# 200-201 Q&As

Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)

## Pass Cisco 200-201 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

**https://www.leads4pass.com/200-201.html**

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco Official Exam Center

**QUESTION 1**

What is a difference between inline traffic interrogation and traffic mirroring?

A. Inline inspection acts on the original traffic data flow

B. Traffic mirroring passes live traffic to a tool for blocking

C. Traffic mirroring inspects live traffic for analysis and mitigation

D. Inline traffic copies packets for analysis and security

Correct Answer: A

Inline traffic interrogation analyzes traffic in real time and has the ability to prevent certain traffic from being forwarded Traffic mirroring doesn\\'t pass the live traffic instead it copies traffic from one or more source ports and sends the copied traffic to one or more destinations for analysis by a network analyzer or other monitoring device

**QUESTION 2**

What describes the defense-m-depth principle?

A. defining precise guidelines for new workstation installations

B. categorizing critical assets within the organization

C. isolating guest Wi-Fi from the focal network

D. implementing alerts for unexpected asset malfunctions

Correct Answer: C

**QUESTION 3**

According to CVSS, what is attack complexity?

A. existing exploits available in the wild exploiting the vulnerability

B. existing circumstances beyond the attacker\\'s control to exploit the vulnerability

C. number of actions an attacker should perform to exploit the vulnerability

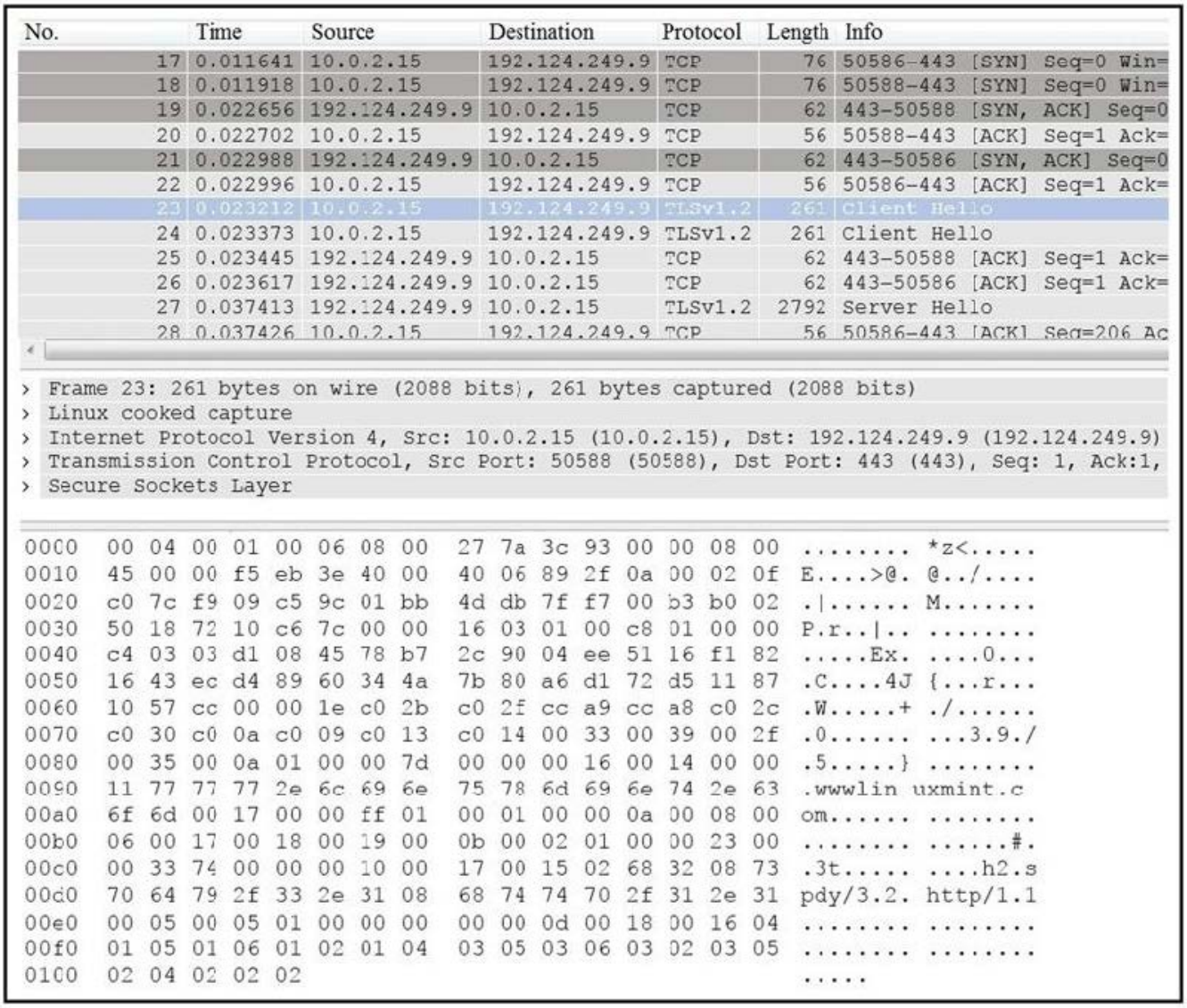
D. number of patches available for certain attack mitigation and how complex the workarounds are

