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

QUESTION 1

What is the difference between process orchestration and automation?

A. Orchestration combines a set of automated tools, while automation is focused on the tools to automate process flows.

B. Orchestration arranges the tasks, while automation arranges processes.

C. Orchestration minimizes redundancies, while automation decreases the time to recover from redundancies.

D. Automation optimizes the individual tasks to execute the process, while orchestration optimizes frequent and repeatable processes.

Correct Answer: A

QUESTION 2

An engineer is moving data from NAS servers in different departments to a combined storage database so that the data can be accessed and analyzed by the organization on-demand. Which data management process is being used?

A. data clustering

B. data regression

C. data ingestion

D. data obfuscation

Correct Answer: A

QUESTION 3

An engineer returned to work and realized that payments that were received over the weekend were sent to the wrong recipient. The engineer discovered that the SaaS tool that processes these payments was down over the weekend. Which step should the engineer take first?

A. Utilize the SaaS tool team to gather more information on the potential breach

B. Contact the incident response team to inform them of a potential breach

C. Organize a meeting to discuss the services that may be affected

D. Request that the purchasing department creates and sends the payments manually

Correct Answer: A

QUESTION 4

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

Correct Answer: A

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

QUESTION 5

A SOC engineer discovers that the organization had three DDOS attacks overnight. Four servers are reported offline, even though the hardware seems to be working as expected. One of the offline servers is affecting the pay system reporting times. Three employees, including executive management, have reported ransomware on their laptops. Which steps help the engineer understand a comprehensive overview of the incident?

A. Run and evaluate a full packet capture on the workloads, review SIEM logs, and define a root cause.

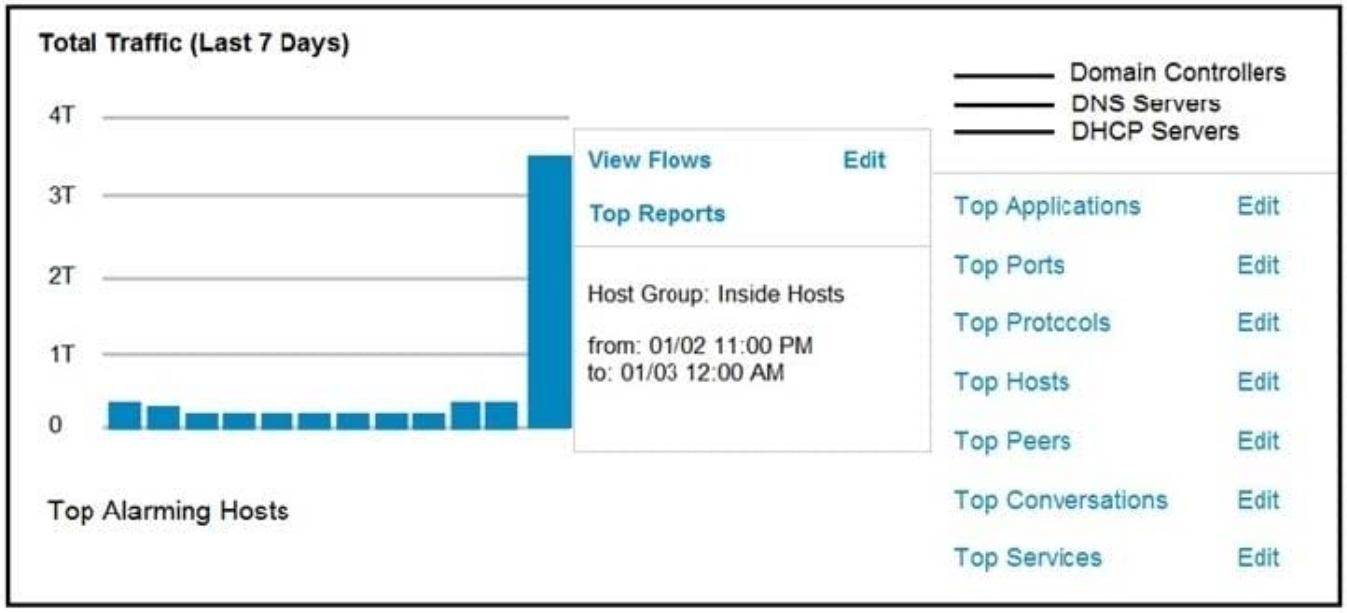
B. Run and evaluate a full packet capture on the workloads, review SIEM logs, and plan mitigation steps.

C. Check SOAR to learn what the security systems are reporting about the overnight events, research the attacks, and plan mitigation step.

D. Check SOAR to know what the security systems are reporting about the overnight events, review the threat vectors, and define a root cause.

