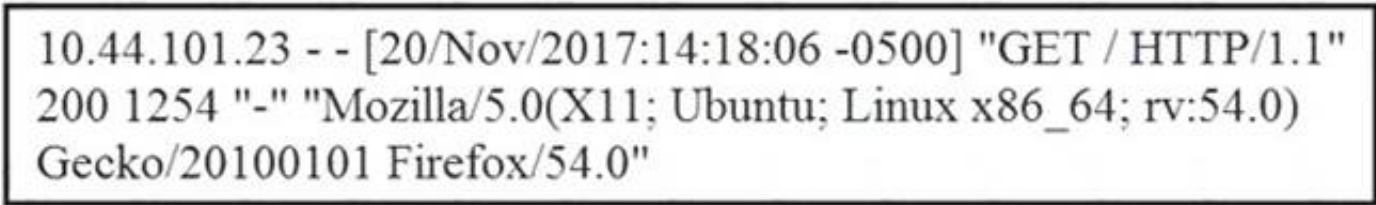
What should an engineer use to aid the trusted exchange of public keys between user tom0411976943 and dan1968754032?

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

**Answer:** C

#### NEW QUESTION 220

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 225

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

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

Answer: C

**NEW QUESTION 228**

Refer to the exhibit.



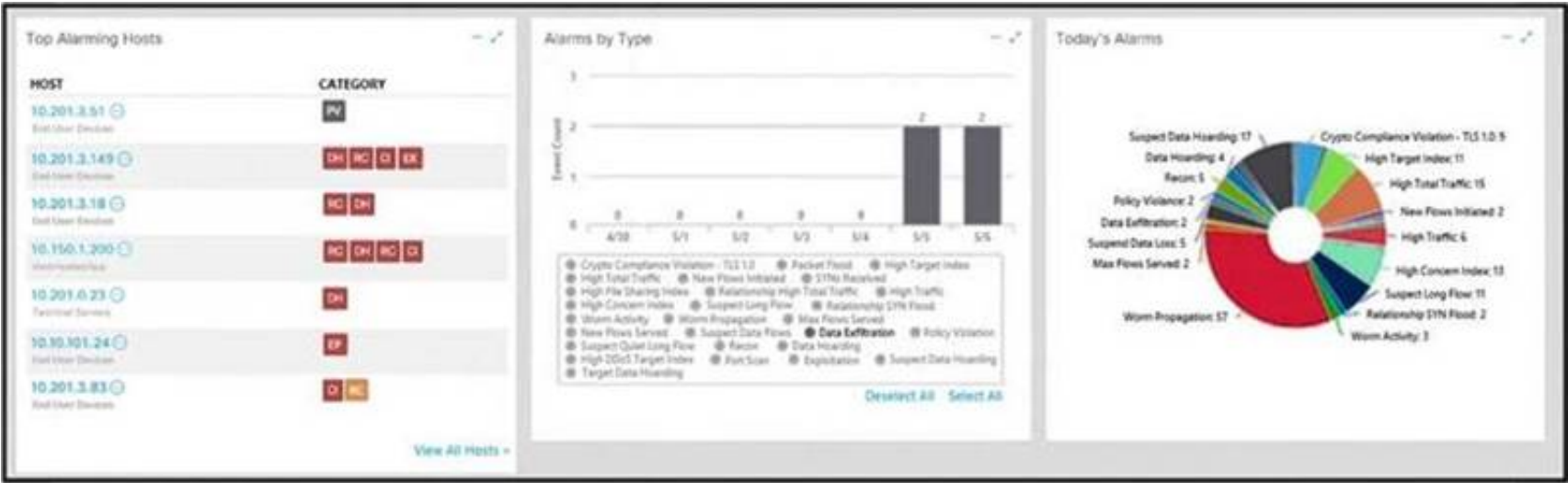
An engineer is reviewing a Cuckoo report of a file. What must the engineer interpret from the report?

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

Answer: B

**NEW QUESTION 232**

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 233**

What is the practice of giving an employee access to only the resources needed to accomplish their job?

- A. principle of least privilege
- B. organizational separation
- C. separation of duties
- D. need to know principle

Answer: A

**NEW QUESTION 237**

Drag and drop the security concept from the left onto the example of that concept on the right.



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

- A. Mastered  
B. Not Mastered

Answer: A

Explanation:  
Table Description automatically generated

NEW QUESTION 239  
Drag and drop the technology on the left onto the data type the technology provides on the right.

