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

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%2Fuseast-1%2Fs3%2Faws4_requestandX-Amz-Date=20201231T141156ZandX-Amz-Expires=172800andX-Amz-SignedHeaders=hostandX-Amz-Signature=e122ab6eb1659e13b3bc6bb2451ce693c0298b76c1962c3743924bc5fd83d382

QUESTION 2

A threat actor attacked an organization\\'s Active Directory server from a remote location, and in a thirty-minute timeframe, stole the password for the administrator account and attempted to access 3 company servers. The threat actor successfully accessed the first server that contained sales data, but no files were downloaded. A second server was also accessed that contained marketing information and 11 files were downloaded. When the threat actor accessed the third server that contained corporate financial data, the session was disconnected, and the administrator\\'s account was disabled.

Which activity triggered the behavior analytics tool?

A. accessing the Active Directory server

B. accessing the server with financial data

C. accessing multiple servers

D. downloading more than 10 files

Correct Answer: C

QUESTION 3

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 4

An analyst wants to upload an infected file containing sensitive information to a hybrid-analysis sandbox. According to the NIST.SP 800-150 guide to cyber threat information sharing, what is the analyst required to do before uploading the file to safeguard privacy?

A. Verify hash integrity.

B. Remove all personally identifiable information.

C. Ensure the online sandbox is GDPR compliant.

D. Lock the file to prevent unauthorized access.

Correct Answer: B

QUESTION 5

DRAG DROP

Drag and drop the type of attacks from the left onto the cyber kill chain stages at which the attacks are seen on the right.

Select and Place:

Answer Area

not visible to the victim	reconnaissance
virus scanner turning off	weaponization
malware placed on the targeted system	delivery
open port scans and multiple failed logins from the website	exploitation
large amount of data leaving the network through unusual ports	installation
system phones connecting to countries where no staff are located	command & control
USB with infected files inserted into company laptop	actions on objectives

Correct Answer:

Answer Area

	system phones connecting to countries where no staff are located
	malware placed on the targeted system
	not visible to the victim
	large amount of data leaving the network through unusual ports
	USB with infected files inserted into company laptop
	virus scanner turning off
	open port scans and multiple failed logins from the website

QUESTION 6

A SOC team receives multiple alerts by a rule that detects requests to malicious URLs and informs the incident response team to block the malicious URLs requested on the firewall. Which action will improve the effectiveness of the process?

A. Block local to remote HTTP/HTTPS requests on the firewall for users who triggered the rule.

B. Inform the user by enabling an automated email response when the rule is triggered.

C. Inform the incident response team by enabling an automated email response when the rule is triggered.

D. Create an automation script for blocking URLs on the firewall when the rule is triggered.

Correct Answer: A

QUESTION 7

A new malware variant is discovered hidden in pirated software that is distributed on the Internet. Executives have asked for an organizational risk assessment. The security officer is given a list of all assets. According to NIST, which two elements are missing to calculate the risk assessment? (Choose two.)

A. incident response playbooks

B. asset vulnerability assessment

C. report of staff members with asset relations

D. key assets and executives

E. malware analysis report

Correct Answer: BE

Reference: https://cloudogre.com/risk-assessment/

QUESTION 8

An engineer is utilizing interactive behavior analysis to test malware in a sandbox environment to see how the malware performs when it is successfully executed. A location is secured to perform reverse engineering on a piece of malware. What is the next step the engineer should take to analyze this malware?

A. Run the program through a debugger to see the sequential actions

B. Unpack the file in a sandbox to see how it reacts

C. Research the malware online to see if there are noted findings

D. Disassemble the malware to understand how it was constructed

Correct Answer: C

QUESTION 9

An employee abused PowerShell commands and script interpreters, which lead to an indicator of compromise (IOC) trigger. The IOC event shows that a known malicious file has been executed, and there is an increased likelihood of a breach.

Which indicator generated this IOC event?

A. ExecutedMalware.ioc

B. Crossrider.ioc

C. ConnectToSuspiciousDomain.ioc

D. W32 AccesschkUtility.ioc

Correct Answer: D

QUESTION 10

Max (K)	Retain	OverflowAction	Entries	Log
15,168	0	OverwriteAsNeeded	20,792	Application
15,168	0	OverwriteAsNeeded	12,559	System
15,360	0	OverwriteAsNeeded	11,173	Windows PowerShell

Refer to the exhibit. An employee is a victim of a social engineering phone call and installs remote access software to allow an "MS Support" technician to check his machine for malware. The employee becomes suspicious after the remote technician requests payment in the form of gift cards. The employee has copies of multiple, unencrypted database files, over 400 MB each, on his system and is worried that the scammer copied the files off but has no proof of it. The remote technician was connected sometime between 2:00 pm and 3:00 pm over https.

What should be determined regarding data loss between the employee\\'s laptop and the remote technician\\'s system?

A. No database files were disclosed

B. The database files were disclosed

C. The database files integrity was violated

D. The database files were intentionally corrupted, and encryption is possible

Correct Answer: C

QUESTION 11

According to GDPR, what should be done with data to ensure its confidentiality, integrity, and availability?

A. Perform a vulnerability assessment

B. Conduct a data protection impact assessment

C. Conduct penetration testing

D. Perform awareness testing

Correct Answer: B

Reference: https://apdcat.gencat.cat/web/.content/03-documentacio/Reglament_general_de_proteccio_de_dades/documents/DPIA-Guide.pdf

QUESTION 12

An engineer is analyzing a possible compromise that happened a week ago when the company? (Choose two.)

