



## **Cisco**

### **Exam Questions 200-201**

Understanding Cisco Cybersecurity Operations Fundamentals

## About ExamBible

### *Your Partner of IT Exam*

## Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

## Our Advances

### \* 99.9% Uptime

All examinations will be up to date.

### \* 24/7 Quality Support

We will provide service round the clock.

### \* 100% Pass Rate

Our guarantee that you will pass the exam.

### \* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

### NEW QUESTION 1

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

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

**Answer: D**

### NEW QUESTION 2

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

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

**Answer: A**

### NEW QUESTION 3

Refer to the exhibit.



Which component is identifiable in this exhibit?

- A. Trusted Root Certificate store on the local machine
- B. Windows PowerShell verb
- C. Windows Registry hive
- D. local service in the Windows Services Manager

**Answer: C**

#### Explanation:

<https://docs.microsoft.com/en-us/windows/win32/sysinfo/registry-hives>

[https://ldapwiki.com/wiki/HKEY\\_LOCAL\\_MACHINE#:~:text=HKEY\\_LOCAL\\_MACHINE%20Windows%2](https://ldapwiki.com/wiki/HKEY_LOCAL_MACHINE#:~:text=HKEY_LOCAL_MACHINE%20Windows%2)

### NEW QUESTION 4

Which regex matches only on all lowercase letters?

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

**Answer: A**

### NEW QUESTION 5

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**

### NEW QUESTION 6

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 7

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 8**

Drag and drop the type of evidence from the left onto the description of that evidence on the right.

direct evidence	log that shows a command and control check-in from verified malware
corroborative evidence	firewall log showing successful communication and threat intelligence stating an IP is known to host malware
indirect evidence	NetFlow-based spike in DNS traffic

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Graphical user interface, application Description automatically generated

**NEW QUESTION 9**

Refer to the exhibit.

```
#Time Format: Local
#Fields: date time action protocol src-ip dst-ip src-port dst-port size tcpflags tcpsyn tcpack tcpwin icmp type 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
```

An engineer received an event log file to review. Which technology generated the log?

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

**Answer: C**

**NEW QUESTION 10**

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 10

What is the difference between discretionary access control (DAC) and role-based access control (RBAC)?

- A. DAC requires explicit authorization for a given user on a given object, and RBAC requires specific conditions.
- B. RBAC access is granted when a user meets specific conditions, and in DAC, permissions are applied on user and group levels.
- C. RBAC is an extended version of DAC where you can add an extra level of authorization based on time.
- D. DAC administrators pass privileges to users and groups, and in RBAC, permissions are applied to specific groups

**Answer:** A

#### NEW QUESTION 12

What should a security analyst consider when comparing inline traffic interrogation with traffic tapping to determine which approach to use in the network?

- A. Tapping interrogation replicates signals to a separate port for analyzing traffic
- B. Tapping interrogations detect and block malicious traffic
- C. Inline interrogation enables viewing a copy of traffic to ensure traffic is in compliance with security policies
- D. Inline interrogation detects malicious traffic but does not block the traffic

**Answer:** A

#### Explanation:

A network TAP is a simple device that connects directly to the cabling infrastructure to split or copy packets for use in analysis, security, or general network management

#### NEW QUESTION 17

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 22

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

- A. Deep packet inspection gives insights up to Layer 7, and stateful inspection gives insights only up to Layer 4.
- B. Deep packet inspection is more secure due to its complex signatures, and stateful inspection requires less human intervention.
- C. Stateful inspection is more secure due to its complex signatures, and deep packet inspection requires less human intervention.
- D. Stateful inspection verifies data at the transport layer and deep packet inspection verifies data at the application layer

**Answer:** B

#### NEW QUESTION 24

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 25

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 27

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

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

**Answer: C**

#### NEW QUESTION 30

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 35

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 36

Which signature impacts network traffic by causing legitimate traffic to be blocked?

- A. false negative
- B. true positive
- C. true negative
- D. false positive

**Answer: D**

**NEW QUESTION 38**

Refer to the exhibit.



Where is the executable file?

- A. info
- B. tags
- C. MIME
- D. name

**Answer: C**

**NEW QUESTION 42**

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 43**

Refer to the exhibit.

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

Which stakeholders must be involved when a company workstation is compromised?

- 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

**NEW QUESTION 48**

Which artifact is used to uniquely identify a detected file?

- A. file timestamp
- B. file extension
- C. file size
- D. file hash

**Answer:** D

**NEW QUESTION 51**

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 this type of event belong?

- A. weaponization
- B. delivery
- C. exploitation
- D. reconnaissance

**Answer:** B

**NEW QUESTION 53**

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 58**

Which two components reduce the attack surface on an endpoint? (Choose two.)

- A. secure boot
- B. load balancing
- C. increased audit log levels
- D. restricting USB ports
- E. full packet captures at the endpoint

**Answer:** AD

**NEW QUESTION 61**

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 62**

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 67**

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



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

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

**Answer: D**

**NEW QUESTION 70**

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 72**

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 73**

During which phase of the forensic process are tools and techniques used to extract information from the collected data?

- A. investigation
- B. examination
- C. reporting
- D. collection

**Answer: D**

**NEW QUESTION 78**

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 79**

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 83**

What does cyber attribution identify in an investigation?

- A. cause of an attack
- B. exploit of an attack
- C. vulnerabilities exploited
- D. threat actors of an attack

**Answer:** D

**Explanation:**

<https://www.techtarget.com/searchsecurity/definition/cyber-attribution>

**NEW QUESTION 85**

Which evasion technique is a function of ransomware?

