

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.certbus.com/200-201.html>

100% Passing Guarantee
100% Money Back Assurance

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

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers



QUESTION 1

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.

Correct Answer: B

QUESTION 2

Refer to the exhibit.

```
Nov 30 17:48:38 ip-172-31-27-153 sshd[22997]: Invalid user password from 218.26.11.11
Nov 30 17:48:39 ip-172-31-27-153 sshd[22997]: Invalid user password from 218.26.11.11
Nov 30 17:48:41 ip-172-31-27-153 sshd[22999]: Invalid user password from 218.26.11.11
Nov 30 17:48:41 ip-172-31-27-153 sshd[22999]: Invalid user password from 218.26.11.11
Nov 30 17:48:41 ip-172-31-27-153 sshd[22999]: Invalid user password from 218.26.11.11
Nov 30 17:48:41 ip-172-31-27-153 sshd[22999]: Invalid user password from 218.26.11.11
Nov 30 17:48:43 ip-172-31-27-153 sshd[23001]: Invalid user password from 218.26.11.11
Nov 30 17:48:43 ip-172-31-27-153 sshd[23001]: Invalid user password from 218.26.11.11
Nov 30 17:48:43 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[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 17:48:48 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 17:48:49 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[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 file1?

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

Correct Answer: D

QUESTION 3

Which evasion technique is a function of ransomware?

- A. extended sleep calls

- B. encryption
- C. resource exhaustion
- D. encoding

Correct Answer: B

QUESTION 4

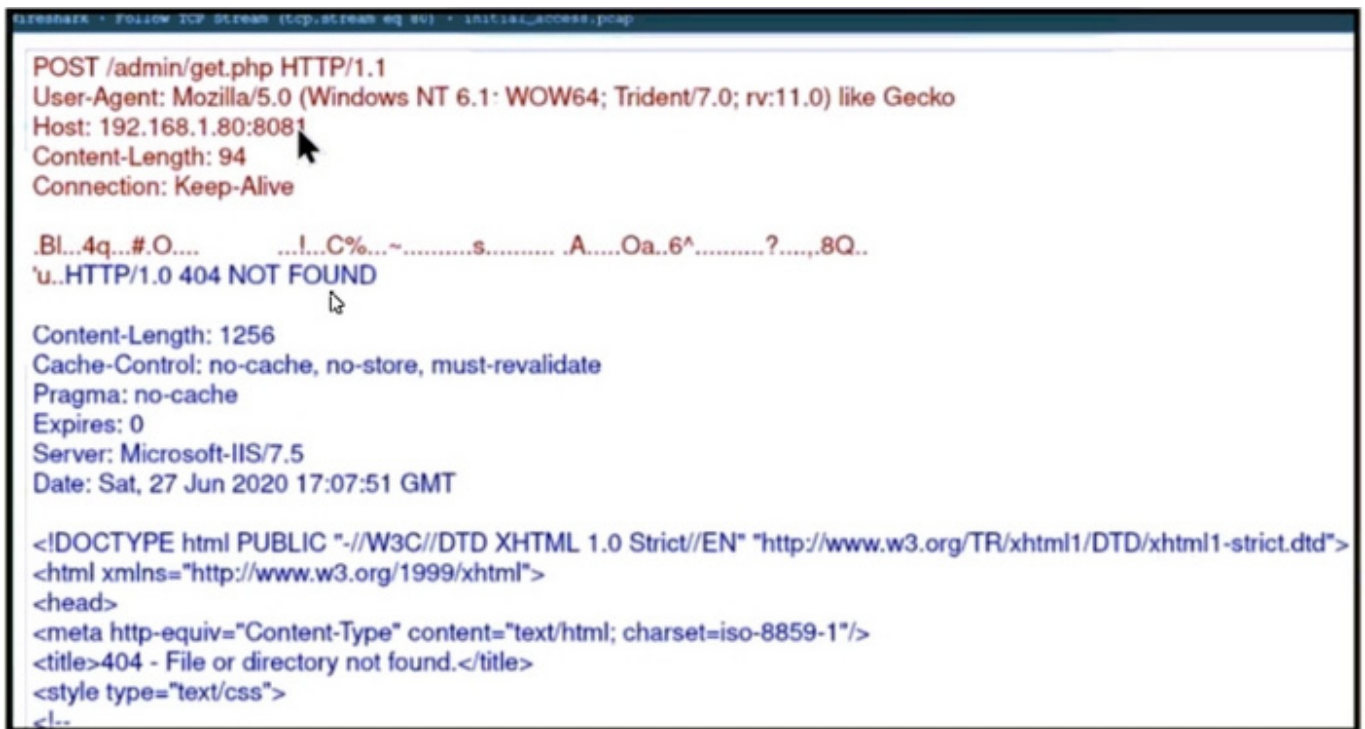
What is an example of social engineering attacks?

- A. receiving an unexpected email from an unknown person with an attachment from someone in the same company
- B. receiving an email from human resources requesting a visit to their secure website to update contact information
- C. sending a verbal request to an administrator who knows how to change an account password
- D. receiving an invitation to the department's weekly WebEx meeting

Correct Answer: C

QUESTION 5

Refer to the exhibit.