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

- A. Mastered  
B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 242  
Which utility blocks a host portscan?

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

Answer: C

NEW QUESTION 243  
Which two elements are used for profiling a network? (Choose two.)

- A. session duration  
B. total throughput  
C. running processes

- D. listening ports
- E. OS fingerprint

**Answer:** AB

**Explanation:**

A network profile should include some important elements, such as the following:

Total throughput – the amount of data passing from a given source to a given destination in a given period of time

Session duration – the time between the establishment of a data flow and its termination Ports used – a list of TCP or UDP processes that are available to accept data

Critical asset address space – the IP addresses or the logical location of essential systems or data

Profiling data are data that system has gathered, these data helps for incident response and to detect incident Network profiling = throughput, sessions duration, port used, Critical Asset Address Space Host profiling = Listening ports, logged in accounts, running processes, running tasks, applications

**NEW QUESTION 246**

What is the difference between a threat and an exploit?

- A. A threat is a result of utilizing flow in a system, and an exploit is a result of gaining control over the system.
- B. A threat is a potential attack on an asset and an exploit takes advantage of the vulnerability of the asset
- C. An exploit is an attack vector, and a threat is a potential path the attack must go through.
- D. An exploit is an attack path, and a threat represents a potential vulnerability

**Answer:** B

**NEW QUESTION 250**

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 253**

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 engages in identification and selection of targets.	reconnaissance
An exploit is coupled with a remote access trojan.	weaponization
The weapon is transferred to the target environment.	delivery

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Delivery: This step involves transmitting the weapon to the target.

Weaponization: In this step, the intruder creates a malware weapon like a virus, worm or such in order to exploit the vulnerabilities of the target. Depending on the target and the purpose of the attacker, this malware can exploit new, undetected vulnerabilities (also known as the zero-day exploits) or it can focus on a combination of different vulnerabilities.

Reconnaissance: In this step, the attacker / intruder chooses their target. Then they conduct an in-depth research on this target to identify its vulnerabilities that can be exploited.

**NEW QUESTION 254**

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 259**

Refer to the exhibit.

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

Which type of log is displayed?

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

**Answer: A**

**Explanation:**

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

**NEW QUESTION 263**

Refer to the exhibit.

<b>File name</b>	CVE-2009-4324 PDF 2009-11-30 note200911.pdf
<b>File size</b>	400918 bytes
<b>File type</b>	PDF document, version 1.6
<b>CRC32</b>	11638A9B
<b>MD5</b>	61baabd6fc12e01ff73ceacc07c84f9a
<b>SHA1</b>	0805d0ae62f5358b9a3f4c1868d552fc3561b17
<b>SHA256</b>	27cced58a0fcbb0bbe3894f74d3014611039fefdf3bd2b0ba7ad85b18194c
<b>SHA512</b>	5a43bc7eef279b209e2590432cc3e2eb480d0f78004e265f00b98b4afdc9a
<b>Ssdeep</b>	1536:p0AAH2KthGBjcdBj8VETeePxsT65ZZ3pdx/ves/QR/875+prahGV6B
<b>PEID</b>	None matched
<b>Yara</b>	<ul style="list-style-type: none"> <li>• embedded_pe (Contains an embedded PE32 file)</li> <li>• embedded_win_api (A non-Windows executable contains win32 API)</li> <li>• vmdetect (Possibly employs anti-virtualization techniques)</li> </ul>
<b>Virus Total</b>	<a href="#">Permalink</a> VirusTotal Scan Date: 2013-12-27 06:51:52 Detection Rate: 32/46 ( <a href="#">collapse</a> )

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 264**

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 265**

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

**NEW QUESTION 269**

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 273**

Which two pieces of information are collected from the IPv4 protocol header? (Choose two.)