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

**Answer:** B

**NEW QUESTION 89**

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: 00:0C: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 91**

Which process is used when IPS events are removed to improve data integrity?

- A. data availability
- B. data normalization
- C. data signature
- D. data protection

**Answer:** B

**NEW QUESTION 92**

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 95**

Refer to the exhibit.

```
Nov 30 17:48:43 ip-172-31-27-153 sshd[23001]: Invalid user password from 218.26.11.11
Nov 30 17:48:44 ip-172-31-27-153 sshd[23001]: Invalid user password from 218.26.11.11
Nov 30 17:48:46 ip-172-31-27-153 sshd[23003]: Invalid user password from 218.26.11.11
Nov 30 17:48:46 ip-172-31-27-153 sshd[23003]: Invalid user password from 218.26.11.11
Nov 30 17:48:46 ip-172-31-27-153 sshd[23003]: Invalid user password from 218.26.11.11
Nov 30 17:48:46 ip-172-31-27-153 sshd[23003]: Invalid user password from 218.26.11.11
Nov 30 17:48:48 ip-172-31-27-153 sshd[23005]: Invalid user password from 218.26.11.11
Nov 30 17:48:48 ip-172-31-27-153 sshd[23005]: Invalid user password from 218.26.11.11
Nov 30 17:48:48 ip-172-31-27-153 sshd[23005]: Invalid user password from 218.26.11.11
Nov 30 17:48:49 ip-172-31-27-153 sshd[23005]: Invalid user password from 218.26.11.11
Nov 30 17:48:51 ip-172-31-27-153 sshd[23007]: Invalid user password from 218.26.11.11
Nov 30 17:48:51 ip-172-31-27-153 sshd[23007]: Invalid user password from 218.26.11.11
Nov 30 17:48:51 ip-172-31-27-153 sshd[23007]: Invalid user password from 218.26.11.11
Nov 30 17:48:51 ip-172-31-27-153 sshd[23007]: Invalid user password from 218.26.11.11
Nov 30 17:48:54 ip-172-31-27-153 sshd[23009]: Invalid user password from 218.26.11.11
Nov 30 17:48:54 ip-172-31-27-153 sshd[23009]: Invalid user password from 218.26.11.11
Nov 30 17:48:54 ip-172-31-27-153 sshd[23009]: Invalid user password from 218.26.11.11
Nov 30 17:48:54 ip-172-31-27-153 sshd[23009]: Invalid user password from 218.26.11.11
Nov 30 17:48:56 ip-172-31-27-153 sshd[23011]: Invalid user password from 218.26.11.11
Nov 30 17:48:56 ip-172-31-27-153 sshd[23011]: Invalid user password from 218.26.11.11
Nov 30 17:48:56 ip-172-31-27-153 sshd[23011]: Invalid user password from 218.26.11.11
Nov 30 17:48:56 ip-172-31-27-153 sshd[23011]: Invalid user password from 218.26.11.11
Nov 30 17:48:59 ip-172-31-27-153 sshd[23013]: Invalid user password from 218.26.11.11
Nov 30 17:48:59 ip-172-31-27-153 sshd[23013]: Invalid user password from 218.26.11.11
```

A security analyst is investigating unusual activity from an unknown IP address Which type of evidence is this file?

- A. indirect evidence
- B. best evidence
- C. corroborative evidence
- D. direct evidence

**Answer:** A

**NEW QUESTION 99**

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 101**

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 104**

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 107**

Refer to the exhibit.

Interface	IP Address	Physical Address	Type
192.168.1.10	192.168.1.10	d8-a7-56-d7-19-ea	dynamic
192.168.1.67	192.168.1.67	d8-a7-56-d7-19-ea	dynamic
192.168.1.1	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 110**

Refer to the exhibit.

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

What must be interpreted from this packet capture?

- A. IP address 192.168.88.12 is communicating with 192.168.88.149 with a source port 74 to destination port 49098 using TCP protocol
- B. IP address 192.168.88.12 is communicating with 192.168.88.149 with a source port 49098 to destination port 80 using TCP protocol.
- C. IP address 192.168.88.149 is communicating with 192.168.88.12 with a source port 80 to destination port 49098 using TCP protocol.
- D. IP address 192.168.88.149 is communicating with 192.168.88.12 with a source port 49098 to destination port 80 using TCP protocol.

**Answer:** B

**NEW QUESTION 113**

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 114**

Which system monitors local system operation and local network access for violations of a security policy?

- A. host-based intrusion detection
- B. systems-based sandboxing
- C. host-based firewall
- D. antivirus

**Answer:** A

**Explanation:**

HIDS is capable of monitoring the internals of a computing system as well as the network packets on its network interfaces. Host-based firewall is a piece of software running on a single Host that can restrict incoming and outgoing Network activity for that host only.

**NEW QUESTION 115**

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

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

**Answer:** AB

**NEW QUESTION 120**

A company receptionist received a threatening call referencing stealing assets and did not take any action assuming it was a social engineering attempt. Within 48 hours, multiple assets were breached, affecting the confidentiality of sensitive information. What is the threat actor in this incident?

- A. company assets that are threatened
- B. customer assets that are threatened
- C. perpetrators of the attack
- D. victims of the attack

**Answer:** C

**NEW QUESTION 125**

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: D**

#### NEW QUESTION 128

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 129

What is a difference between SOAR and SIEM?

