



350-201^{Q&As}

Performing CyberOps Using Cisco Security Technologies (CBRCOR)

Pass Cisco 350-201 Exam with 100% Guarantee

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

<https://www.pass4itsure.com/350-201.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**

A security manager received an email from an anomaly detection service, that one of their contractors has downloaded 50 documents from the company's confidential document management folder using a company-owned asset al039-ice4ce687TL0500. A security manager reviewed the content of downloaded documents and noticed that the data affected is from different departments. What are the actions a security manager should take?

- A. Measure confidentiality level of downloaded documents.
- B. Report to the incident response team.
- C. Escalate to contractor's manager.
- D. Communicate with the contractor to identify the motives.

Correct Answer: B

QUESTION 2

Refer to the exhibit. An engineer notices a significant anomaly in the traffic in one of the host groups in Cisco Secure Network Analytics (Stealthwatch) and must analyze the top data transmissions. Which tool accomplishes this task?

- A. Top Peers
- B. Top Hosts
- C. Top Conversations
- D. Top Ports

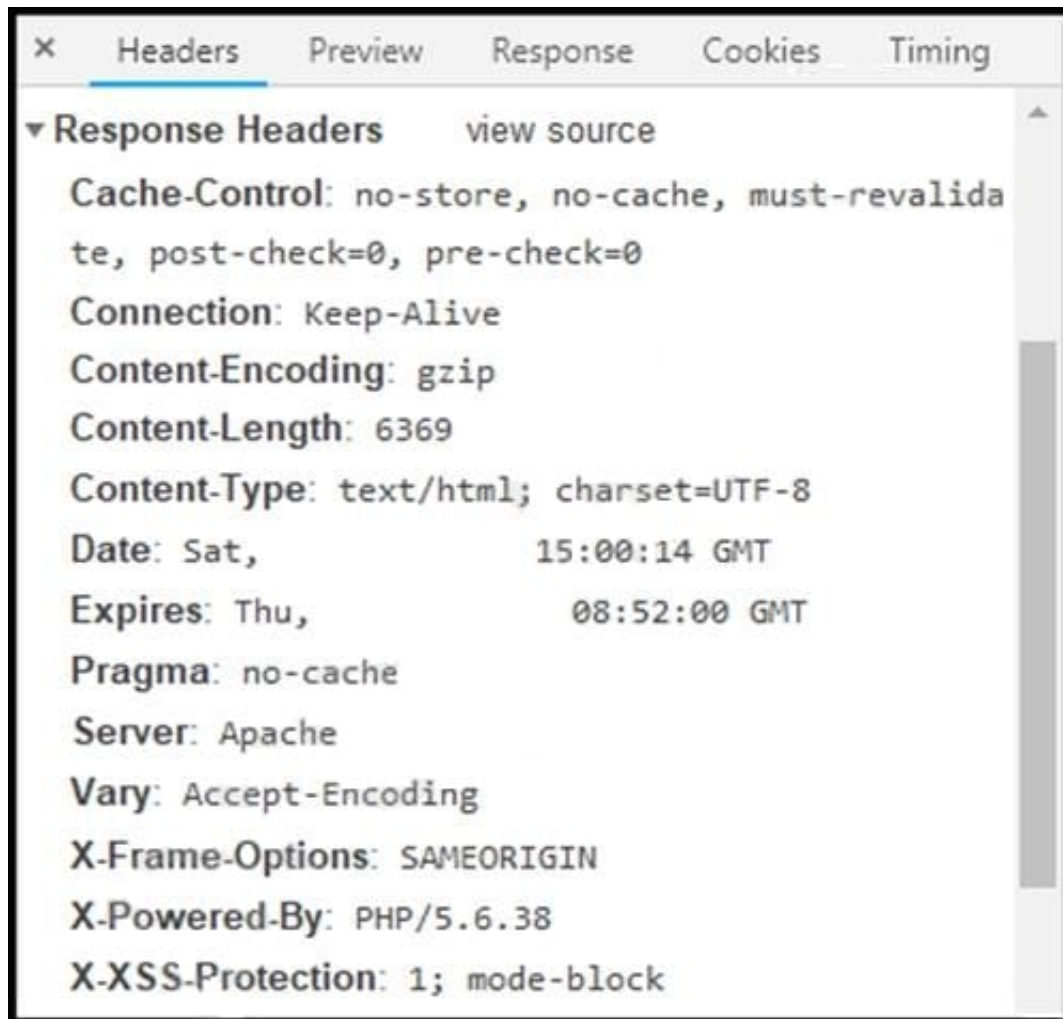


Correct Answer: B

Reference: <https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2018/pdf/BRKSEC-3014.pdf>

QUESTION 3

Refer to the exhibit. Where are the browser page rendering permissions displayed?