Correct Answer: D

QUESTION 6



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 7

An engineer detects an intrusion event inside an organization\\'s network and becomes aware that files that contain personal data have been accessed. Which action must be taken to contain this attack?

A. Disconnect the affected server from the network.

B. Analyze the source.

C. Access the affected server to confirm compromised files are encrypted.

D. Determine the attack surface.

Correct Answer: C

QUESTION 8

Refer to the exhibit. Which indicator of compromise is represented by this STIX?

```
{
  "type": "bundle",
  "id": "bundle--56be2a39",
  "objects": [
        {
          "type": "indicator",
          "spec_version": "2.1",
          "id": "indicator--d81f86b9-9f",
          "created": "2020-08-10T13:49:37.079Z",
          "modified": "2020-08-10T13:49:37.079Z",
          "name": "Malicious site hosting downloader",
          "indicator_types":[
                "malicious-activity"
          ],
          "pattern": "[url:value = 'http://y2z7atc.cn/4823/']",
          "pattern_type": "stix",
          "valid_from": "2020-08-10T13:49:37.079Z"
        },
        {
          "type": "malware",
          "spec_version": "2.1",
          "id": "malware- -162d9 a",
          "created": "2020-08-13T09:15:17.182Z",
          "modified": "2020-08-13T09:15:17.182Z",
          "name": "y2z7atc backdoor",
          "malware_types": [
                "backdoor",
                "remote-access-trojan"
          ],
          "is_family": false,
          "kil_chain_phases": [
                {
                  "kill_chain_name": "mandant-attack-lifecycle-model",
                  "phase_name": "establish-foothold"
                }
          ]

        },
        {
          "type": "relationship",
          "spec_version": "2.1",
          "id": "relationship--864af2e5",
          "created": "2020-08-15T18:03:58.029Z",
          "modified": "2020-08-15T18:03:58.029Z",
          "relationship_type": "indicates",
          "source_ref": "indicator--d81f86b9-975b-4c0b-875e-810c5ad45a4"
          "target_ref": "malware--162d917e07661-4611-b5d6-652791454fca"
        }
    ]
}
```

A. website redirecting traffic to ransomware server

B. website hosting malware to download files

C. web server vulnerability exploited by malware

D. cross-site scripting vulnerability to backdoor server

Correct Answer: C

QUESTION 9

An engineer is developing an application that requires frequent updates to close feedback loops and enable teams to quickly apply patches. The team wants their code updates to get to market as often as possible. Which software development approach should be used to accomplish these goals?

A. continuous delivery

B. continuous integration

C. continuous deployment

D. continuous monitoring

Correct Answer: A

QUESTION 10

A security incident affected an organization\\'s critical business services, and the customer-side web API became unresponsive and crashed. An investigation revealed a spike of API call requests and a high number of inactive sessions during the incident. Which two recommendations should the engineers make to prevent similar incidents in the future? (Choose two.)