- A. SOAR platforms are used for threat and vulnerability management, but SIEM applications are not
- B. SIEM applications are used for threat and vulnerability management, but SOAR platforms are not
- C. SOAR receives information from a single platform and delivers it to a SIEM
- D. SIEM receives information from a single platform and delivers it to a SOAR

**Answer: A**

#### NEW QUESTION 132

An engineer received an alert affecting the degraded performance of a critical server. Analysis showed a heavy CPU and memory load. What is the next step the engineer should take to investigate this resource usage?

- A. Run "ps -d" to decrease the priority state of high load processes to avoid resource exhaustion.
- B. Run "ps -u" to find out who executed additional processes that caused a high load on a server.
- C. Run "ps -ef" to understand which processes are taking a high amount of resources.
- D. Run "ps -m" to capture the existing state of daemons and map required processes to find the gap.

**Answer: C**

#### NEW QUESTION 137

Refer to the exhibit.

```
SELECT * FROM people WHERE username = " OR '1'='1';
```

Which type of attack is being executed?

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

**Answer: A**

#### NEW QUESTION 142

What is the principle of defense-in-depth?

- A. Agentless and agent-based protection for security are used.
- B. Several distinct protective layers are involved.
- C. Access control models are involved.
- D. Authentication, authorization, and accounting mechanisms are used.

**Answer: B**

#### NEW QUESTION 144

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 149**

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 150**

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 within the exhibit?

- A. regular GET requests
- B. XML External Entities attack
- C. insecure deserialization
- D. cross-site scripting attack

**Answer: A**

**NEW QUESTION 153**

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 file size is exceeded. Which action resolves the issue?

- A. Add space to the existing partition and lower the retention period.
- 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**

**NEW QUESTION 154**

Why is encryption challenging to security monitoring?

- A. Encryption analysis is used by attackers to monitor VPN tunnels.
- B. Encryption is used by threat actors as a method of evasion and obfuscation.
- C. Encryption introduces additional processing requirements by the CPU.
- D. Encryption introduces larger packet sizes to analyze and store.

**Answer: B**

**NEW QUESTION 156**

Refer to the exhibit.

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

Which packet contains a file that is extractable within Wireshark?

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

**Answer: D**

**NEW QUESTION 157**

Which attack is the network vulnerable to when a stream cipher like RC4 is used twice with the same key?

- A. forgery attack
- B. plaintext-only attack
- C. ciphertext-only attack
- D. meet-in-the-middle attack

Answer: C

**NEW QUESTION 158**

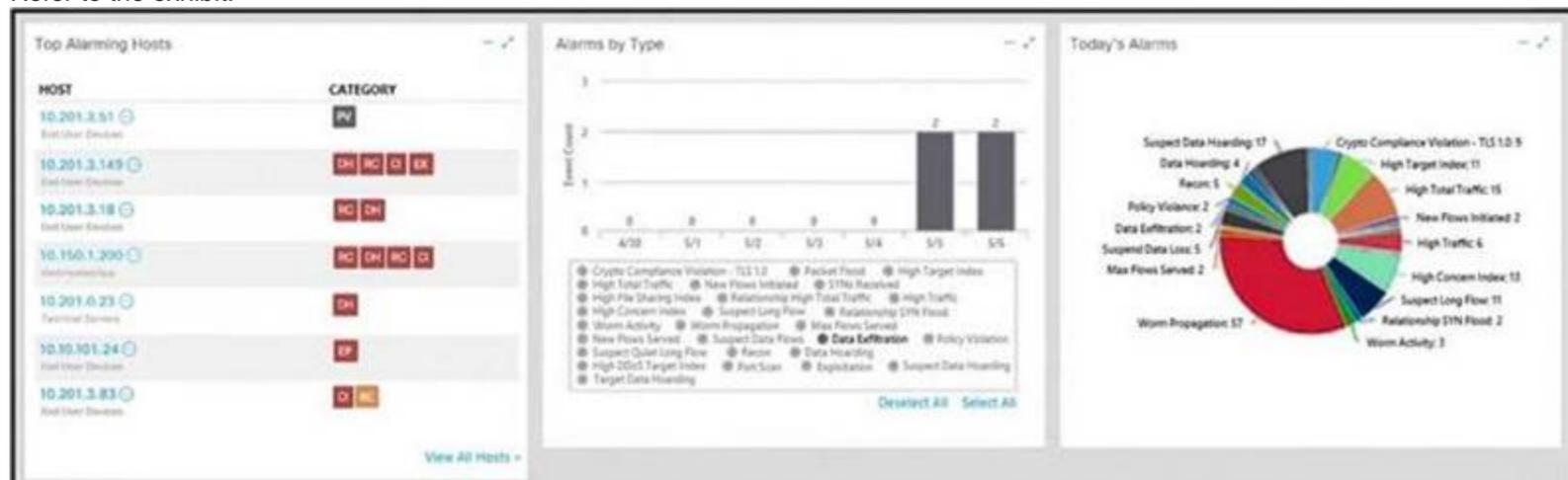
Which data format is the most efficient to build a baseline of traffic seen over an extended period of time?

- A. syslog messages
- B. full packet capture
- C. NetFlow
- D. firewall event logs

Answer: C

**NEW QUESTION 159**

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 162**

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 167**

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

#### NEW QUESTION 168

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 173

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 174

Refer to the exhibit.

```
Mar 6 10:35:34 user sshd[12900]: pam_unix(sshd:auth):authentication failure;
logname= uid=0 euid=0 tty=ssh ruser= rhost=127.0.0.1
Mar 6 10:35:36 user sshd[12900]: Failed password for invalid user not_bill from
127.0.0.1 port 38346 ssh2
```

In which Linux log file is this output found?

