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.leads4pass.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

Leads4Pass

800,000+ Satisfied Customers



Leads4Pass

QUESTION 1

A malware outbreak is detected by the SIEM and is confirmed as a true positive. The incident response team follows the playbook to mitigate the threat. What is the first action for the incident response team?

- A. Assess the network for unexpected behavior
- B. Isolate critical hosts from the network
- C. Patch detected vulnerabilities from critical hosts
- D. Perform analysis based on the established risk factors

Correct Answer: B

QUESTION 2

Elle Edit View Action	Help	_																	BIN: 102: 1033
🗅 💋 🖪 🐻		P	-			•		Dialo Merit	9	0		-	to	C)	Ċ	1	0	
BIN	00019848	4D	54	90	00	03	00	00	00	04	00	00	00	TT	TT	00	00		
102 : 1033	000198B8	88	1	-	00	00	00			40	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
	00019808	00	00	00	00	00	00	00	00	00	00	00	00	C8	00	00	00		! L !Th
L 2 1:1033	00019828	OE	1F	BA	0E	00	84	09	CD	21	38	01	4C	CD	21	54	68		is program cannot
	00019878	69	73	20	70	72	6F	67	72	61	60	20	63	61	6E	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	6F	64	65	2E	OD	00	0A	24	00	00	00	00	00	00	00		v
	00019928	A7	C4	76	F6	E3	A5	18	A5	E3	AS	18	AS	E3	25	18	AS		
	00019938	E3	AS	19	A5	EB	AS	18	AS	EA	00	88	A5	E6	A5	18	AS		Rich
	00019948	EA	DD	98	A5	E7	35	18	25	EA	DD	89	AS.	£2	A5	18	AS		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		201
	00019978	75	CC	51	56	00	00	0.0	00	00	00	00	00	EG	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-

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

Leads4Pass

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

QUESTION 3

A customer is using a central device to manage network devices over SNMPv2. A remote attacker caused a denial of service condition and can trigger this vulnerability by issuing a GET request for the ciscoFlashMIB OID on an affected device.

Which should be disabled to resolve the issue?

A. SNMPv2

- B. TCP small services
- C. port UDP 161 and 162
- D. UDP small services
- Correct Answer: A

Reference: https://nvd.nist.gov/vuln/detail/CVE-2018-0161

QUESTION 4

What is the HTTP response code when the REST API information requested by the authenticated user cannot be found?

- A. 401
- B. 402
- C. 403
- D. 404
- E. 405

Correct Answer: A

Reference: https://airbrake.io/blog/http-errors/401-unauthorizederror#:~:text=The%20401%20Unauthorized%20Error%20is,client%20could%20not%20be%20authenticated.

QUESTION 5

Leads4Pass

pragma: no-cache server: Apache status: 200 strict-transport-security: max-age=31536000 vary: Accept-Encoding x-content-type-options: nosniff x-frame-options: SAMEORIGIN x-test-debug: nURL=www.cisco.com, realm-0, isRealm=0, realmDomain=0, shortrealm=0 x-xss-protection: 1; mode=block

Refer to the exhibit. Where does it signify that a page will be stopped from loading when a scripting attack is detected?

- A. x-frame-options
- B. x-content-type-options
- C. x-xss-protection
- D. x-test-debug
- Correct Answer: C

Reference: https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/operations/customize-http-security-headers-ad-fs

Latest 350-201 Dumps

350-201 Study Guide

350-201 Exam Questions