Correct Answer: B

**QUESTION 4**

DRAG DROP

Refer to the exhibit.



| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 17 | 0.011641 | 10.0.2.15 | 192.124.249.9 | TCP | 76 | 50586-443 [SYN] Seq=0 Win= |
| 18 | 0.011918 | 10.0.2.15 | 192.124.249.9 | TCP | 76 | 50588-443 [SYN] Seq=0 Win= |
| 19 | 0.022656 | 192.124.249.9 | 10.0.2.15 | TCP | 62 | 443-50588 [SYN, ACK] Seq=0 |
| 20 | 0.022702 | 10.0.2.15 | 192.124.249.9 | TCP | 56 | 50588-443 [ACK] Seq=1 Ack= |
| 21 | 0.022988 | 192.124.249.9 | 10.0.2.15 | TCP | 62 | 443-50586 [SYN, ACK] Seq=0 |
| 22 | 0.022996 | 10.0.2.15 | 192.124.249.9 | TCP | 56 | 50586-443 [ACK] Seq=1 Ack= |
| 23 | 0.023212 | 10.0.2.15 | 192.124.249.9 | TLSv1.2 | 261 | Client Hello |
| 24 | 0.023373 | 10.0.2.15 | 192.124.249.9 | TLSv1.2 | 261 | Client Hello |
| 25 | 0.023445 | 192.124.249.9 | 10.0.2.15 | TCP | 62 | 443-50588 [ACK] Seq=1 Ack= |
| 26 | 0.023617 | 192.124.249.9 | 10.0.2.15 | TCP | 62 | 443-50586 [ACK] Seq=1 Ack= |
| 27 | 0.037413 | 192.124.249.9 | 10.0.2.15 | TLSv1.2 | 2792 | Server Hello |
| 28 | 0.037426 | 10.0.2.15 | 192.124.249.9 | TCP | 56 | 50586-443 [ACK] Seq=206 Ac |

```
> Frame 23: 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: 50588 (50588), Dst Port: 443 (443), Seq: 1, Ack:1,
> Secure Sockets Layer
```

```
0000  00 04 00 01 00 06 08 00  27 7a 3c 93 00 00 08 00  ........ 'z<.....
0010  45 00 00 f5 eb 3e 40 00  40 06 89 2f 0a 00 02 0f  E....>@. @../....
0020  c0 7c f9 09 c5 9c 01 bb  4d db 7f f7 00 b3 b0 02  .|...... M.......
0030  50 18 72 10 c6 7c 00 00  16 03 01 00 c8 01 00 00  P.r..|.. ........
0040  c4 03 03 d1 08 45 78 b7  2c 90 04 ee 51 16 f1 82  .....Ex. ....0...
0050  16 43 ec d4 89 60 34 4a  7b 80 a6 d1 72 d5 11 87  .C....4J {...r...
0060  10 57 cc 00 00 1e c0 2b  c0 2f cc a9 cc a8 c0 2c  .W.....+ ./......
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/3.2. 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                                    .....
```

Drag and drop the element name from the left onto the correct piece of the PCAP file on the right.