- A. /var/log/authorization.log
- B. /var/log/dmesg
- C. var/log/var.log
- D. /var/log/auth.log

**Answer: D**

#### NEW QUESTION 176

What is obtained using NetFlow?

- A. session data
- B. application logs
- C. network downtime report
- D. full packet capture

**Answer: A**

#### NEW QUESTION 181

Refer to the exhibit.

No.	Time	Source	Destination	Protocol	Length	Info
18	0.011310	10.0.2.15	192.124.249.9	TCP	70	50588-443 [FIN] Seq=1
19	0.022656	192.124.249.9	10.0.2.15	TCP	62	443-50588 [SYN, ACK]
20	0.022702	10.0.2.15	192.124.249.9	TCP	56	50588-443 [ACK] Seq=1
21	0.022988	192.124.249.9	10.0.2.15	TCP	62	443-50586 [SYN, ACK]
22	0.022996	10.0.2.15	192.124.249.9	TCP	56	50586-443 [ACK] Seq=1
23	0.023212	10.0.2.15	192.124.249.9	TCP	261	50588-443 [PSH, ACK]
24	0.023373	10.0.2.15	192.124.249.9	TCP	261	50586-443 [PSH, ACK]
25	0.023445	192.124.249.9	10.0.2.15	TCP	62	443-50588 [ACK] Seq=1
26	0.023617	192.124.249.9	10.0.2.15	TCP	62	443-50586 [ACK] Seq=1
27	0.037413	192.124.249.9	10.0.2.15	TCP	2792	443-50586 [PSH, ACK]
28	0.037426	10.0.2.15	192.124.249.9	TCP	56	50586-443 [ACK] Seq=2

> Frame 24: 261 bytes on wire (2088 bits), 261 bytes captured (2088 bits)  
 > Linux cooked capture  
 > Internet Protocol Version 4, Src: 10.0.2.15 (10.0.2.15), Dst: 192.124.249.9 (192.124.249.9)  
 > Transmission Control Protocol, Src Port: 50586 (50586), Dst Port: 443 (443), Seq: 1, A  
 > Data [205 bytes]  
 Data: 16030100c8010000c403030e06ead078d17676c13ab46ebf...  
 [Length: 205]

```

0000  00 04 00 01 00 06 08 00 27 7a 3c 93 00 00 08 00  ..... *z<.....
0010  45 00 00 f5 48 7b 40 00 40 06 2b f3 0a 00 02 0f  E...H{@. @.+.....
0020  c0 7c f9 09 c5 9a 01 bb 0e 1f dc b4 00 b4 aa 02  .|.....
0030  50 18 72 10 c6 7c 00 00 16 03 01 00 c8 01 00 00  P.r..|..
0040  c4 03 03 0e 06 ea d0 78 d1 76 76 c1 3a b4 6e bf  .....x .vv.:n..
0050  e6 b8 b8 b2 ba 08 d6 6d 0d 38 fb 91 45 de fc ee  .....m .8..E...
0060  8b 6e f8 00 00 1e c0 2b c0 2f cc a9 cc a8 c0 2c  .n.....+ ./.....
0070  c0 30 c0 0a c0 09 c0 13 c0 14 00 33 00 39 00 2f  .0..... ...3.9./
0080  00 35 00 0a 01 00 00 7d 00 00 00 16 00 14 00 00  .5.....} .....
0090  11 77 77 77 2e 6c 69 6e 75 78 6d 69 6e 74 2e 63  .wwwlin uxmint.c
00a0  6f 6d 00 17 00 00 ff 01 00 01 00 00 0a 00 08 00  om.....
00b0  06 00 17 00 18 00 19 00 0b 00 02 01 00 00 23 00  .....
00c0  00 33 74 00 00 00 10 00 17 00 15 02 68 32 08 73  .3t..... .h2.s
00d0  70 64 79 2f 33 2e 31 08 68 74 74 70 2f 31 2e 31  pdy/3.1. http/1.1
00e0  00 05 00 05 01 00 00 00 00 00 0d 00 18 00 16 04  .....
00f0  01 05 01 06 01 02 01 04 03 05 03 06 03 02 03 05  .....
0100  02 04 02 02 02  .....
  
```

Which application protocol is in this PCAP file?