- A. UDP port to which the traffic is destined
- B. TCP port from which the traffic was sourced
- C. source IP address of the packet
- D. destination IP address of the packet
- E. UDP port from which the traffic is sourced

**Answer: CD**

**NEW QUESTION 277**

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 281**

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 283**

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 286

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:

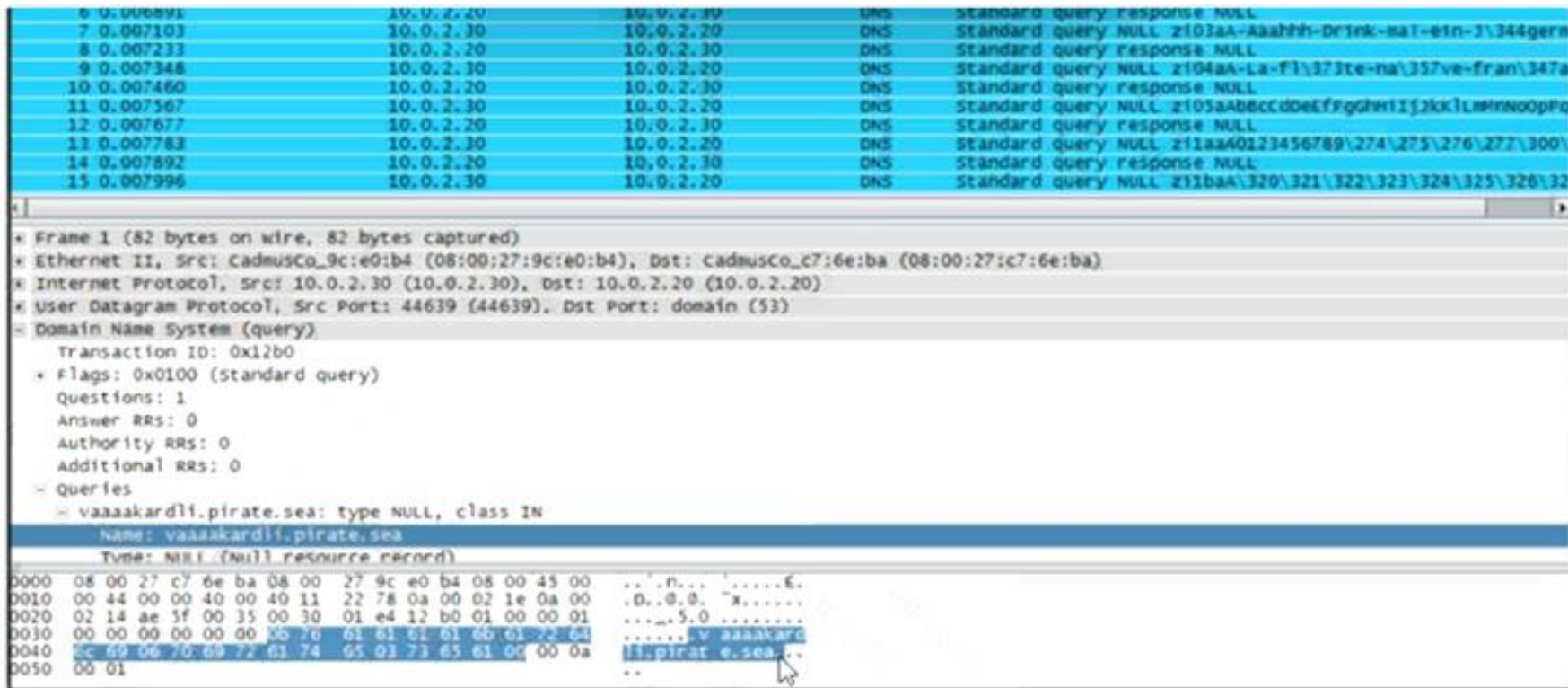
A precursor is a sign that a cyber-attack is about to occur on a system or network. An indicator is the actual alerts that are generated as an attack is happening. Therefore, as a security professional, it's important to know where you can find both precursor and indicator sources of information.

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 289

Refer to the exhibit.



What is occurring?

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

**Answer: D**

#### NEW QUESTION 291

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 296

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 300

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 304**

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 306**

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 308**

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 309**

What is a purpose of a vulnerability management framework?

- A. identifies, removes, and mitigates system vulnerabilities
- B. detects and removes vulnerabilities in source code
- C. conducts vulnerability scans on the network
- D. manages a list of reported vulnerabilities

