

# 350-201<sup>Q&As</sup>

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.geekcert.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**

What is a benefit of key risk indicators?

- A. clear perspective into the risk position of an organization
- B. improved visibility on quantifiable information
- C. improved mitigation techniques for unknown threats
- D. clear procedures and processes for organizational risk

#### Correct Answer: C

Reference: https://www.metricstream.com/insights/Key-Risk-indicators-ERM.htm#:~:text=Risk%20Management%20(ERM)-,Overview,and%20mitigate%20them%20in%20time.

#### **QUESTION 2**

Elle Edit View Action	Help																		BIN: 102: 1033
		P				•		Dialo Merit	9	D		-	to	C	)	Ĉ	1	0	
- BIN	00019888	4D	54	90	00	03	00	00	00	04	00	00	00	TT	FF	00	00		
102 : 1033	000198B8	88	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00	1	e e
Manifest	000198C8	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	13	e
Contraction of the second s	00019808	00	00	00	00	00	00	00	00	00	00	00	00	C8	00	00	00		! L !Th
1 : 1033	00019828	OE	1F	BA	0E	00	84	09	CD	21	88	01	4C	CD	21	54	68		is program cannot
	00019878	69	73	20	70	72	6F	67	72	61	60	20	63	61	62	6E	6F		be run in DOS
	00019908	74	20	62	65	20	72	75	6E	20	69	6E	20	44	4E	53	20		mode. &
	00019918	6D	65	64	65	2E	OD	00	0A	24	00	00	00	00	00	00	00		v
	00019928	A7	C4	76	F6	E3	A5	18	25	E3	AS	18	A5	E3	<b>A</b> 5	18	AS		
	00019938	E3	A5	19	A5	EB	AS	18	<b>A</b> 5	EA	00	88	A5	E6	<b>A</b> 5	18	AS		Rich
	00019948	Eλ	DD	98	A5	E7	A5	18	45	EA	DD	89	AS	E2	A5	18	A5		PE L
	00019958	52	69	63	68	E3.	AS	18	AS	00	00	00	00	00	00	00	00		QV
	00019968	00	00	00	00	00	00	00	00	50	45	00	00	40	01	05	00		
	00019978	75	CC	51	56	00	0.0	0.0	00	00	00	00	00	E0	00	02	01		>@

Refer to the exhibit. An engineer is reverse engineering a suspicious file by examining its resources. What does this file indicate?

#### A. a DOS MZ executable format

B. a MS-DOS executable archive

- C. an archived malware
- D. a Windows executable file

Correct Answer: D

Reference: https://stackoverflow.com/questions/2577545/why-is-this-program-cannot-be-run-in-dos-mode-text-present-in-dll-

 $files \#: \sim: text = The \% 20 linker \% 20 places \% 20 a \% 20 default, using \% 20 the \% 20 \% 2 FSTUB \% 20 linker \% 20 option. and text = This \% 20 minute the first state of the first st$ 



%20information%20enables%20Windows%20to,has%20an%20MS-DOS%20stub.

### **QUESTION 3**

An engineer wants to review the packet overviews of SNORT alerts. When printing the SNORT alerts, all the packet headers are included, and the file is too large to utilize. Which action is needed to correct this problem?

A. Modify the alert rule to "output alert\_syslog: output log"

- B. Modify the output module rule to "output alert\_quick: output filename"
- C. Modify the alert rule to "output alert\_syslog: output header"
- D. Modify the output module rule to "output alert\_fast: output filename"

Correct Answer: A

 $Reference: https://snort-org-site.s3.amazonaws.com/production/document_files/files/000/000/249/original/snort_manual. pdf?X-Amz-Algorithm=AWS4-HMAC-SHA256andX-Amz-Credential=AKIAIXACIED2SPMSC7GA%2F20201231%2Fuse ast-1%2Fs3%2Faws4_requestandX-Amz-Date=20201231T141156ZandX-Amz-Expires=172800andX-Amz-SignedHead ers=hostandX-Amz-Signature=e122ab6eb1659e13b3bc6bb2451ce693c0298b76c1962c3743924bc5fd83d382$ 

#### **QUESTION 4**

An engineer received multiple reports from users trying to access a company website and instead of landing on the website, they are redirected to a malicious website that asks them to fill in sensitive personal data. Which type of attack is occurring?

- A. Address Resolution Protocol poisoning
- B. session hijacking attack
- C. teardrop attack
- D. Domain Name System poisoning
- Correct Answer: D

#### **QUESTION 5**



	0	4		đ			×	C	Q	<	> 3	Ŧ	+		0	1				×	0
Rer: (	webs	sochet.p	ryload							•	Expression	L. Clear	Apply	Save							
	1	Time					Source					Lengt	th.	Destination		Prot	lecel	Info			
528 528 528	43						2948. 149. 2958. 149.						551 547 314	296. 296. 296. 296.		Web5 Web5	ocket ocket ocket ocket	lebSocket lebSocket lebSocket lebSocket	Text Text Text	[FIN]	MASKED MASKED MASKED MASKED
thern #2.10 Intern Transe 3 Ana	et II Virt et Pr	on Cont	rol Pri	on 4, 5	Src Por	0:45: : 1029	(10.	), 0	), Dst:	206.	6332), Sec	206.									
thern #2.10 Intern ranse 3 Ana	et II Virt et Pr	on Cont	rol Pri	on 4, 5	Src Por	0:45: : 1029	(10.	30), 0 50), 0 67), 0 1	0. Dst: t Port: 2641(13)	206. 6332 ( 17), #5		206.		,							
Ethern M2.10 Intern	et II Virt et Pr	on Cont	rol Pri	on 4, 5	Src Por	0:45: : 1029	(10.	30), Dr 30), Dr 67), #7	), Dst: t Port: 2641(13)	206. 6332 ( 97), #5	6332), 54	206.		,							

Refer to the exhibit. An engineer is analyzing this Vlan0386-int12-117.pcap file in Wireshark after detecting a suspicious network activity. The origin header for the direct IP connections in the packets was initiated by a google chrome extension on a WebSocket protocol. The engineer checked message payloads to determine what information was being sent off-site but the payloads are obfuscated and unreadable.

What does this STIX indicate?

A. The extension is not performing as intended because of restrictions since ports 80 and 443 should be accessible

B. The traffic is legitimate as the google chrome extension is reaching out to check for updates and fetches this information

C. There is a possible data leak because payloads should be encoded as UTF-8 text

D. There is a malware that is communicating via encrypted channels to the command and control server

Correct Answer: C

350-201 VCE Dumps

350-201 Study Guide

350-201 Braindumps