Practice Exam Questions



# Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)

EXAMKILLER

Help Pass Your Exam At First Try

# Cisco

## Exam 200-201

### Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)

**Version: 10.0**

**[ Total Questions: 263 ]**

## Question No : 1

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**

## Question No : 2

An analyst is investigating a host in the network that appears to be communicating to a command and control server on the Internet. After collecting this packet capture, the analyst cannot determine the technique and payload used for the communication.

```
File     Actions     Edit     View     Help

    48 41.270348133 185.199.111.153 → 192.168.88.164 TLSv1.2 123 Application Data
    49 41.270348165 185.199.111.153 → 192.168.88.164 TLSv1.2 104 Application Data
    50 41.270356290 192.168.88.164 → 185.199.111.153 TCP 66 44736 → 443 [ACK]
Seq=834 Ack=3104 Win=64128 Len=0 TSval=3947973757 TSecr=2989424849
    51 41.270369874 192.168.88.164 → 185.199.111.153 TCP 66 44736 → 443 [ACK]
Seq=834 Ack=3142 Win=64128 Len=0 TSval=3947973757 TSecr=2989424849
    52 41.270430171 192.168.88.164 → 185.199.111.153 TLSv1.2 104 Application Data
    53 41.271767772 185.199.111.153 → 192.168.88.164 TLSv1.2 2854 Application Data
    54 41.271767817 185.199.111.153 → 192.168.88.164 TLSv1.2 904 Application Data
    55 41.271788996 192.168.88.164 → 185.199.111.153 TCP 66 44736 → 443 [ACK]
Seq=872 Ack=6768 Win=62592 Len=0 TSval=3947973758 TSecr=2989424849
    56 41.271973293 192.168.88.164 → 185.199.111.153 TLSv1.2 97 Encrypted Alert
    57 41.272411701 192.168.88.164 → 185.199.111.153 TCP 66 44736 → 443 [FIN, ACK]
Seq=903 Ack=6768 Win=64128 Len=0 TSval=3947973759 TSecr=2989424849
    58 41.283301751 185.199.111.153 → 192.168.88.164 TCP 66 443 → 44736 [ACK]
Seq=6768 Ack=903 Win=28160 Len=0 TSval=2989424852 TSecr=3947973757
    59 41.283301808 185.199.111.153 → 192.168.88.164 TLSv1.2 97 Encrypted Alert
    60 41.283321947 192.168.88.164 → 185.199.111.153 TCP 54 44736 → 443 [RST]
Seq=903 Win=0 Len=0
    61 41.283939151 185.199.111.153 → 192.168.88.164 TCP 66 443 → 44736 [FIN, ACK]
Seq=6799 Ack=903 Win=28160 Len=0 TSval=2989424852 TSecr=3947973757
    62 41.283945760 192.168.88.164 → 185.199.111.153 TCP 54 44736 → 443 [RST]
Seq=903 Win=0 Len=0
    63 41.284635561 185.199.111.153 → 192.168.88.164 TCP 66 443 → 44736 [ACK]
Seq=6800 Ack=904 Win=28160 Len=0 TSval=2989424853 TSecr=3947973759
    64 41.284642324 192.168.88.164 → 185.199.111.153 TCP 54 44736 → 443 [RST]
Seq=904 Win=0 Len=0
```

Which obfuscation technique is the attacker using?

**A.** Base64 encoding

**B.** TLS encryption
**C.** SHA-256 hashing
**D.** ROT13 encryption

**Answer: B**

**Explanation:** ROT13 is considered weak encryption and is not used with TLS (HTTPS:443). Source: https://en.wikipedia.org/wiki/ROT13

## Question No : 3

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

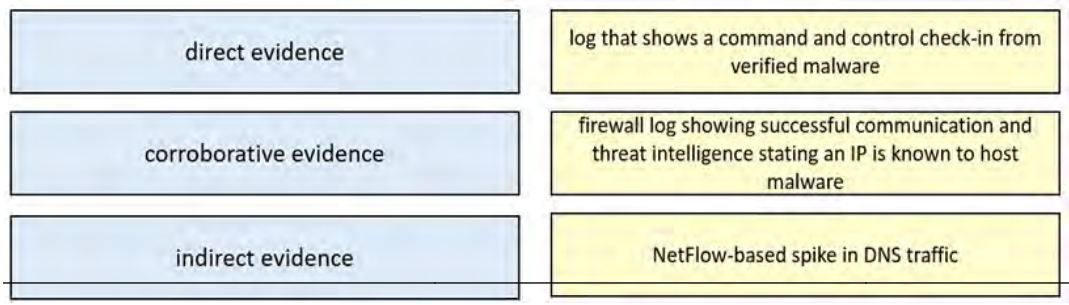
**A.** sandbox
**B.** application allow list
**C.** application block list
**D.** host-based firewall

