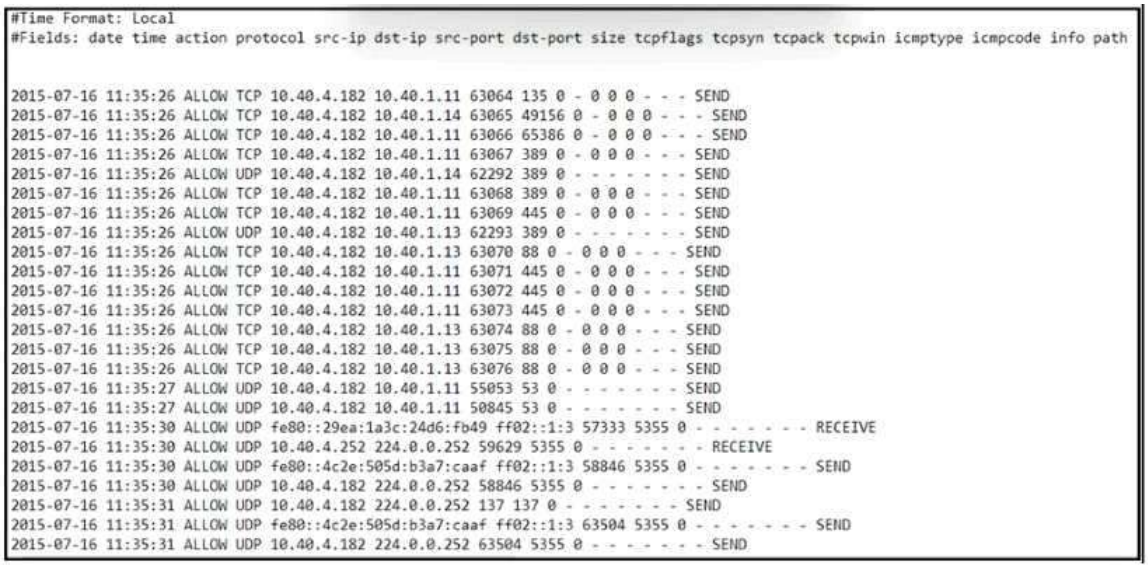
QUESTION 201
What is a difference between signature-based and behavior-based detection?

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/

QUESTION 202
Refer to the exhibit. An engineer received an event log file to review.
Which technology generated the log?



```
#Time Format: Local
#Fields: date time action protocol src-ip dst-ip src-port dst-port size tcpflags tcpsyn tcpack tcpwin icmptype icmpcode info path


2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63064 135 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.14 63065 49156 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63066 65386 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63067 389 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW UDP 10.40.4.182 10.40.1.14 62292 389 0 - - - - - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63068 389 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63069 445 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW UDP 10.40.4.182 10.40.1.13 62293 389 0 - - - - - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.13 63070 88 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63071 445 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63072 445 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63073 445 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.13 63074 88 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.13 63075 88 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.13 63076 88 0 - 0 0 0 - - - SEND
2015-07-16 11:35:27 ALLOW UDP 10.40.4.182 10.40.1.11 55053 53 0 - - - - - - - SEND
2015-07-16 11:35:27 ALLOW UDP 10.40.4.182 10.40.1.11 50845 53 0 - - - - - - - SEND
2015-07-16 11:35:30 ALLOW UDP fe80::29ea:1a3c:24d6:fb49 ff02::1:3 57333 5355 0 - - - - - - - RECEIVE
2015-07-16 11:35:30 ALLOW UDP 10.40.4.252 224.0.0.252 59629 5355 0 - - - - - - - RECEIVE
2015-07-16 11:35:30 ALLOW UDP fe80::4c2e:505d:b3a7:caaf ff02::1:3 58846 5355 0 - - - - - - - SEND
2015-07-16 11:35:30 ALLOW UDP 10.40.4.182 224.0.0.252 58846 5355 0 - - - - - - - SEND
2015-07-16 11:35:31 ALLOW UDP 10.40.4.182 224.0.0.252 137 137 0 - - - - - - - SEND
2015-07-16 11:35:31 ALLOW UDP fe80::4c2e:505d:b3a7:caaf ff02::1:3 63504 5355 0 - - - - - - - SEND
2015-07-16 11:35:31 ALLOW UDP 10.40.4.182 224.0.0.252 63504 5355 0 - - - - - - - SEND
```