Select and Place:

| | |
|---|---|
| source address | 10.0.2.15 |
| destination address | 50588 |
| source port | 443 |
| destination port | 192.124.249.9 |
| Network Protocol | Transmission Control Protocol |
| Transport Protocol | Internet Protocol v4 |
| Application Protocol | Transport Layer Security v1.2 |

Correct Answer:

| | |
|---|---|
| | source address |
| | source port |
| | destination port |
| | destination address |
| | Transport Protocol |
| | Network Protocol |
| | Application Protocol |

**QUESTION 5**

What is a Heartbleed vulnerability?

A. denial of service

B. information disclosure

C. buffer overflow

D. command injection

Correct Answer: B

**QUESTION 6**

Which of these describes volatile evidence?

A. logs

B. registers and cache

C. disk and removable drives

D. usernames

Correct Answer: B

Caches and Registers- Data in memory is the most volatile. This includes data in centralprocessor unit (CPU) registers, caches, and system random access memory(RAM).- The data in cache and CPU registers is the most volatile,

mostlybecause the storage space is so small.

https://blogs.getcertifiedgetahead.com/cfr-and-order-of-volatility/#:~:text=Caches%20and%20Registers,storage%20space%20is%20so%20small.

**QUESTION 7**

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.

Correct Answer: B

**QUESTION 8**

Which regular expression is needed to capture the IP address 192.168.20.232?

A. ^ (?:[0-9]{1,3}\.){3}[0-9]{1,3}

B. ^ (?:[0-9]f1,3}\.){1,4}

C. ^ (?:[0-9]{1,3}\.)\\'

D. ^ ([0-9]-{3})

Correct Answer: A

Reference: https://www.cisco.com/c/en/us/td/docs/security/security_management/cs-mars/4-3/user/guide/local_controller/appreexp.html

**QUESTION 9**

What is the role of NAT in data visibility?