**Answer: A**

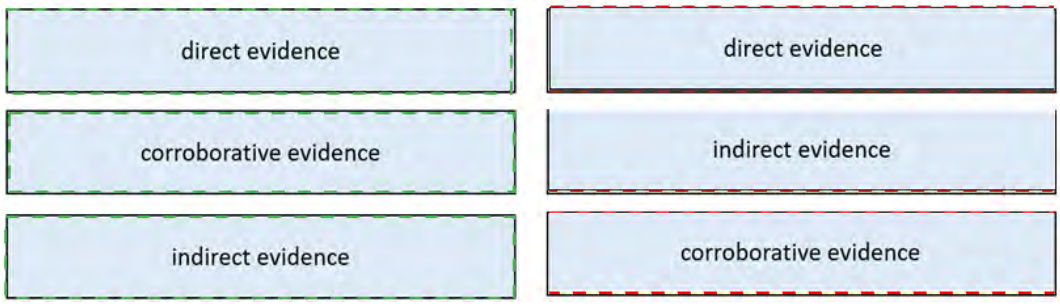
Reference: https://searchsecurity.techtarget.com/definition/sandbox#:~:text=Sandboxes%20can%20be%20used%20to,be%20run%20inside%20a%20sandbox

## Question No : 4 DRAG DROP

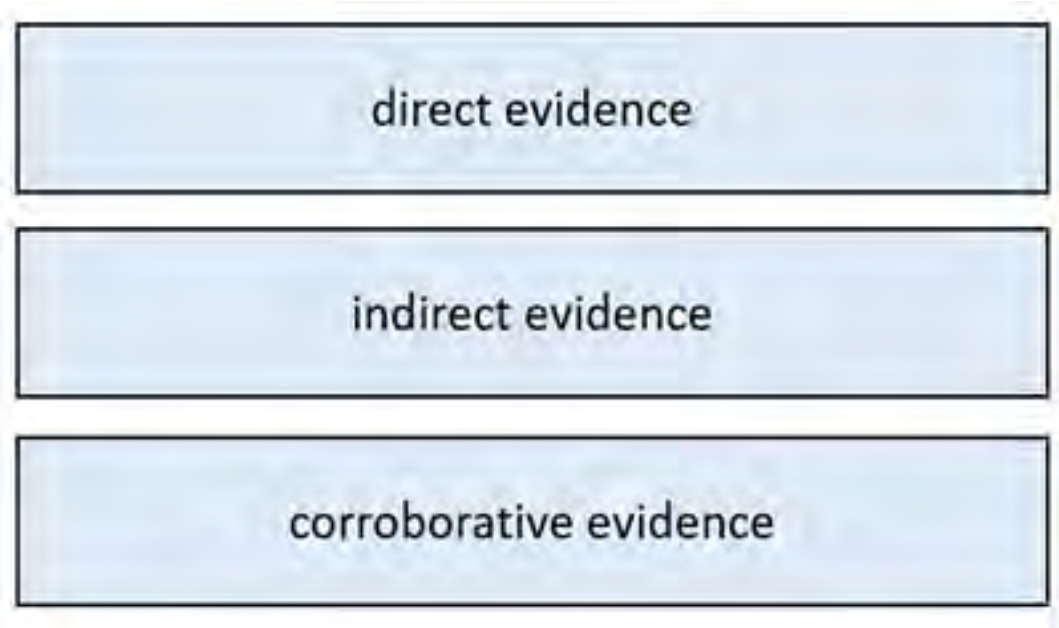
Drag and drop the type of evidence from the left onto the description of that evidence on the right.



