QUESTION 144
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

QUESTION 145
What is the impact of false positive alerts on business compared to true positive?

A. True positives affect security as no alarm is raised when an attack has taken place, resulting in a potential breach.
B. True positive alerts are blocked by mistake as potential attacks affecting application availability.
C. False positives affect security as no alarm is raised when an attack has taken place, resulting in a potential breach.
D. False positive alerts are blocked by mistake as potential attacks affecting application availability.

Answer: C

QUESTION 146
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

QUESTION 147
Refer to the exhibit. Which technology generates this log?

```
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]
```

A. NetFlow
B. IDS
C. web proxy
D. firewall

Answer: D

QUESTION 148
Which filter allows an engineer to filter traffic in Wireshark to further analyze the PCAP file by only showing the traffic for LAN 10.11.x.x, between workstations and servers without the Internet?

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

Answer: B

QUESTION 149
Which tool provides a full packet capture from network traffic?

A. Nagios
B. CAINE
C. Hydra
D. Wireshark

Answer: D

QUESTION 150
A company is using several network applications that require high availability and responsiveness, such that milliseconds of latency on network traffic is not acceptable. An engineer needs to analyze the network and identify ways to improve traffic movement to minimize delays. Which information must the engineer obtain for this analysis?

A. total throughput on the interface of the router and NetFlow records
B. output of routing protocol authentication failures and ports used
C. running processes on the applications and their total network usage
D. deep packet captures of each application flow and duration

Answer: C

QUESTION 151
Refer to the exhibit. What is depicted in the exhibit?

```
root@:~# cat access-logs/access_130603.txt | grep '192.168.1.91' | cut -d "\"" -f 2 |
uniq -c
    1 GET /portal.php?mode=addevent&date=2018-05-01 HTTP/1.1
    1 GET /blog/?attachment_id=2910 HTTP/1.1
    1 GET /blog/?attachment_id=2998&feed=rss2 HTTP/1.1
    1 GET /blog/?attachment_id=3156 HTTP/1.1
```

A. Windows Event logs
B. Apache logs
C. IIS logs
D. UNIX-based syslog

Answer: D

QUESTION 152
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: B

QUESTION 153
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

QUESTION 154
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

QUESTION 155
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

QUESTION 156
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: DE

QUESTION 157
Which category relates to improper use or disclosure of PII data?

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

Answer: C

QUESTION 158
Which type of evidence supports a theory or an assumption that results from initial evidence?

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

Answer: D

QUESTION 159
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: AE

QUESTION 160
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

QUESTION 161
In a SOC environment, what is a vulnerability management metric?

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

Answer: C

QUESTION 162
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: C

QUESTION 163
Which two elements of the incident response process are stated in NIST Special Publication 800-61 r2? (Choose two.)

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

Answer: AB

QUESTION 164
Refer to the exhibit. What does this output indicate?

```
PS C:\Program Files (x86)\Nmap> nmap --top-ports 5 172.31.45.240
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-22 22:05 Coordinated Universal Time
'map scan report for ip-172-31-45-240.us-west-2.compute.internal (172.31.45.240)
Host is up (0.00s latency).

PORT      STATE    SERVICE
21/tcp    closed   ftp
22/Lt_p   Clusal   "It
23/tcp    closed   telnet
80/tcp    closed   http
443/tcp   closed   https

'nap done: 1. IP address (1 host up) scanned in 0.19 seconds
Ps C:\Program Files (x86)\Nmap> nmap --top-ports 10 172.31.45.240
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-22 22:05 Coordinated Universal Time
'nap scan report for ip-172-31-45-240.us-west-2.compute.internal (172.31.45.240)
Host is up (0.00s latency).

PORT      STATE    SERVICE
21/tcp    closed   ftp
22/tcp    closed   ssh
23/tcp    closed   telnet
25/tcp    closed   smtp
80/tcp    closed   http
110/tcp   closed   pop3

139/tcp   open     netbios-ssn|
443/tcp   closed   https
445/tcp   open     microsoft-ds
3389/tcp  open     ms-wbt-server

'map done: 1 IP address (1 host up) scanned in 0.19 seconds PS
C:\Program Files (x86)\Nmap>
```

A. HTTPS ports are open on the server.
B. SMB ports are closed on the server.
C. FTP ports are open on the server.
D. Email ports are closed on the server.