A. load balancing

B. hiding IP addresses

C. web filtering

D. encrypting files

Correct Answer: B

**QUESTION 10**

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

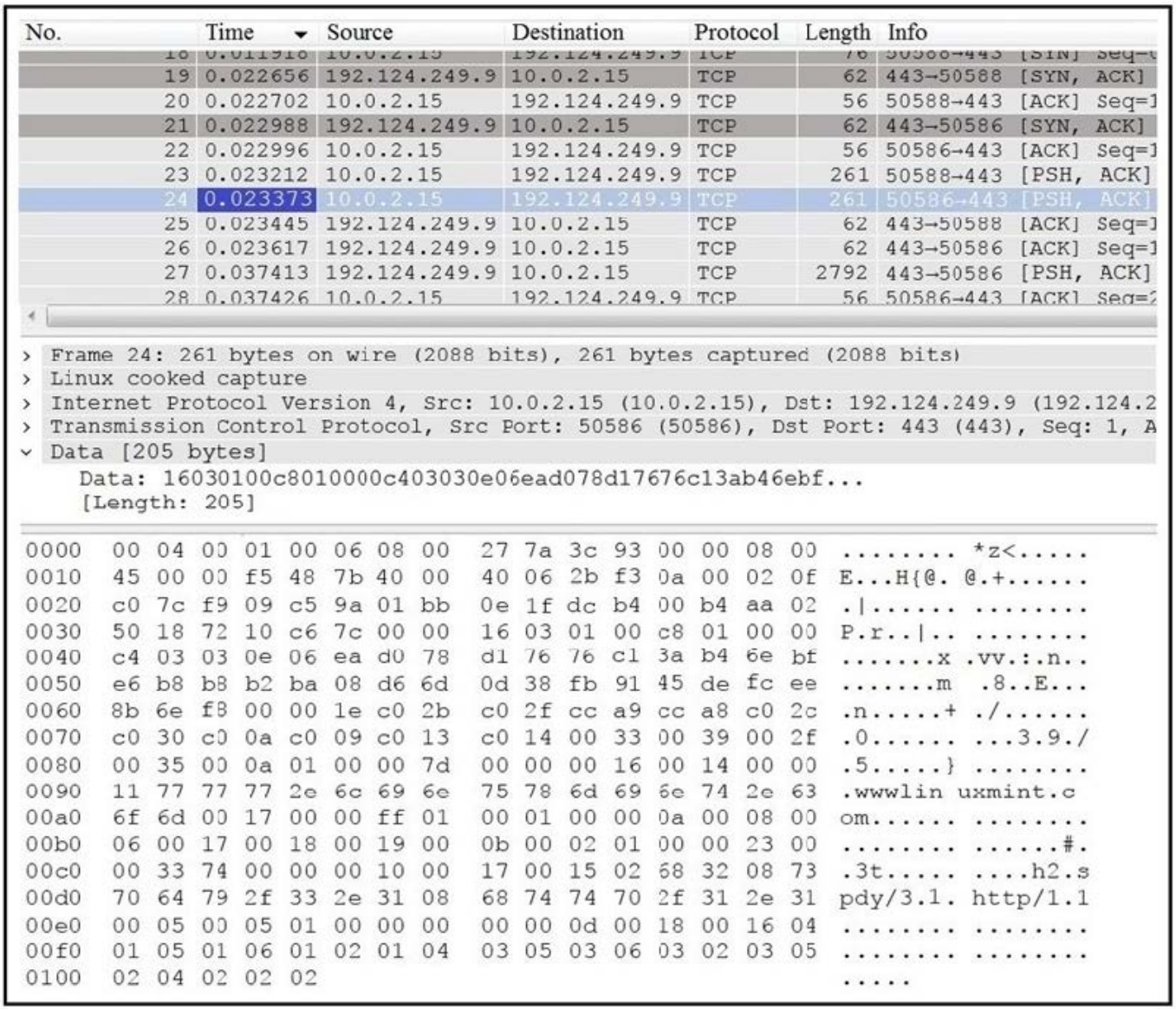
D. metrics collection and exporting

E. application recognition

Correct Answer: AE

**QUESTION 11**

Refer to the exhibit.




Which application protocol is in this PCAP file?

A. SSH

B. TCP

C. TLS

D. HTTP

Correct Answer: C

**QUESTION 12**

Refer to the exhibit.

**File Details**

| | |
|---|---|
| **File name** | lfile_saw.exe |
| **File size** | 95084 bytes |
| **File type** | PE32 executable (GUI) Intel 80386, for MS Windows |
| **CRC32** | 3D2C6A23 |
| **MD5** | d215cb65b405ab31b1b516a781c6b1ed |
| **SHA1** | 1a855455a912c721b42f2665a9a0365b97d68a42 |
| **SHA256** | e24669e5a2f74ab567c72d5030abedc4ed9f90ba23436b8db43b8fe63adecdd2 |
| **SHA512** | 56dbf450d5908bf958cd11928d7c1bf847ee82613e006fc692888872281f69ca370aae3d93c2b803febc3372845bb5ef36b |
| **Ssdeep** | 1536:WfX+sEYF75idaQwndckc9esY3iSa4Hlp2uLEKBa0e3IyWTWc80MzY75:qXBEYF7KmQwnRc9esYSSG9fnxdW4vS |
| **PEiD** | None matched |
| **Yara** | • zeus_1 (Zeus Trojan) |

A SOC engineer is analyzing the provided Cuckoo Sandbox report for a file that has been downloaded from an URL, received via email. What is the state of this file?

A. The file was identified as PE32 executable for MS Windows and the Yara filed lists it as Trojan.

B. The file was detected as executable and was matched by PEiD threat signatures for further analysis.

C. The file was detected as executable, but no suspicious features are identified.

D. The calculated SHA256 hash of the file was matched and identified as malicious.

Correct Answer: A

**QUESTION 13**

What is session data used for in network security?

A. It contains the set of parameters used for fetching logs.

B. It tracks cookies within each session initiated from user.

C. It is the transaction log between monitoring software.

D. It is the summary of the transmission between two network devices.

Correct Answer: D

Session data is a record of a conversation between two network endpoints, which are often a client and a server.

**QUESTION 14**

Which example represents the defense-in-depth principle?

A. implementing a CMDB

B. creating a separate VLAN to isolate networks

C. creating a privileged group in AD

D. implementing new security policy within the organization

Correct Answer: B

**QUESTION 15**

How does statistical detection differ from rule-based detection?

A. Statistical detection involves the evaluation of events, and rule-based detection requires an evaluated set of events to function.

B. Statistical detection defines legitimate data over time, and rule-based detection works on a predefined set of rules

C. Rule-based detection involves the evaluation of events, and statistical detection requires an evaluated set of events to function Rule-based detection defines

D. legitimate data over a period of time, and statistical detection works on a predefined set of rules

Correct Answer: B