QUESTION 172
The SOC team has confirmed a potential indicator of compromise on an endpoint. The team has narrowed the executable file's type to a new trojan family.
According to the NIST Computer Security Incident Handling Guide, what is the next step in handling this event?

A. Isolate the infected endpoint from the network.
B. Perform forensics analysis on the infected endpoint.
C. Collect public information on the malware behavior.
D. Prioritize incident handling based on the impact.

Answer: C

QUESTION 173
Which technology on a host is used to isolate a running application from other applications?

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

Answer: A

QUESTION 174
An analyst received a ticket regarding a degraded processing capability for one of the HR department's servers. On the same day, an engineer noticed a disabled antivirus software and was not able to determine when or why it occurred. According to the NIST Incident Handling Guide, what is the next phase of this investigation?

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

Answer: B

QUESTION 175
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: C

QUESTION 176
Refer to the exhibit. Which type of attack is being executed?

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

Answer: A

QUESTION 177
Which attack represents the evasion technique of resource exhaustion?

A. SQL injection
B. man-in-the-middle
C. bluesnarfing
D. denial-of-service

Answer: D

QUESTION 178
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

QUESTION 179
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

QUESTION 180
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

QUESTION 181
What is the impact of false positive alerts on business compared to true positive?

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

Answer: C

QUESTION 182
An organization's security team has detected network spikes coming from the internal network. An investigation has concluded that the spike in traffic was from intensive network scanning How should the analyst collect the traffic to isolate the suspicious host?

A. by most active source IP
B. by most used ports
C. based on the protocols used
D. based on the most used applications

Answer: C

QUESTION 183
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 ot operational services
D. an organizational approach to system backup and data archiving aligned to regulations

Answer: C

QUESTION 184
An engineer is addressing a connectivity issue between two servers where the remote server is unable to establish a successful session. Initial checks show that the remote server is not receiving an SYN-ACK while establishing a session by sending the first SYN.
What is causing this issue?

A. incorrect TCP handshake
B. incorrect UDP handshake
C. incorrect OSI configuration
D. incorrect snaplen configuration

Answer: A

QUESTION 185

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: A

QUESTION 186
Refer to the exhibit. An analyst received this alert from the Cisco ASA device, and numerous activity logs were produced.

```
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]
```

How should this type of evidence be categorized?

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

Answer: D

QUESTION 187
W[^t 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

QUESTION 188
A user received an email attachment named "Hr405-report2609-empl094.exe" but did not run it. Which category of the cyber kill chain should be assigned to this type of event?

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

Answer: A

QUESTION 189
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: D

QUESTION 190
What is a difference between data obtained from Tap and SPAN ports?

A. Tap mirrors existing traffic from specified ports, while SPAN presents more structured data for deeper analysis.
B. SPAN passively splits traffic between a network device and the network without altering it, while Tap alters response times.
C. SPAN improves the detection of media errors, while Tap provides direct access to traffic with lowered data visibility.
D. Tap sends traffic from physical layers to the monitoring device, while SPAN provides a copy of network traffic from switch to destination

Answer: A

QUESTION 191
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
be exploited.