Answer: A

QUESTION 165
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

QUESTION 166
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
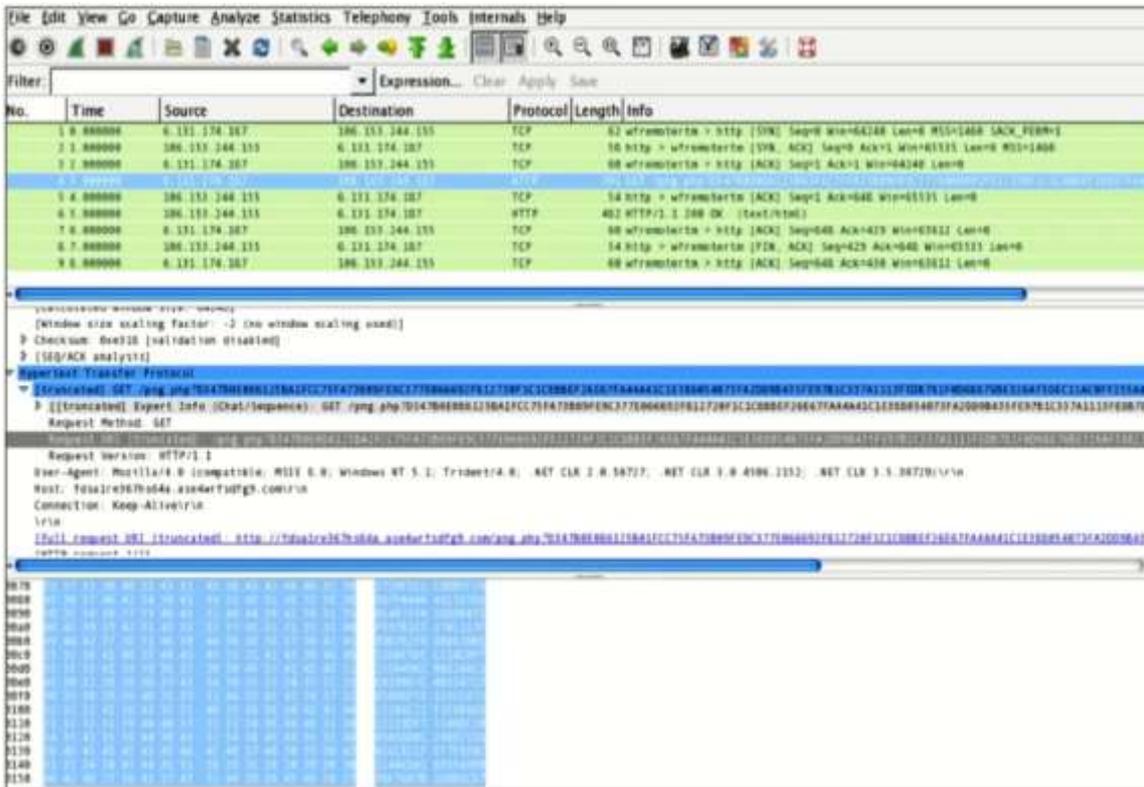
Answer: D

QUESTION 167
An engineer discovered a breach, identified the threat's entry point, and removed access. The engineer was able to identify the host, the IP address of the threat actor, and the application the threat actor targeted. What is the next step the engineer should take according to the NIST SP 800-61 Incident handling guide?

A. Recover from the threat.
B. Analyze the threat.
C. Identify lessons learned from the threat.
D. Reduce the probability of similar threats.

Answer: D

QUESTION 168
Refer to the exhibit. What is shown in this PCAP file?

A. Timestamps are indicated with error.
B. The protocol is TCP.
C. The User-Agent is Mozilla/5.0.
D. The HTTP GET is encoded.

Answer: A

QUESTION 169
What is a difference between tampered and untampered disk images?

A. Tampered images have the same stored and computed hash.
B. Tampered images are used as evidence.
C. Untampered images are used for forensic investigations.
D. Untampered images are deliberately altered to preserve as evidence

Answer: B

QUESTION 170
Drag and Drop Question
Drag and drop the definition from the left onto the phase on the right to classify intrusion events according to the Cyber Kill Chain model.

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

Answer:

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

QUESTION 171
Drag and Drop Question
Drag and drop the elements from the left into the correct order for incident handling on the right.

Preparation	step 1
Containment, eradication and recovery	step 2
Post-incident analysis	step 3
Detection and analysis	step 4

Answer:

Preparation
Detection and analysis
Containment, eradication and recovery
Post-incident analysis

200-201 Exam Dumps 200-201 Exam Questions 200-201 PDF Dumps 200-201 VCE Dumps

https://www.braindump2go.com/200-201.html