A. Configure shorter timeout periods.

B. Determine API rate-limiting requirements.

C. Implement API key maintenance.

D. Automate server-side error reporting for customers.

E. Decrease simultaneous API responses.

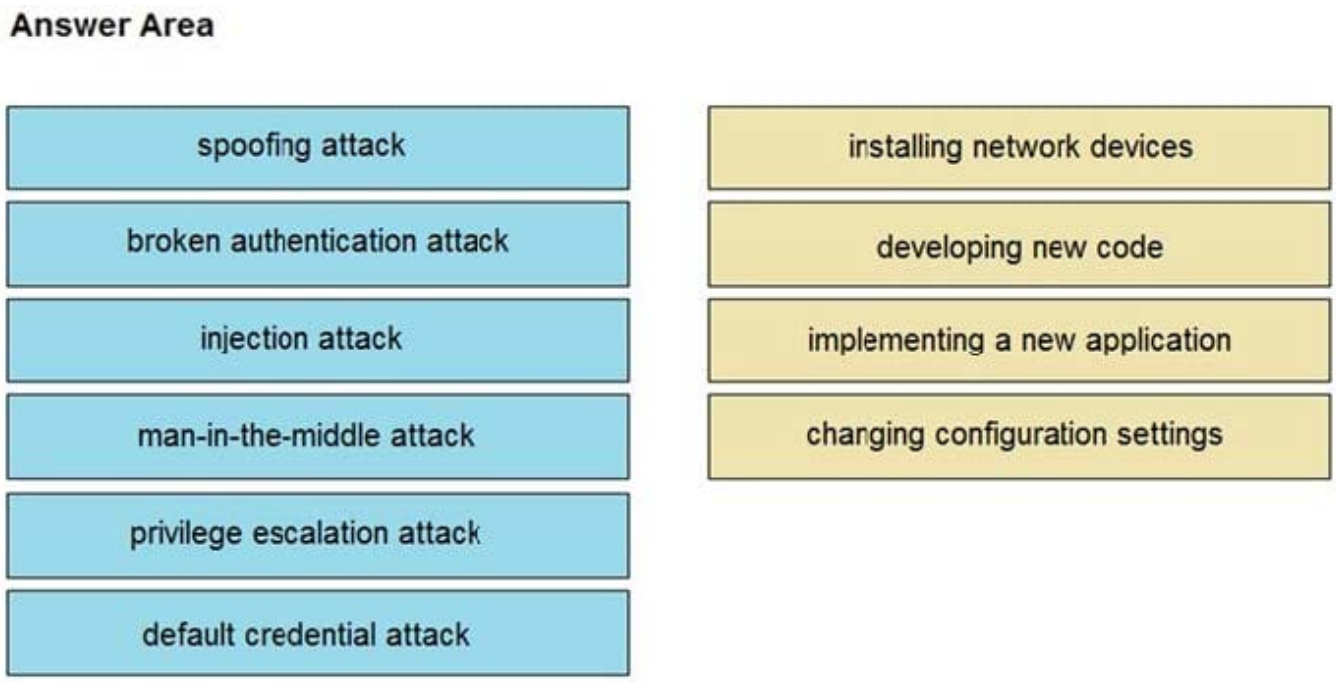
Correct Answer: BD

QUESTION 11

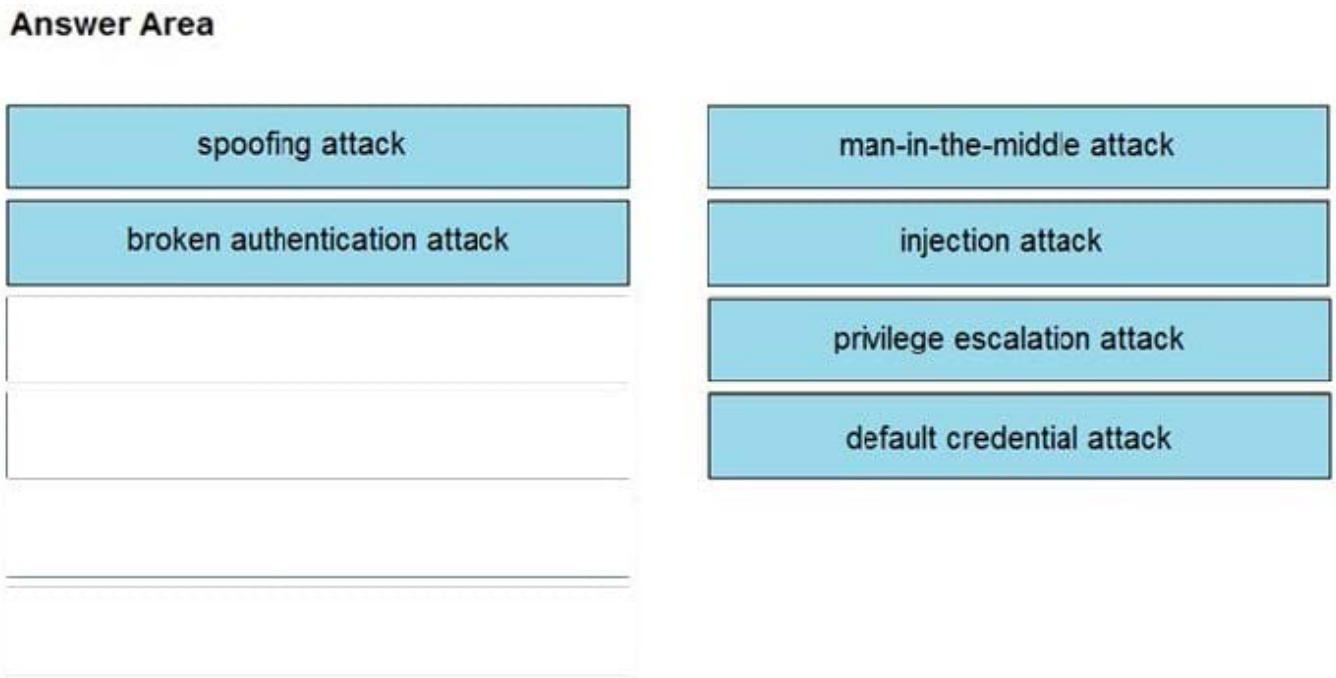
DRAG DROP

Drag and drop the threat from the left onto the scenario that introduces the threat on the right. Not all options are used.