A. NetFlow
B. proxy
C. firewall
D. IDS/IPS

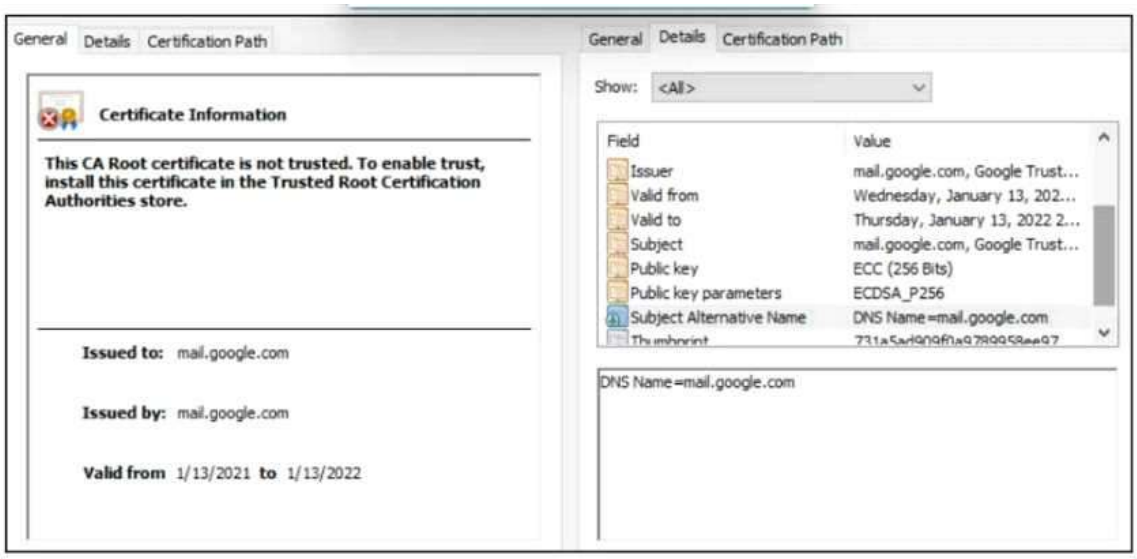
Answer: C

QUESTION 203
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

QUESTION 204
Refer to the exhibit. A company employee is connecting to mail google.com from an endpoint device. The website is loaded but with an error. What is occurring?



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

Answer: C

QUESTION 205
An analyst is using the SIEM platform and must extract a custom property from a Cisco device and capture the phrase, "File: Clean." Which regex must the analyst import?

A. File: Clean
B. ^Parent File Clean$
C. File: Clean (.*)
D. ^File: Clean$

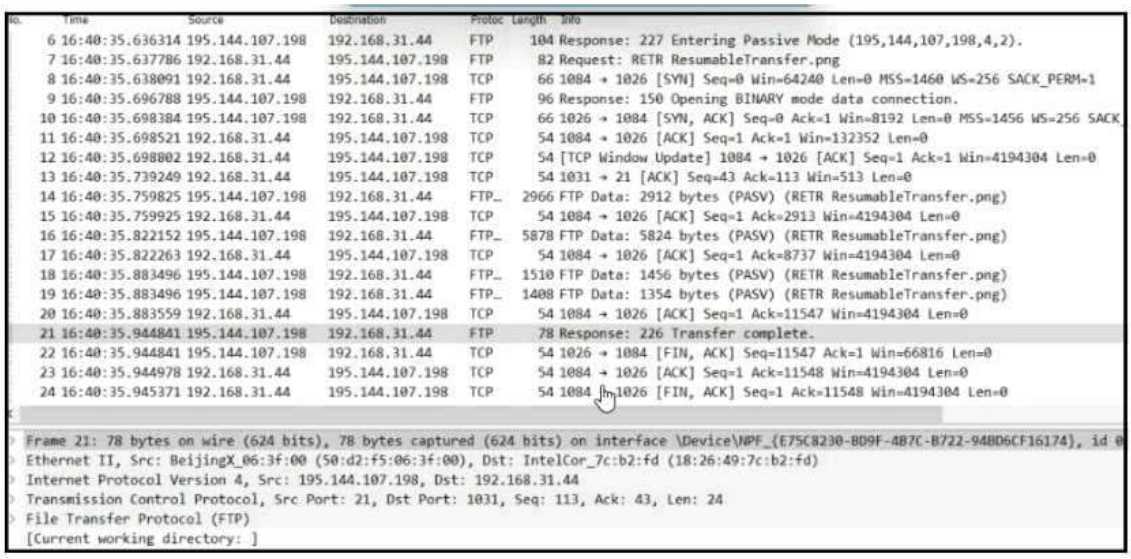
Answer: B

QUESTION 206
What describes the concept of data consistently and readily being accessible for legitimate users?