- A. X-Frame-Options
- B. X-XSS-Protection
- C. Content-Type
- D. Cache-Control

Correct Answer: C



QUESTION 4

An engineer receives an incident ticket with hundreds of intrusion alerts that require investigation. An analysis of the incident log shows that the alerts are from trusted IP addresses and internal devices. The final incident report stated that these alerts were false positives and that no intrusions were detected.

What action should be taken to harden the network?

- A. Move the IPS to after the firewall facing the internal network
- B. Move the IPS to before the firewall facing the outside network
- C. Configure the proxy service on the IPS
- D. Configure reverse port forwarding on the IPS

Correct Answer: C

QUESTION 5

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.0.2	10.128.0.2	TCP	54	3341 -> 80 [SYN] Seq=0 Win=512 Len=0
2	0.003987	10.128.0.2	10.0.0.2	TCP	58	80 -> 3222 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
3	0.005514	10.128.0.2	10.0.0.2	TCP	54	80 -> 3341 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
4	0.008429	10.0.0.2	10.128.0.2	TCP	54	3342 -> 80 [SYN] Seq=0 Win=512 Len=0
5	0.010233	10.128.0.2	10.0.0.2	TCP	58	80 -> 3220 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
6	0.014072	10.128.0.2	10.0.0.2	TCP	58	80 -> 3342 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
7	0.016830	10.0.0.2	10.128.0.2	TCP	54	3343 -> 80 [SYN] Seq=0 Win=512 Len=0
8	0.022220	10.128.0.2	10.0.0.2	TCP	58	80 -> 3343 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
9	0.023496	10.128.0.2	10.0.0.2	TCP	58	80 -> 3219 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
10	0.025243	10.0.0.2	10.128.0.2	TCP	58	3344 -> 80 [SYN] Seq=0 Win=512 Len=0
11	0.026672	10.128.0.2	10.0.0.2	TCP	58	80 -> 3218 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
12	0.028038	10.128.0.2	10.0.0.2	TCP	58	80 -> 3221 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
13	0.030523	10.128.0.2	10.0.0.2	TCP	58	80 -> 3344 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460

Frame 1 : 54 bytes on wire (432 bits), 54 bytes captured (432 bits)	
Ethernet II, Src: 42:01:0a:f0:00:17 (42:01:0a:f0:00:17), Dst: 42:01:0a:f0:00:01 (42:01:0a:f0:00:01)	
Internet Protocol Version 4, Src: 10.0.0.2, Dst: 10.128.0.2	
Transmission Control Protocol, Src Port: 3341, Dst Port: 80, Seq: 0, Len: 0	
Source port: 3341	
Destination port: 80	
[Stream index: 0]	
[TCP Segment Len: 0]	
Sequence number: 0 (relative sequence number)	
[Next sequence number: 0 (relative sequence number)]	
Acknowledgment number: 1023350804	
0101 = Header Length: 20 bytes (5)	
Flags: 0x002 (SYN)	
Window size value: 512	
[Calculated window size: 512]	
Checksum: 0x8d5a [unverified]	
[Checksum Status: Unverified]	
Urgent pointer: 0	
[Timestamps]	

Refer to the exhibit. What is the threat in this Wireshark traffic capture?

- A. A high rate of SYN packets being sent from multiple sources toward a single destination IP
- B. A flood of ACK packets coming from a single source IP to multiple destination IPs
- C. A high rate of SYN packets being sent from a single source IP toward multiple destination IPs



D. A flood of SYN packets coming from a single source IP to a single destination IP

Correct Answer: D

[350-201 VCE Dumps](#)

[350-201 Study Guide](#)

[350-201 Exam Questions](#)