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

Answer: D

**NEW QUESTION 183**

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 188**

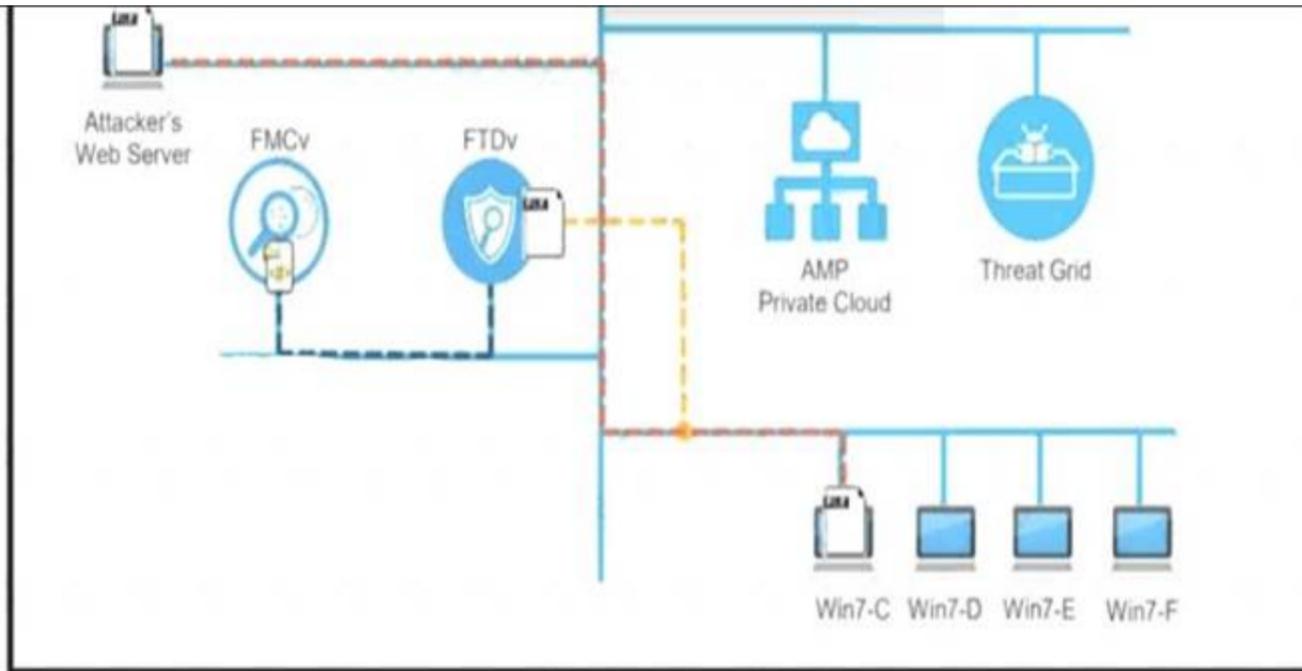
How does an SSL certificate impact security between the client and the server?

- 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 192**

Refer to the exhibit.



A workstation downloads a malicious docx file from the Internet and a copy is sent to FTDv. The FTDv sends the file hash to FMC and the tile event is recorded. What would have occurred with stronger data visibility?

- A. The traffic would have been monitored at any segment in the network.
- B. Malicious traffic would have been blocked on multiple devices
- C. An extra level of security would have been in place
- D. Detailed information about the data in real time would have been provided

**Answer: B**

**NEW QUESTION 195**

When trying to evade IDS/IPS devices, which mechanism allows the user to make the data incomprehensible without a specific key, certificate, or password?

- A. fragmentation
- B. pivoting
- C. encryption
- D. steganography

**Answer: C**

**Explanation:**

<https://techdifferences.com/difference-between-steganography-and-cryptography.html#:~:text=The%20steganog>

**NEW QUESTION 196**

What are the two characteristics of the full packet captures? (Choose two.)

- A. Identifying network loops and collision domains.
- B. Troubleshooting the cause of security and performance issues.
- C. Reassembling fragmented traffic from raw data.
- D. Detecting common hardware faults and identify faulty assets.
- E. Providing a historical record of a network transaction.

**Answer: CE**

**NEW QUESTION 201**

Refer to the exhibit.

Category	Started On	Completed On	Duration	Cuckoo Version
FILE	2014-02-23 21:52:16	2014-02-23 21:52:34	18 seconds	1.0
<b>File Details</b>				
File name	[REDACTED]			
File size	114720 bytes			
File type	PE32 executable (GUI) Intel: 80386, for MS Windows			
CRC32	8848E2EA			
MD5	890f9069a778b0c8e928fcb4c0ce08			
SHA1	f891d31d3e4a5885a1f9b136322d8ec973b79ba			
SHA256	f4855d1b1077ab1a2e0b99016437f72c5f98579d09f08b6312cc24400f483177			
SHA512	9756e0af8981bc9796a3879fe02d0e182c5557ba99a094238ca4f1df083592cf497c123d2a6a0598607432188aaf42976e0bd9da742c0900275be721db2595			
Siddeep	6144)Eu2077e1Lnfr87pR18T+5zLqJ249XCUg0g0yCvut/1r9Dep1YX1+o6YUPL:Eu2077eand1d+5WGC3g07CK/1r7EE			
PEID	None matched			
Yara	• shellcode (Matched shellcode byte patterns)			
VirusTotal	Pending VirusTotal Scan Date: 2014-01-12 23:43:56 Detection Rate: 26/47 (collapse)			

An employee received an email from an unknown sender with an attachment and reported it as a phishing attempt. An engineer uploaded the file to Cuckoo for further analysis. What should an engineer interpret from the provided Cuckoo report?

- A. Win32.polip.a.exe is an executable file and should be flagged as malicious.
- B. The file is clean and does not represent a risk.
- C. Cuckoo cleaned the malicious file and prepared it for usage.
- D. MD5 of the file was not identified as malicious.

**Answer:** C

**NEW QUESTION 204**

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

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

**Answer:** A

**NEW QUESTION 207**

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 211**

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 213**

What describes the impact of false-positive alerts compared to false-negative alerts?

- A. A false negative is alerting for an XSS attac
- B. An engineer investigates the alert and discovers that an XSS attack happened A false positive is when an XSS attack happens and no alert is raised
- C. A false negative is a legitimate attack triggering a brute-force aler
- D. An engineer investigates the alert and finds out someone intended to break into the system A false positive is when no alert and no attack is occurring
- E. A false positive is an event alerting for a brute-force attack An engineer investigates the alert and discovers that a legitimate user entered the wrong credential

several times A false negative is when a threat actor tries to brute-force attack a system and no alert is raised.  
 F. A false positive is an event alerting for an SQL injection attack An engineer investigates the alert and discovers that an attack attempt was blocked by IPS A false negative is when the attack gets detected but succeeds and results in a breach.

