



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.pass4itsure.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**

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 2

How is attacking a vulnerability categorized?

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

Correct Answer: C

QUESTION 3

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

Correct Answer: A

QUESTION 4

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

Correct Answer: A

Reference: https://www.tutorialspoint.com/http/http_requests.htm
<https://github.com/gwroblew/detectXSSlib/blob/master/test/attacks.txt>

QUESTION 5

Refer to the exhibit.



```
Wireshark - Follow TCP Stream (tcp.stream eq 80) - Initial Address: 192.168.1.80:8081
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

[Latest 200-201 Dumps](#)

[200-201 Practice Test](#)

[200-201 Braindumps](#)