**Answer:**




**Explanation:**




Graphical user interface, application

Description automatically generated

## Question No : 5

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: B**

**Question No : 6**

An analyst received an alert on their desktop computer showing that an attack was successful on the host. After investigating, the analyst discovered that no mitigation action occurred during the attack. What is the reason for this discrepancy?

**A.** The computer has a HIPS installed on it.
**B.** The computer has a NIPS installed on it.
**C.** The computer has a HIDS installed on it.
**D.** The computer has a NIDS installed on it.

**Answer: C**

**Question No : 7**

A user received a targeted spear-phishing email and identified it as suspicious before opening the content. To which category of the Cyber Kill Chain model does to this type of event belong?

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

**Answer: B**

**Question No : 8**

What is a difference between tampered and untampered disk images?

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

**Answer: D**

**Explanation:** The disk image must be intact for forensics analysis. As a cybersecurity professional, you may be given the task of capturing an image of a disk in a forensic manner. Imagine a security incident has occurred on a system and you are required to perform some forensic investigation to determine who and what caused the attack. Additionally, you want to ensure the data that was captured is not tampered with or modified during the creation of a disk image process. Ref: Cisco Certified CyberOps Associate 200-201 Certification Guide

**Question No : 9**

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**

**Question No : 10**

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**

## Question No : 11

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**

## Question No : 12

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**

## Question No : 13

At which layer is deep packet inspection investigated on a firewall?

**A.** internet
**B.** transport
**C.** application
**D.** data link

**Answer: C**

**Explanation:**

Deep packet inspection is a form of packet filtering usually carried out as a function of your firewall. It is applied at the Open Systems Interconnection's application layer. Deep packet inspection evaluates the contents of a packet that is going through a checkpoint.

## Question No : 14

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** | 0805d0ae62f5358b9a3f4c1868d552f5c3561b17 |
| **SHA256** | 27cced58a0fcbb0bbe3894f74d3014611039fefdf3bd2b0ba7ad85b18194c |
| **SHA512** | 5a43bc7eef279b209e2590432cc3e2eb480d0f78004e265f00b98b4afdc9a |
| **Ssdeep** | 1536:p0AAH2KthGBjcdBj8VETeePxsT65ZZ3pdx/ves/SQR/875+:prahGV6B |
| **PEiD** | None matched |
| **Yara** | • embedded_pe (Contains an embedded PE32 file)<br>• embedded_win_api (A non-Windows executable contains win32 API<br>• vmdetect (Possibly employs anti-virtualization techniques) |
| **VirusTotal** | Permalink<br>VirusTotal Scan Date: 2013-12-27 06:51:52<br>Detection Rate: 32/46 (collapse) |

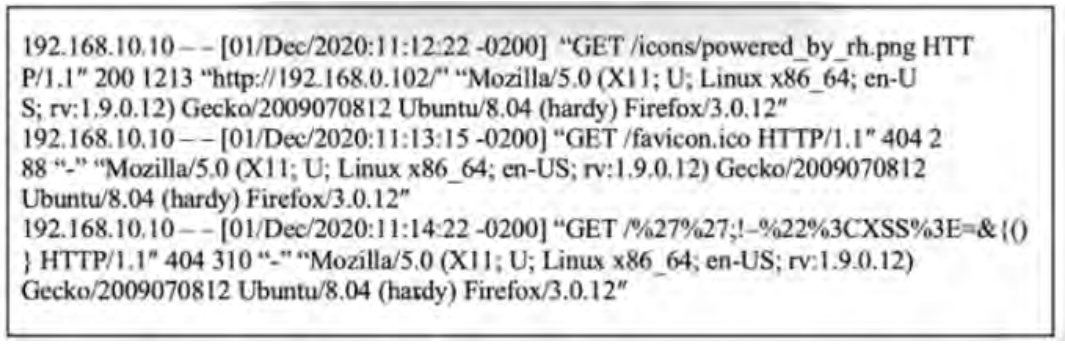
An engineer is analyzing this Cuckoo Sandbox report for a PDF file that has been downloaded from an email. What is the state of this file?

**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**

## Question No : 15

Refer to the exhibit.