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

Answer: B

QUESTION 207
Refer to the exhibit. Which frame numbers contain a file that is extractable via TCP stream within Wireshark?



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

Answer: B

QUESTION 208
Refer to the exhibit. Which stakeholders must be involved when a company workstation is compromised?

Employee Name	Role
Employee 1	Chief Accountant
Employee 2	Head of Managed Cyber Security Services
Employee 3	System Administration
Employee 4	Security Operation Center Analyst
Employee 5	Head of Network & Security Infrastructure Services
Employee 6	Financial Manager
Employee 7	Technical Director

A. Employee 1 Employee 2, Employee 3, Employee 4, Employee 5, Employee 7
B. Employee 1, Employee 2, Employee 4, Employee 5
C. Employee 4, Employee 6, Employee 7
D. Employee 2, Employee 3, Employee 4, Employee 5

Answer: D

QUESTION 209
How does an attack surface differ from an attack vector?

A. An attack vector recognizes the potential outcomes of an attack, and the attack surface is choosing a method of an attack.
B. An attack surface identifies vulnerable parts for an attack, and an attack vector specifies which

attacks are feasible to those parts.

C. An attack surface mitigates external vulnerabilities, and an attack vector identifies mitigation techniques and possible workarounds.

D. An attack vector matches components that can be exploited, and an attack surface classifies the potential path for exploitation

Answer: C

QUESTION 210
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: D

QUESTION 211
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

QUESTION 212
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

QUESTION 213
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

QUESTION 214
Syslog collecting software is installed on the server For the log containment, a disk with FAT type partition is used An engineer determined that log files are being corrupted when the 4 GB tile size is exceeded. Which action resolves the issue?

A. Add space to the existing partition and lower the retention penod.
B. Use FAT32 to exceed the limit of 4 GB.
C. Use the Ext4 partition because it can hold files up to 16 TB.
D. Use NTFS partition for log file containment

Answer: D

QUESTION 215
What ate two categories of DDoS attacks? (Choose two.)

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

Answer: CE

QUESTION 216
What is an advantage of symmetric over asymmetric encryption?

A. A key is generated on demand according to data type.
B. A one-time encryption key is generated for data transmission
C. It is suited for transmitting large amounts of data.
D. It is a faster encryption mechanism for sessions

Answer: C

QUESTION 217
What ate two denial-of-service (DoS) attacks? (Choose two)

A. port scan
B. SYN flood
C. man-in-the-middle
D. phishing
E. teardrop

Answer: BC

QUESTION 218
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

QUESTION 219
How does TOR alter data content during transit?

A. It spoofs the destination and source information protecting both sides.
B. It encrypts content and destination information over multiple layers.
C. It redirects destination traffic through multiple sources avoiding traceability.
D. It traverses source traffic through multiple destinations before reaching the receiver

Answer: B

QUESTION 220
Refer to the exhibit. What is occurring?

```
192.168.10.10 – – [01/Dec/2020:11:12:22 -0200] "GET /icons/powered_by_rh.png HTT
P/1.1" 200 1213 "http://192.168.0.102/" "Mozilla/5.0 (X11; U; Linux x86_64; en-U
S; rv:1.9.0.12) Gecko/2009070812 Ubuntu/8.04 (hardy) Firefox/3.0.12"
192.168.10.10 – – [01/Dec/2020:11:13:15 -0200] "GET /favicon.ico HTTP/1.1" 404 2
88 "-" "Mozilla/5.0 (X11; U; Linux x86_64; en-US; rv:1.9.0.12) Gecko/2009070812
Ubuntu/8.04 (hardy) Firefox/3.0.12"
192.168.10.10 – – [01/Dec/2020:11:14:22 -0200] "GET /%27%27;!–%22%3CXSS%3E=&{()
} HTTP/1.1" 404 310 "-" "Mozilla/5.0 (X11; U; Linux x86_64; en-US; rv:1.9.0.12)
Gecko/2009070812 Ubuntu/8.04 (hardy) Firefox/3.0.12"
```

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

Answer: B

QUESTION 221
What is a collection of compromised machines that attackers use to carry out a DDoS attack?

A. subnet
B. botnet
C. VLAN
D. command and control

Answer: B

QUESTION 222
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

QUESTION 223

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