```
POST /admin/get.php HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: 192.168.1.80:8081
Content-Length: 94
Connection: Keep-Alive

.BI..4q...#..O....   ...!..C%...~.....s..... A....Oa..6^.....?.....8Q..
'u..HTTP/1.0 404 NOT FOUND

Content-Length: 1256
Cache-Control: no-cache, no-store, must-revalidate
Pragma: no-cache
Expires: 0
Server: Microsoft-IIS/7.5
Date: Sat, 27 Jun 2020 17:07:51 GMT

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/>
<title>404 - File or directory not found.</title>
<style type="text/css">
<!--
```

A security analyst received a ticket about suspicious traffic from one of the workstations. During the investigation, the analyst discovered that the workstation is communicating with an external IP. The analyst was not able to investigate further and escalated the case to a T2 security analyst. What are the two data visibility challenges that the security

analyst should identify? (Choose two.)

- A. A default user agent is present in the headers.
- B. Traffic is not encrypted.
- C. Encrypted data is being transmitted.
- D. POST requests have a "Microsoft-IIS/7.5" server header.
- E. HTTP requests and responses are sent in plaintext.

Correct Answer: BE

QUESTION 6

An engineer configured regular expression ".*\.[Dd][Oo][Cc][Xx][Ll][Ss][Pp][Pp][Tt) HTTP/1.[01]" on Cisco ASA firewall. What does this regular expression do?

- A. It captures .doc, .xls, and .pdf files in HTTP v1.0 and v1.1.
- B. It captures documents in an HTTP network session.
- C. It captures Word, Excel, and PowerPoint files in HTTP v1.0 and v1.1.
- D. It captures .doc, .xls, and .ppt files extensions in HTTP v1.0.

Correct Answer: C

Explanation:

The regular expression pattern captures file extensions like .doc, .xls, and .ppt (or variations in letter case, such as DOC, XLS, PPT) within HTTP traffic sessions, as indicated by the ".([Dd][Oo][Cc][Xx][Ll][Ss][Pp][Pp][Tt)" part of the regex.

Additionally, it specifies HTTP versions 1.0 and 1.1 by ending with " HTTP/1.[01]" to focus the matching on HTTP sessions using these versions.

QUESTION 7

Refer to the exhibit.