Answer: C

**NEW QUESTION 215**

Refer to the exhibit.

File name	CVE-2009-4324 PDF 2009-11-30 note200911.pdf
File size	400918 bytes
File type	PDF document, version 1.6
CRC32	11638A9B
MD5	61baabd6fc12e01ff73ceacc07c84f9a
SHA1	0805d0ae62f5358b9a3f4c1868d552fc3561b17
SHA256	27cced58a0fcb0bbe3894f74d3014611039fefdf3bd2b0ba7ad85b18194c
SHA512	5a43bc7eef279b209e2590432cc3e2eb480d0f78004e265f00b98b4afdc9a
Ssdeep	1536:p0AAH2KthGBjcdBj8VETeePxsT65ZZ3pdx/ves/QR/875+prahGV6B
PEID	None matched
Yara	<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>
VirusTotal	<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 219**

What are the two differences between stateful and deep packet inspection? (Choose two )

- A. Stateful inspection is capable of TCP state tracking, and deep packet filtering checks only TCP source and destination ports
- B. Deep packet inspection is capable of malware blocking, and stateful inspection is not
- C. Deep packet inspection operates on Layer 3 and 4. and stateful inspection operates on Layer 3 of the OSI model
- D. Deep packet inspection is capable of TCP state monitoring only, and stateful inspection can inspect TCP and UDP.
- E. Stateful inspection is capable of packet data inspections, and deep packet inspection is not

Answer: AB

**NEW QUESTION 220**

During which phase of the forensic process is data that is related to a specific event labeled and recorded to preserve its integrity?

- A. examination
- B. investigation
- C. collection
- D. reporting

Answer: C

**NEW QUESTION 225**

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 happend inside network, presented evidence could be used to support other evidences or make our narreation stronger but alone it's mean nothing.

**NEW QUESTION 230**

An engineer needs to have visibility on TCP bandwidth usage, response time, and latency, combined with deep packet inspection to identify unknown software by its network traffic flow. Which two features of Cisco Application Visibility and Control should the engineer use to accomplish this goal? (Choose two.)

- A. management and reporting
- B. traffic filtering
- C. adaptive AVC
- D. metrics collection and exporting
- E. application recognition

**Answer:** AE

**NEW QUESTION 232**

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 236**

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 241**

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 245**

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

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

**Answer:** D

**NEW QUESTION 247**

Refer to the exhibit.

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

What is depicted in the exhibit?

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

**Answer: B**

#### NEW QUESTION 249

A security incident occurred with the potential of impacting business services. Who performs the attack?

- A. malware author
- B. threat actor
- C. bug bounty hunter
- D. direct competitor

**Answer: B**

#### NEW QUESTION 251

An offline audit log contains the source IP address of a session suspected to have exploited a vulnerability resulting in system compromise. Which kind of evidence is this IP address?

- A. best evidence
- B. corroborative evidence
- C. indirect evidence
- D. forensic evidence

**Answer: B**

#### NEW QUESTION 256

What is the difference between an attack vector and attack surface?

- A. An attack surface identifies vulnerabilities that require user input or validation; and an attack vector identifies vulnerabilities that are independent of user actions.
- B. An attack vector identifies components that can be exploited, and an attack surface identifies the potential path an attack can take to penetrate the network.
- C. An attack surface recognizes which network parts are vulnerable to an attack; and an attack vector identifies which attacks are possible with these vulnerabilities.
- D. An attack vector identifies the potential outcomes of an attack; and an attack surface launches an attack using several methods against the identified vulnerabilities.