**Answer:** A

#### **NEW QUESTION 310**

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

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

**Answer:** D

#### **NEW QUESTION 313**

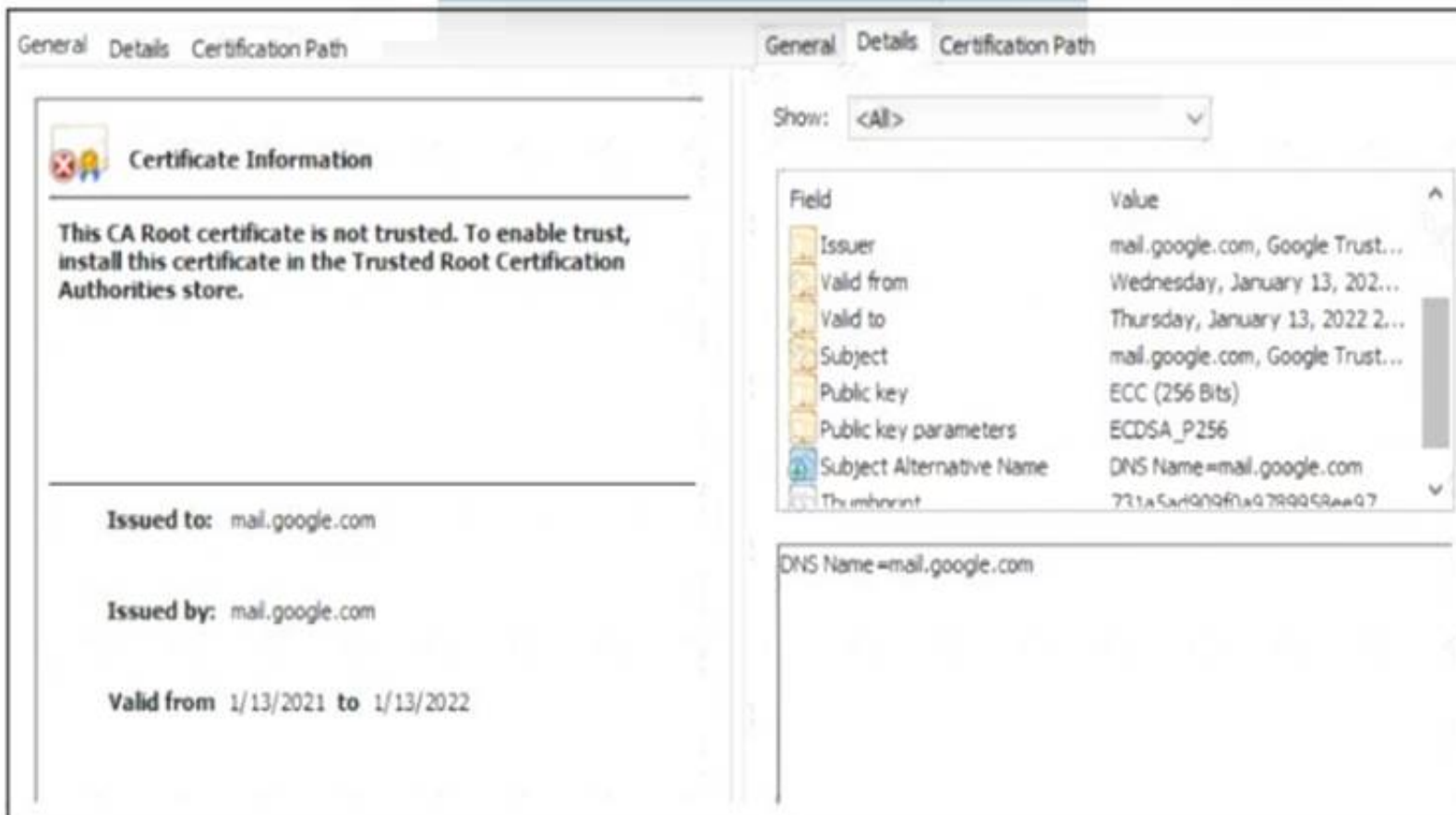
How is attacking a vulnerability categorized?

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

**Answer:** C

#### **NEW QUESTION 314**

Refer to the exhibit.



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

- A. DNS hijacking attack
- B. Endpoint local time is invalid.
- C. Certificate is not in trusted roots.
- D. man-in-the-middle attack

**Answer: C**

#### NEW QUESTION 318

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 323

Refer to the exhibit.