```
$ cuckoo submit --machine cuckoo1 /path/to/binary
```

Which event is occurring?

- A. A binary named "submit" is running on VM cuckoo1.

- B. A binary is being submitted to run on VM cuckoo1
- C. A binary on VM cuckoo1 is being submitted for evaluation
- D. A URL is being evaluated to see if it has a malicious binary

Correct Answer: B

<https://cuckoo.readthedocs.io/en/latest/usage/submit/>

QUESTION 8

Refer to the exhibit.

No.	Time	Source	Destination	Protocol	Info
30225	*REF*	192.168.10.1	192.168.10.132	POP	C: PASS eeeeevw
30226	0.000422	192.168.10.1	192.168.10.132	POP	C: PASS eeeeevw
30264	0.074131	192.168.10.1	192.168.10.132	POP	C: PASS eeeeevy
30312	0.199417	192.168.10.1	192.168.10.132	POP	C: PASS eeeeevY
30322	0.249480	192.168.10.1	192.168.10.132	POP	C: PASS eeeeevb
30325	0.262069	192.168.10.1	192.168.10.132	POP	C: PASS eeeeevB
30326	0.262111	192.168.10.1	192.168.10.132	POP	C: PASS eeeeevv
30330	0.277704	192.168.10.1	192.168.10.132	POP	C: PASS eeeeevV
30331	0.277711	192.168.10.1	192.168.10.132	POP	C: PASS eeeeevK
30332	0.277711	192.168.10.1	192.168.10.132	POP	C: PASS eeeeevk
30345	0.327554	192.168.10.1	192.168.10.132	POP	C: PASS eeeeevx
30346	0.327642	192.168.10.1	192.168.10.132	POP	C: PASS eeeeevX

Which alert is identified from this packet capture?

- A. man-in-the-middle attack
- B. brute-force attack
- C. ARP poisoning
- D. SQL injection

Correct Answer: B

QUESTION 9

A CMS plugin creates two files that are accessible from the Internet: myplugin.html and exploitable.php. A newly discovered exploit takes advantage of an injection vulnerability in exploitable.php. To exploit the vulnerability, an HTTP POST must be sent with specific variables to exploitable.php. A security engineer notices traffic to the webserver that consists of only HTTP GET requests to myplugin.html. Which category does this activity fall under?

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

Correct Answer: B

QUESTION 10

Which option describes indicators of attack?

- A. blocked phishing attempt on a company
- B. spam emails on an employee workstation
- C. virus detection by the AV software
- D. malware reinfection within a few minutes of removal

Correct Answer: D

QUESTION 11

16	0.000188	76.196.12.250	192.168.0.1	TCP	54	12033	→ 80	[SYN]	Seq=0	Win=16384	Len=0
17	0.000189	164.124.33.94	192.168.0.1	TCP	54	35181	→ 80	[SYN]	Seq=0	Win=16384	Len=0
18	0.000191	164.124.33.160	192.168.0.1	TCP	54	35247	→ 80	[SYN]	Seq=0	Win=16384	Len=0
19	0.000193	38.198.26.94	192.168.0.1	TCP	54	14463	→ 80	[SYN]	Seq=0	Win=16384	Len=0
20	0.000195	132.212.36.219	192.168.0.1	TCP	54	31962	→ 80	[SYN]	Seq=0	Win=16384	Len=0
21	0.000466	164.124.33.172	192.168.0.1	TCP	54	35259	→ 80	[SYN]	Seq=0	Win=16384	Len=0
22	0.000468	164.124.33.90	192.168.0.1	TCP	54	35177	→ 80	[SYN]	Seq=0	Win=16384	Len=0
23	0.000470	132.212.36.218	192.168.0.1	TCP	54	31961	→ 80	[SYN]	Seq=0	Win=16384	Len=0
24	0.000471	164.124.33.70	192.168.0.1	TCP	54	35157	→ 80	[SYN]	Seq=0	Win=16384	Len=0
25	0.000473	76.196.12.237	192.168.0.1	TCP	54	12020	→ 80	[SYN]	Seq=0	Win=16384	Len=0
26	0.000475	164.124.33.73	192.168.0.1	TCP	54	35160	→ 80	[SYN]	Seq=0	Win=16384	Len=0
27	0.000476	189.109.37.206	192.168.0.1	TCP	54	36102	→ 80	[SYN]	Seq=0	Win=16384	Len=0
28	0.000478	164.124.33.71	192.168.0.1	TCP	54	35158	→ 80	[SYN]	Seq=0	Win=16384	Len=0
29	0.000480	61.141.8.140	192.168.0.1	TCP	54	10644	→ 80	[SYN]	Seq=0	Win=16384	Len=0

Refer to the exhibit. What is occurring?

- A. ARP spoofing attack
- B. man-in-the-middle attack
- C. brute-force attack
- D. denial-of-service attack

Correct Answer: D

QUESTION 12

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

Correct Answer: B

Reference: [https://www.paubox.com/blog/what-is-threat-actor/#:~:text=The%20term%20threat%20actor%20refers,CTA\)%20when%20referencing%20cybersecurity%20issues](https://www.paubox.com/blog/what-is-threat-actor/#:~:text=The%20term%20threat%20actor%20refers,CTA)%20when%20referencing%20cybersecurity%20issues)

