Q&A

Up-to-date Questions and
Answers from authentic
resources to improve
knowledge and pass the
exam at very first attempt.
----- Guaranteed.

KILL EXAMS

PASS

killexams.com

Cisco

350-201

*Performing CyberOps Using Core Security Technologies
(CBRCOR)*

ORDER FULL VERSION

Question: 90 Section 1

A Mac laptop user notices that several files have disappeared from their laptop documents folder. While looking for the files, the user notices that the browser history was recently cleared. The user raises a case, and an analyst reviews the network usage and discovers that it is abnormally high. Which step should be taken to continue the investigation?

- A. Run the sudo sysdiagnose command
- B. Run the sh command
- C. Run the w command
- D. Run the who command

Answer: A
Reference:
https://eclecticlight.co/2016/02/06/the-ultimate-diagnostic-tool-sysdiagnose/

Question: 91 Section 1

A SOC analyst is investigating a recent email delivered to a high-value user for a customer whose network their organization monitors. The email includes a suspicious attachment titled "Invoice RE: 0004489". The hash of the file is gathered from the Cisco Email Security Appliance. After searching Open Source Intelligence, no available history of this hash is found anywhere on the web. What is the next step in analyzing this attachment to allow the analyst to gather indicators of compromise?

- A. Run and analyze the DLP Incident Summary Report from the Email Security Appliance
- B. Ask the company to execute the payload for real time analysis
- C. Investigate further in open source repositories using YARA to find matches
- D. Obtain a copy of the file for detonation in a sandbox

Answer: D

Question: 92 Section 1

A SOC analyst is notified by the network monitoring tool that there are unusual types of internal traffic on IP subnet 103.861.2117.0/24. The analyst discovers unexplained encrypted data files on a computer system that belongs on that specific subnet. What is the cause of the issue?