**Answer: C**

#### NEW QUESTION 257

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 261

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 264**

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:**

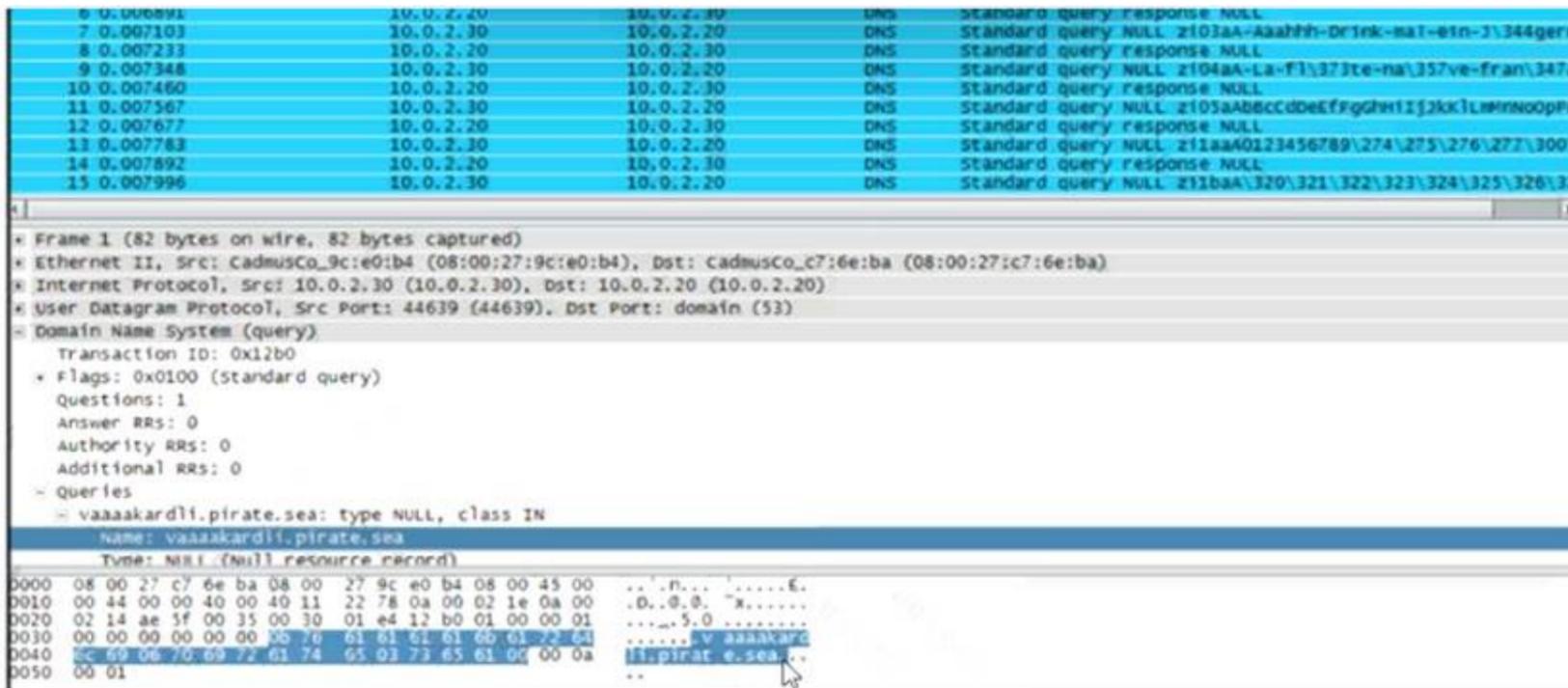
A precursor is a sign that a cyber-attack is about to occur on a system or network. An indicator is the actual alerts that are generated as an attack is happening. Therefore, as a security professional, it's important to know where you can find both precursor and indicator sources of information.

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 267**

Refer to the exhibit.



What is occurring?

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

**Answer: D**

**NEW QUESTION 269**

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**

**NEW QUESTION 272**

What is an incident response plan?

- A. an organizational approach to events that could lead to asset loss or disruption of operations
- B. an organizational approach to security management to ensure a service lifecycle and continuous improvements
- C. an organizational approach to disaster recovery and timely restoration of operational services
- D. an organizational approach to system backup and data archiving aligned to regulations

**Answer:** C

**NEW QUESTION 273**

What is the relationship between a vulnerability and a threat?

- A. A threat exploits a vulnerability
- B. A vulnerability is a calculation of the potential loss caused by a threat
- C. A vulnerability exploits a threat
- D. A threat is a calculation of the potential loss caused by a vulnerability

**Answer:** A

**NEW QUESTION 275**

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

**NEW QUESTION 280**

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 281**

Which type of data collection requires the largest amount of storage space?

- A. alert data
- B. transaction data
- C. session data
- D. full packet capture

**Answer:** D

**NEW QUESTION 284**

While viewing packet capture data, an analyst sees that one IP is sending and receiving traffic for multiple devices by modifying the IP header. Which technology makes this behavior possible?

- A. encapsulation
- B. TOR
- C. tunneling
- D. NAT

**Answer:** D

**Explanation:**

Network address translation (NAT) is a method of mapping an IP address space into another by modifying network address information in the IP header of packets while they are in transit across a traffic routing device.

**NEW QUESTION 289**

Which tool provides a full packet capture from network traffic?