QUESTION 13

What is a description of a man-in-the-middle network attack?

- A. After attackers penetrate a network, they can use privilege escalation to expand their reach.
- B. Attackers build botnets, large fleets of compromised devices, and use them to direct false traffic at networks or servers.
- C. It involves attackers intercepting traffic, either between a network and external sites or within a network.
- D. Attackers replicate malicious traffic as legitimate and bypass network protection solutions.

Correct Answer: C

QUESTION 14

Refer to the exhibit.

No.	Time	Source	Destination	Protoc	Length	Info
6	16:40:35.636314	195.144.107.198	192.168.31.44	FTP	104	Response: 227 Entering Passive Mode (195,144,107,198,4,2).
7	16:40:35.637786	192.168.31.44	195.144.107.198	FTP	82	Request: RETR ResumableTransfer.png
8	16:40:35.638091	192.168.31.44	195.144.107.198	TCP	66	1084 → 1026 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
9	16:40:35.696788	195.144.107.198	192.168.31.44	FTP	96	Response: 150 Opening BINARY mode data connection.
10	16:40:35.698384	195.144.107.198	192.168.31.44	TCP	66	1026 → 1084 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1456 WS=256 SACK_
11	16:40:35.698521	192.168.31.44	195.144.107.198	TCP	54	1024 → 1026 [ACK] Seq=1 Ack=1 Win=132352 Len=0
12	16:40:35.698802	192.168.31.44	195.144.107.198	TCP	54	[TCP Windows Update] 1084 → 1026 [ACK] Seq=1 Ack=1 Win=4194304 Len=0
13	16:40:35.739249	192.168.31.44	195.144.107.198	TCP	54	1031 → 21 [ACK] Seq=43 Ack=113 Win=513 Len=0
14	16:40:35.759825	195.144.107.198	192.168.31.44	FTP...	2966	FTP Data: 2912 bytes (PASV) (RETR ResumableTransfer.png)
15	16:40:35.759925	192.168.31.44	195.144.107.198	TCP	54	1084 → 1026 [ACK] Seq=0 Ack=2913 Win=4194304 Len=0
16	16:40:35.822152	195.144.107.198	192.168.31.44	FTP...	5878	FTP Data: 5824 bytes (PASV) (RETR ResumableTransfer.png)
17	16:40:35.822263	192.168.31.44	195.144.107.198	TCP	54	1084 → 1026 [ACK] Seq=1 Ack=8737 Win=4194304 Len=0
18	16:40:35.883496	195.144.107.198	192.168.31.44	FTP...	1510	FTP Data: 1456 bytes (PASV) (RETR ResumableTransfer.png)
19	16:40:35.883496	195.144.107.198	192.168.31.44	FTP...	1408	FTP Data: 1354 bytes (PASV) (RETR ResumableTransfer.png)
20	16:40:35.883559	192.168.31.44	195.144.107.198	TCP	54	1084 → 1026 [ACK] Seq=1 Ack=11547 Win=4194304 Len=0
21	16:40:35.944841	195.144.107.198	192.168.31.44	FTP	78	Response: 226 Transfer complete.
22	16:40:35.944841	195.144.107.198	192.168.31.44	TCP	54	1026 → 1084 [FIN, ACK] Seq=11547 Ack=1 Win=66816 Len=0
23	16:40:35.944978	192.168.31.44	195.144.107.198	TCP	54	1084 → 1026 [ACK] Seq=0 Ack=11548 Win=4194304 Len=0
24	16:40:35.945371	192.168.31.44	195.144.107.198	TCP	54	1084 → 1026 [FIN, ACK] Seq=1 Ack=11548 Win=4194304 Len=0

```

> Frame 21: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface \Device\NPF_{E75C8230-BD9F-487C-B722-94BD6CF16174}, id 0...
> Ethernet II, Src: BeijingX_06:3f:00 (50:d2:f5:06:3f:00), Dst: IntelCor_7c:b2:fd (18:26:49:7c:b2:fd)
> Internet Protocol Version 4, Src: 195.144.107.198, Dst: 192.168.31.44
> Transmission Control Protocol, Src Port: 21, Dst Port: 1031, Seq: 113, Ack: 43, Len: 24
> File Transfer Protocol (FTP)
> [Current working directory: ]

```

Which frame numbers contain a file that is extractable via TCP stream within Wireshark?

- A. 7,14, and 21
- B. 7 and 21
- C. 14,16,18, and 19
- D. 7 to 21

Correct Answer: C

QUESTION 15

At a company party a guest asks questions about the company's user account format and password complexity. How is this type of conversation classified?

- A. Phishing attack
- B. Password Revelation Strategy
- C. Piggybacking
- D. Social Engineering

Correct Answer: D