A. firewall

B. Wireshark

C. autopsy

D. SHA512

E. IPS

Correct Answer: AB

QUESTION 13

An engineer has created a bash script to automate a complicated process. During script execution, this error occurs: permission denied. Which command must be added to execute this script?

A. chmod +x ex.sh

B. source ex.sh

C. chroot ex.sh

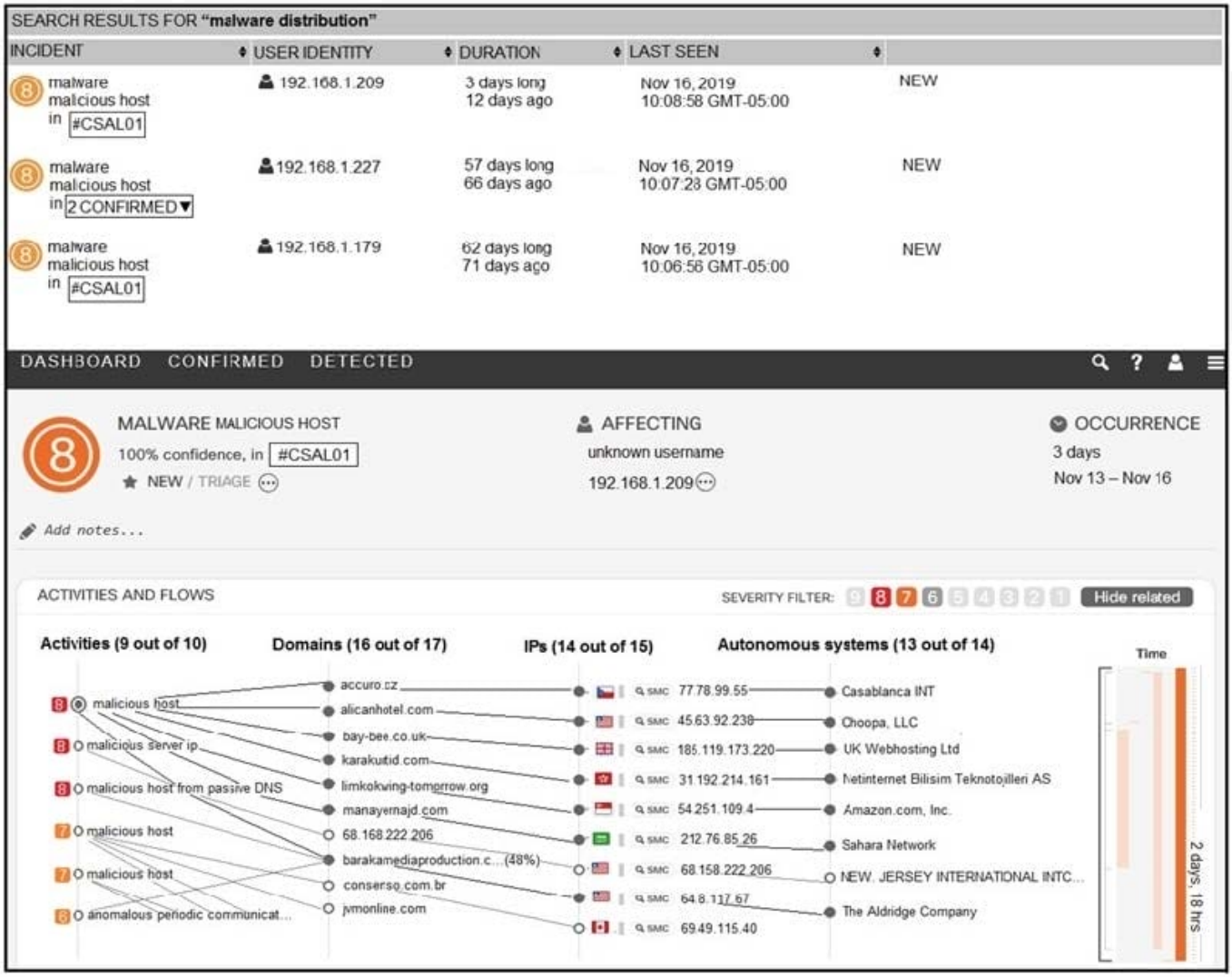
D. sh ex.sh

Correct Answer: A

Reference: https://www.redhat.com/sysadmin/exit-codes-demystified

QUESTION 14

Refer to the exhibit. For IP 192.168.1.209, what are the risk level, activity, and next step?



A. high risk level, anomalous periodic communication, quarantine with antivirus

B. critical risk level, malicious server IP, run in a sandboxed environment

C. critical risk level, data exfiltration, isolate the device

D. high risk level, malicious host, investigate further

Correct Answer: A

QUESTION 15

A company recently started accepting credit card payments in their local warehouses and is undergoing a PCI audit. Based on business requirements, the company needs to store sensitive authentication data for 45 days. How must data

be stored for compliance?

A. post-authorization by non-issuing entities if there is a documented business justification

B. by entities that issue the payment cards or that perform support issuing services

C. post-authorization by non-issuing entities if the data is encrypted and securely stored

D. by issuers and issuer processors if there is a legitimate reason

Correct Answer: C