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

**Answer:** D

**NEW QUESTION 290**

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 291**

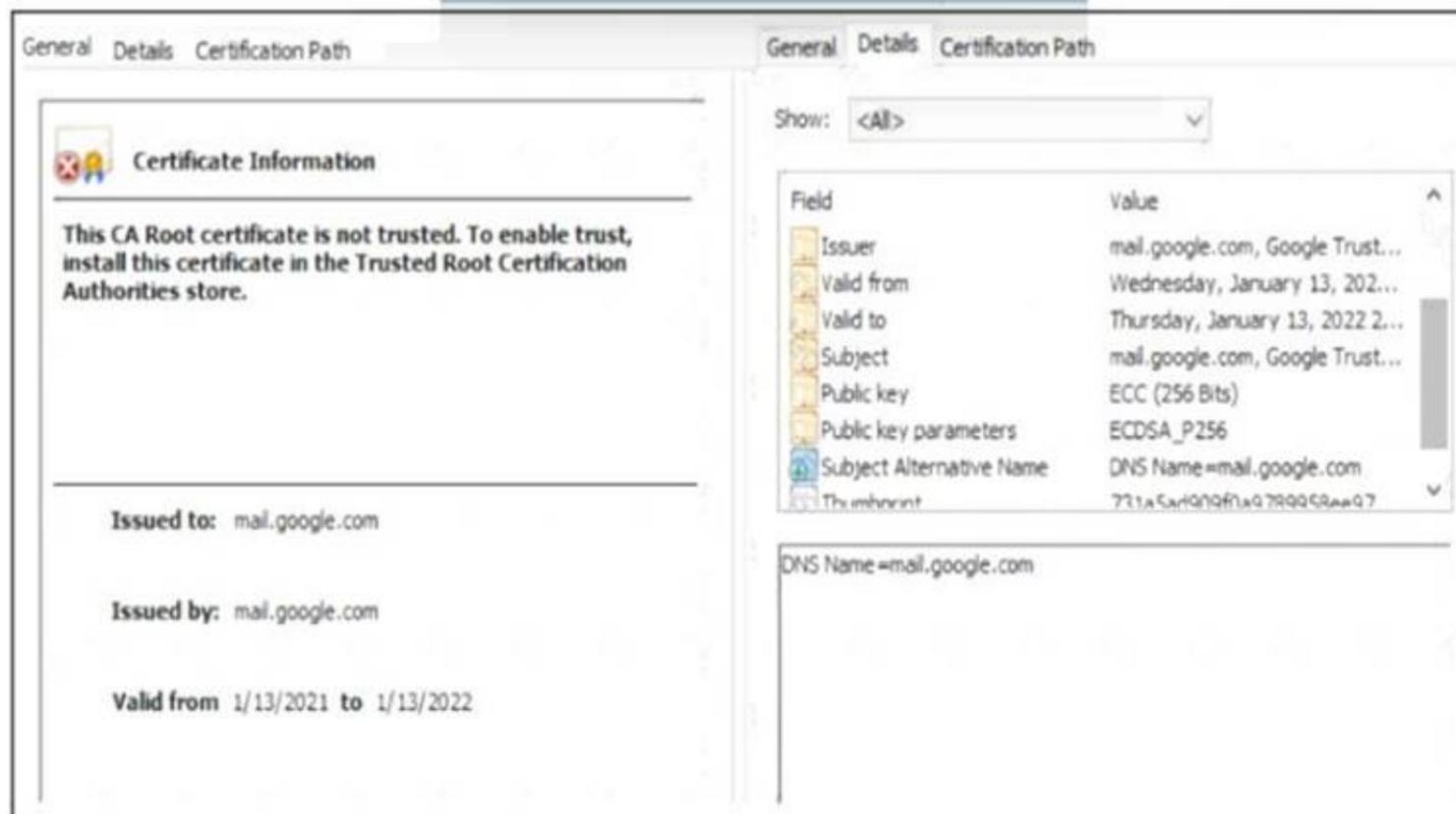
How is attacking a vulnerability categorized?

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

Answer: C

**NEW QUESTION 295**

Refer to the exhibit.



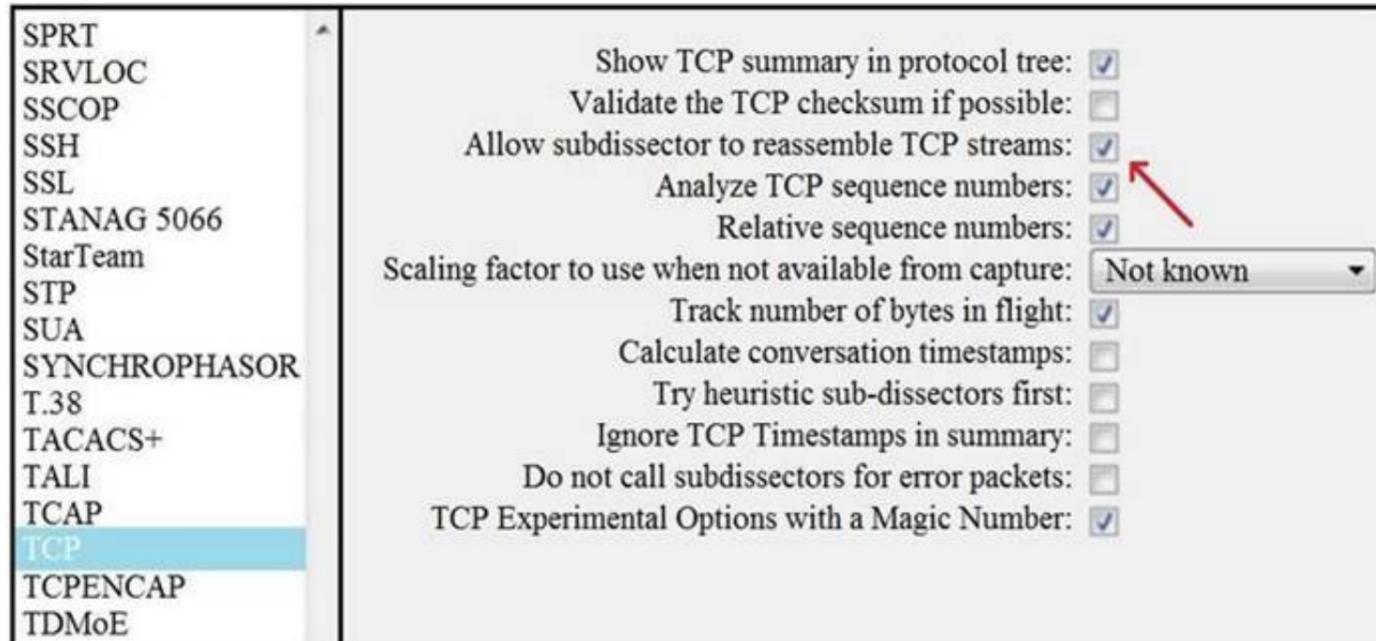
A company employee is connecting to mail google.com from an endpoint device. The website is loaded but with an error. What is occurring?

- 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

**NEW QUESTION 300**

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 303

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 306

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 309

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 314

What are 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**

### NEW QUESTION 316

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 321

.....

## Relate Links

**100% Pass Your 200-201 Exam with ExamBible Prep Materials**

<https://www.exambible.com/200-201-exam/>

## Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>