Select and Place:



Correct Answer:



QUESTION 12

A SOC team is investigating a recent, targeted social engineering attack on multiple employees. Cross-correlated log analysis revealed that two hours before the attack, multiple assets received requests on TCP port 79. Which action should be taken by the SOC team to mitigate this attack?

A. Disable BIND forwarding from the DNS server to avoid reconnaissance.

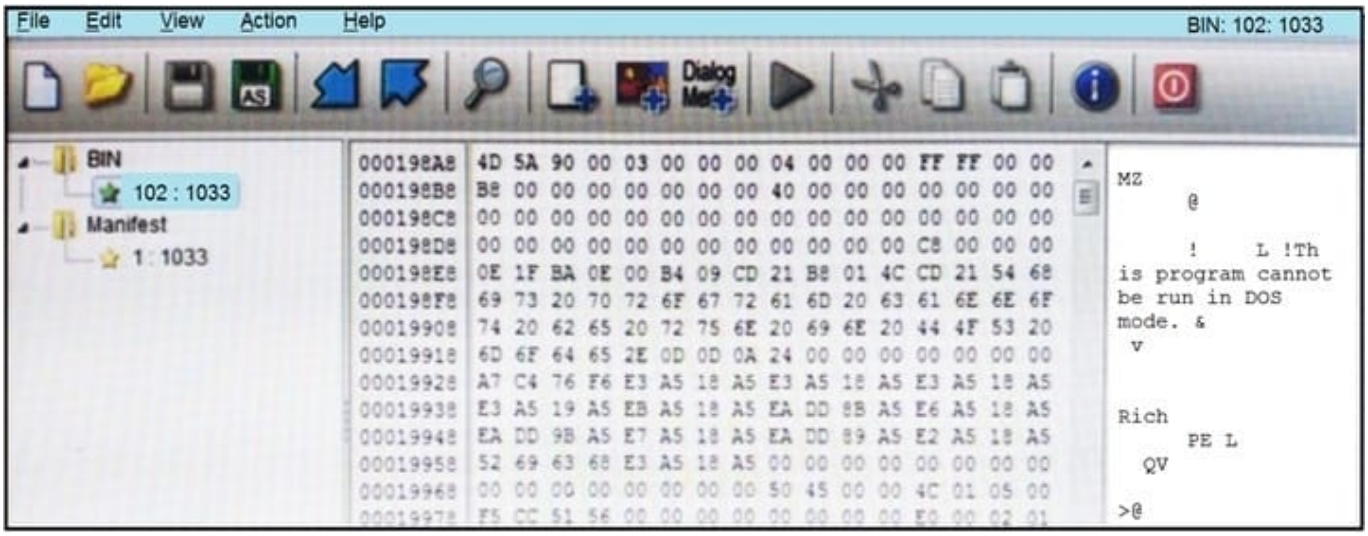
B. Disable affected assets and isolate them for further investigation.

C. Configure affected devices to disable NETRJS protocol.

D. Configure affected devices to disable the Finger service.

Correct Answer: D

QUESTION 13



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#:~:text=The%20linker%20places%20a%20default,using%20the%20%2FSTUB%20linker%20option.andtext=This%20information%20enables%20Windows%20to,has%20an%20MS-DOS%20stub.

QUESTION 14

A security engineer discovers that a spreadsheet containing confidential information for nine of their employees was fraudulently posted on a competitor\\'s website. The spreadsheet contains names, salaries, and social security numbers. What is the next step the engineer should take in this investigation?

A. Determine if there is internal knowledge of this incident.

B. Check incoming and outgoing communications to identify spoofed emails.

C. Disconnect the network from Internet access to stop the phishing threats and regain control.

D. Engage the legal department to explore action against the competitor that posted the spreadsheet.

Correct Answer: D

QUESTION 15

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 143 ( msg:"PROTOCOL-
IMAP login brute force attempt";
flow:to_server,established,no_stream;
content:"LOGIN",fast_pattern,nocase; detection_filter:track
by_dst, count 5, seconds 900; metadata:ruleset community;
service:imap; reference:url,attack.mitre.org/techniques/T1110;
classtype:suspicious-login; sid:2273; rev:12; )
```

Refer to the exhibit. IDS is producing an increased amount of false positive events about brute force attempts on the organization\\'s mail server. How should the Snort rule be modified to improve performance?

A. Block list of internal IPs from the rule

B. Change the rule content match to case sensitive

C. Set the rule to track the source IP

D. Tune the count and seconds threshold of the rule

Correct Answer: B