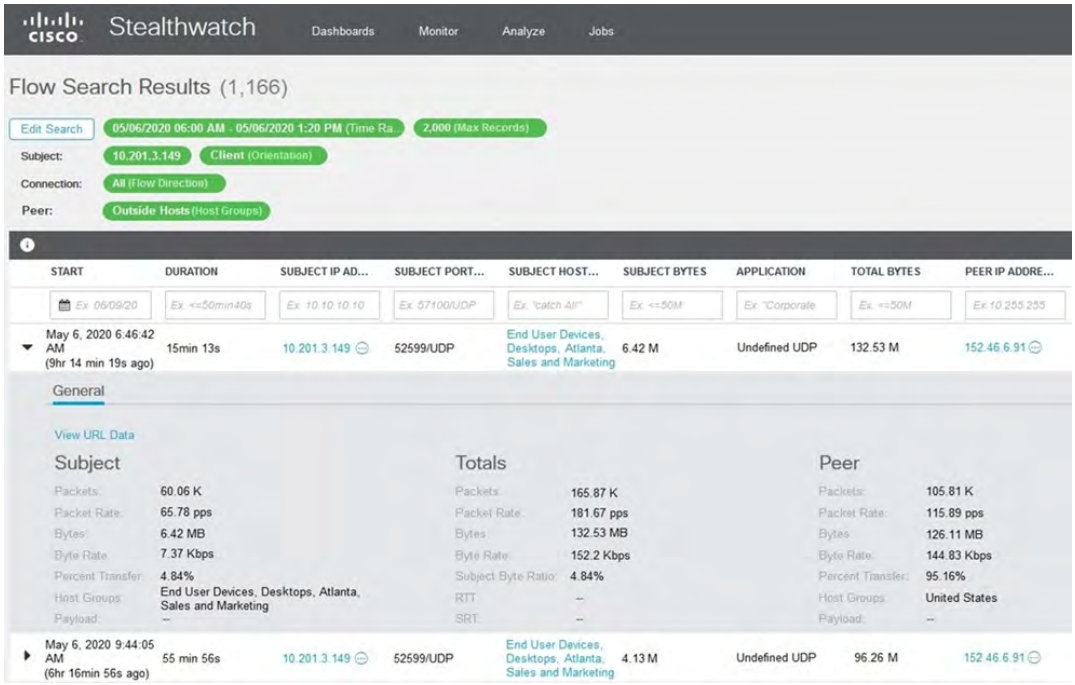

What is occurring?

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

**Answer: B**

## Question No : 16

Refer to the exhibit.




What is the potential threat identified in this Stealthwatch dashboard?

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

**Answer: D**

## Question No : 17

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**
Reference: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

**Question No : 18**

What is the practice of giving employees only those permissions necessary to perform their specific role within an organization?

**A.** least privilege
**B.** need to know
**C.** integrity validation
**D.** due diligence

**Answer: A**

**Question No : 19**

What is a benefit of using asymmetric cryptography?

**A.** decrypts data with one key
**B.** fast data transfer
**C.** secure data transfer
**D.** encrypts data with one key

**Answer: B**

**Question No : 20**

What makes HTTPS traffic difficult to monitor?

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

**Answer: D**

**Question No : 21**

What is a difference between SIEM and SOAR?

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

**Answer: B**
Reference: https://www.cisco.com/c/en/us/products/security/what-is-a-security-platform.html

siem is log managment soar is vulnerability managment that automat and response

## Question No : 22


Refer to the exhibit. An attacker scanned the server using Nmap. What did the attacker obtain from this scan?

**A.** Identified a firewall device preventing the pert 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**

**Question No : 23**

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

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

**Answer: C,E**

**Question No : 24**

What is the virtual address space for a Windows process?

**A.** physical location of an object in memory
**B.** set of pages that reside in the physical memory
**C.** system-level memory protection feature built into the operating system
**D.** set of virtual memory addresses that can be used

**Answer: D**

**Question No : 25**

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 No : 26

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 No : 27

What is the difference between the ACK flag and the RST flag?

**A.** The RST flag approves the connection, and the ACK flag terminates spontaneous connections.
**B.** The ACK flag confirms the received segment, and the RST flag terminates the connection.
**C.** The RST flag approves the connection, and the ACK flag indicates that a packet needs to be resent
**D.** The ACK flag marks the connection as reliable, and the RST flag indicates the failure within TCP Handshake

**Answer: B**

## Question No : 28

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.