- A. DDoS attack
- B. phishing attack
- C. virus outbreak
- D. malware outbreak

Answer: D

Question: 93 Section 1

```
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

Answer: C

Question: 94 Section 1

Refer to the exhibit. Which asset has the highest risk value?

Asset	Threat	Vulnerability	Likelihood (1-10)	Impact (1-10)
Servers	Natural Disasters – Flooding	Server Room is on the zero floor	3	10
Secretary Workstation	Usage of illegitimate software	Inadequate control of software	7	6
Payment Process	Eavesdropping, Misrouting/re-routing of messages	Unencrypted communications	5	10
Website	Website Intrusion	No IDS/IPS usage	6	8

- A. servers
- B. website
- C. payment process
- D. secretary workstation

Answer: C

Question: 95 Section 1

DRAG DROP -

Hosts

Sorted by overall severity

Host Address	Host Name	First Sent	Last Sent	CI	TI	RC	C&C	EP	DS	DT	DH	EX	PV	AN	Location	Host Groups
128.107.78.8		12/15/16 5:26 PM	1/27/17 9:13 PM												United States	United States

| First	Previous	1	Next	Last

Refer to the exhibit. The Cisco Secure Network Analytics (Stealthwatch) console alerted with "New Malware Server Discovered" and the IOC indicates communication from an end-user desktop to a Zeus C&C Server. Drag and drop the actions that the analyst should take from the left into the order on the right to investigate and remediate this IOC.
Select and Place:

Answer Area

Execute rapid threat containment		Step 1
Investigate and classify the exposure		Step 2
Investigate infected hosts		Step 3
Search for infected hosts		Step 4
Examine returned results		Step 5

Answer Area

Execute rapid threat containment	Search for infected hosts
Investigate and classify the exposure	Investigate infected hosts
Investigate infected hosts	Investigate and classify the exposure
Search for infected hosts	Examine returned results
Examine returned results	Execute rapid threat containment
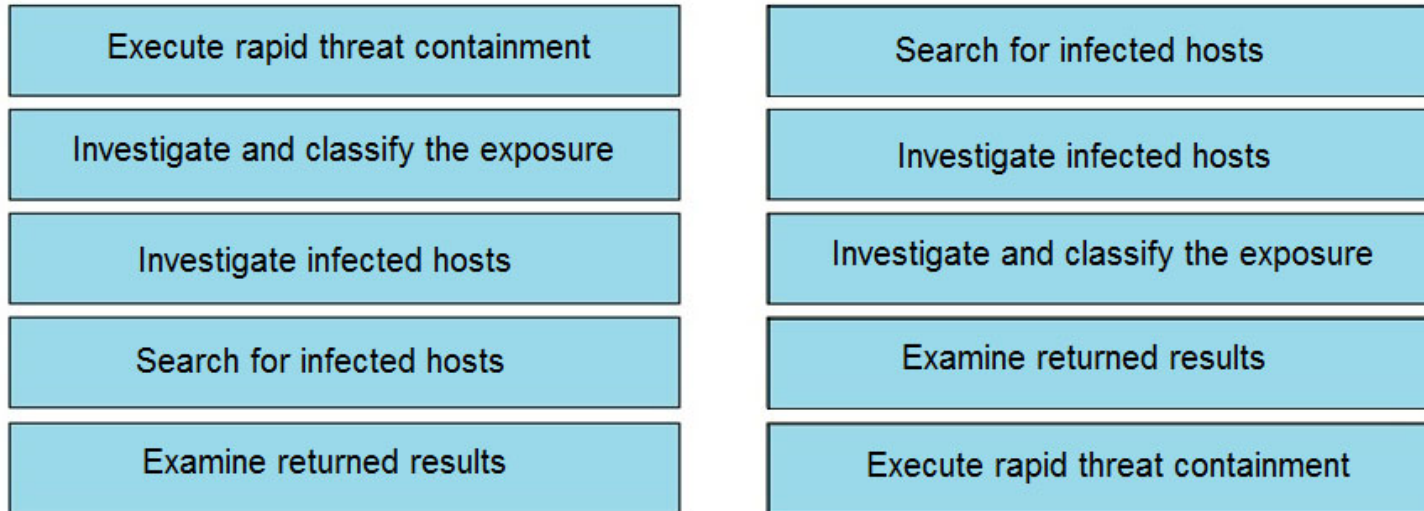
Answer:

Question: 96 Section 1

What is the purpose of hardening systems?

- A. to securely configure machines to limit the attack surface
- B. to create the logic that triggers alerts when anomalies occur
- C. to identify vulnerabilities within an operating system
- D. to analyze attacks to identify threat actors and points of entry

Answer: A

Question: 97 Section 1

A company launched an e-commerce website with multiple points of sale through internal and external e-stores. Customers access the stores from the public website, and employees access the stores from the intranet with an SSO. Which action is needed to comply with PCI standards for hardening the systems?

- A. Mask PAN numbers
- B. Encrypt personal data
- C. Encrypt access
- D. Mask sales details

Answer: B

Question: 98 Section 1

An organization installed a new application server for IP phones. An automated process fetched user credentials from the Active Directory server, and the application will have access to on-premises and cloud services. Which security threat should be mitigated first?

A. aligning access control policies
- B. exfiltration during data transfer
- C. attack using default accounts
- D. data exposure from backups

Answer: B

Question: 99 Section 1

A threat actor has crafted and sent a spear-phishing email with what appears to be a trustworthy link to the site of a conference that an employee recently attended. The employee clicked the link and was redirected to a malicious site through which the employee downloaded a PDF attachment infected with ransomware. The employee opened the attachment, which exploited vulnerabilities on the desktop. The ransomware is now installed and is calling back to its command and control server. Which security solution is needed at this stage to mitigate the attack?

- A. web security solution
- B. email security solution
- C. endpoint security solution
- D. network security solution

Answer: D

Question: 100 Section 1
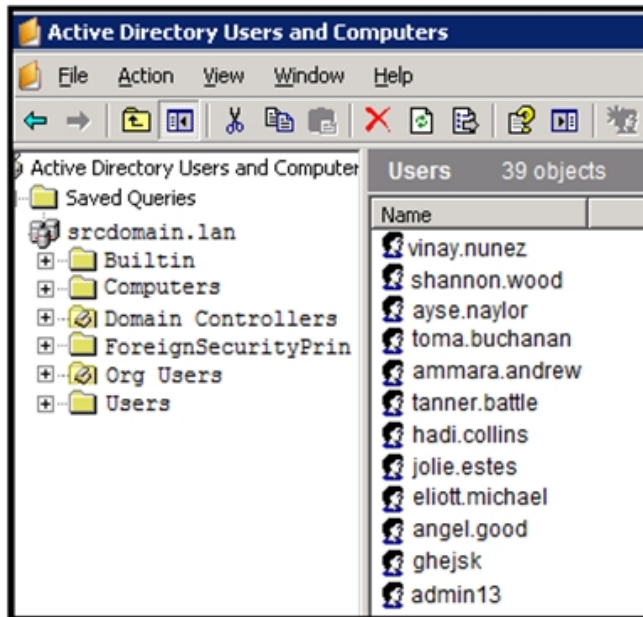
Refer to the exhibit. An engineer is investigating a case with suspicious usernames within the active directory. After the engineer investigates and cross-correlates events from other sources, it appears that the 2 users are privileged, and their creation date matches suspicious network traffic that was initiated from the internal network 2 days prior. Which type of compromise is occurring?

- A. compromised insider
- B. compromised root access
- C. compromised database tables

D. compromised network

Answer: D

SAMPLE QUESTIONS

These questions are for demo purpose only. **Full version** *is up to date and contains actual questions and answers.*

Killexams.com is an online platform that offers a wide range of services related to certification exam preparation. The platform provides actual questions, exam dumps, and practice tests to help individuals prepare for various certification exams with confidence. Here are some key features and services offered by Killexams.com:

ORDER FULL VERSION
Special Discount Coupon

Actual Exam Questions: *Killexams.com provides actual exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these actual questions, candidates can familiarize themselves with the content and format of the real exam.*

Exam Dumps: *Killexams.com offers exam dumps in PDF format. These dumps contain a comprehensive collection of questions and answers that cover the exam topics. By using these dumps, candidates can enhance their knowledge and improve their chances of success in the certification exam.*

Practice Tests: *Killexams.com provides practice tests through their desktop VCE exam simulator and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice tests cover a wide range of questions and enable candidates to identify their strengths and weaknesses.*

Guaranteed Success: *Killexams.com offers a success guarantee with their exam dumps. They claim that by using their materials, candidates will pass their exams on the first attempt or they will refund the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exams.*

Updated Content: *Killexams.com regularly updates its question bank and exam dumps to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.*

Technical Support: *Killexams.com provides free 24x7 technical support to assist candidates with any queries or issues they may encounter while using their services. Their certified experts are available to provide guidance and help candidates throughout their exam preparation journey.*

For More exams visit https://killexams.com/vendors-exam-list
Kill your exam at First Attempt....Guaranteed!