No.	Time	Source	Destination	Protocol	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-B09F-4B7C-B722-948D6CF16174}, 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 325

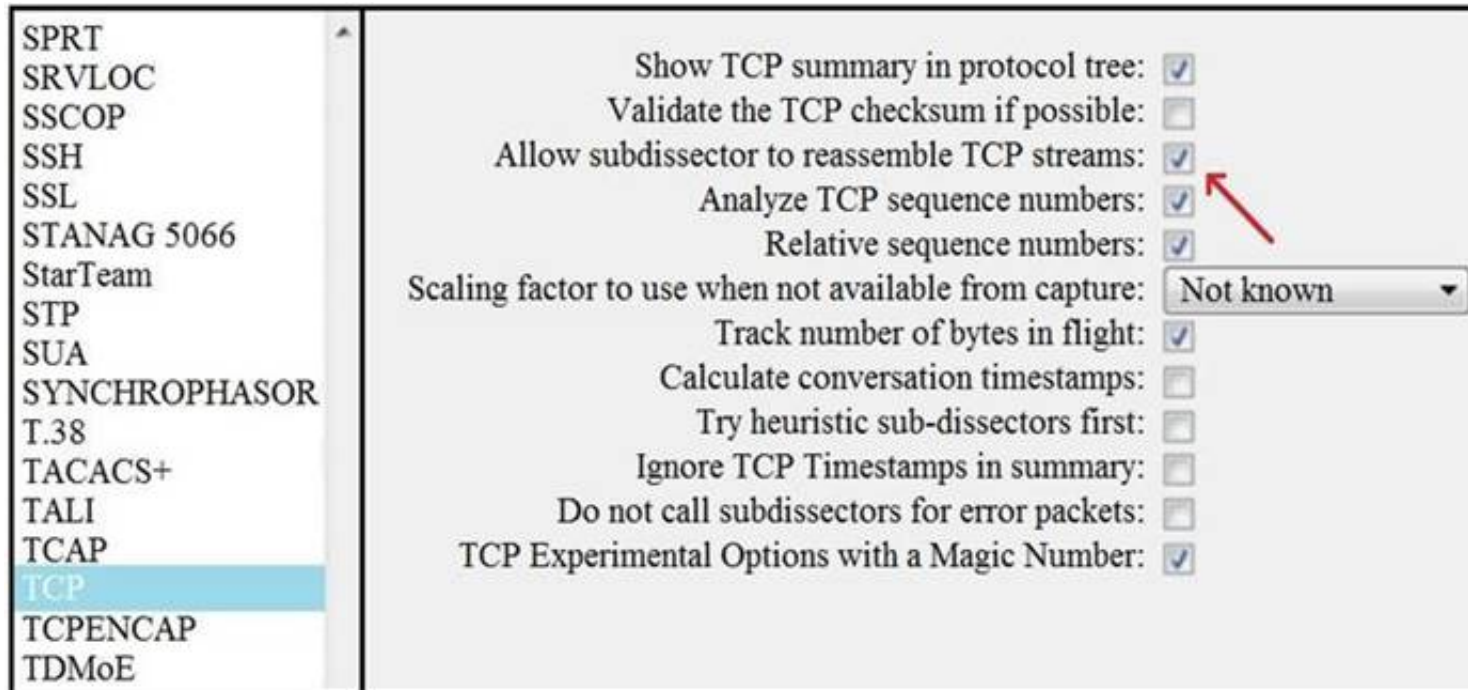
An organization is cooperating with several third-party companies. Data exchange is on an unsecured channel using port 80 Internal employees use the FTP service to upload and download sensitive data An engineer must ensure confidentiality while preserving the integrity of the communication. Which technology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

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

Answer: A

#### NEW QUESTION 330

Refer to the exhibit.



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

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

Answer: D

#### NEW QUESTION 332

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 333

What is the difference between indicator of attack (IoA) and indicators of compromise (IoC)?

- A. IoA is the evidence that a security breach has occurred, and IoC allows organizations to act before the vulnerability can be exploited.
- B. IoA refers to the individual responsible for the security breach, and IoC refers to the resulting loss.
- C. IoC is the evidence that a security breach has occurred, and IoA allows organizations to act before the vulnerability can be exploited.
- D. IoC refers to the individual responsible for the security breach, and IoA refers to the resulting loss.

Answer: C

#### NEW QUESTION 336

Refer to the exhibit.



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 339

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 340

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 345

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

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

**Answer: B**

**NEW QUESTION 346**

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

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

**Answer:** D

**NEW QUESTION 348**

.....

## Thank You for Trying Our Product

### We offer two products:

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

2nd - Questions and Answers in PDF Format

### 200-201 Practice Exam Features:

- \* 200-201 Questions and Answers Updated Frequently
- \* 200-201 Practice Questions Verified by Expert Senior Certified Staff
- \* 200-201 Most Realistic Questions that Guarantee you a Pass on Your First Try
- \* 200-201 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The 200-201 Practice Test Here](#)**