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.passapply.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

Refer to the exhibit. An engineer is performing static analysis of a file received and reported by a user. Which risk is indicated in this STIX?

```
HttpWebRequest httpWebRequest = (HttpWebRequest)WebRequest.Create("http://freegeoip.net/xml/");
httpWebRequest.UserAgent = "Mozilla/5.0 (Windows NT 6.3; rv:48.0) Gecko/20100101 Firefox/48.0";
httpWebRequest.Proxy = null;
httpWebRequest.Timeout = 10000;
using (HttpWebResponse httpWebResponse = (HttpWebResponse)httpWebRequest.GetResponse())
{
    using (Stream responseStream = httpWebResponse.GetRepsonseStream())
    {
        using (StreamReader streamReader = new StreamReader(responseStream))
        {
            string xml = streamReader.ReadToEnd();
            XmlDocument xmlDocument = new XmlDocument();
            xmlDocument.LoadXml(xml);
            string innerXml = xmlDocument.SelectSingleNode("Response//IP").InnerXml;
            string innerXml2 = xmlDocument.SelectSingleNode("Response//CountryName").InnerXml;
            string innerXml3 = xmlDocument.SelectSingleNode("Response//CountryCode").InnerXml;
            string innerXml4 = xmlDocument.SelectSingleNode("Response//RegionName").InnerXml;
            string innerXml5 = xmlDocument.SelectSingleNode("Response//City").InnerXml;
            string innerXml6 = xmlDocument.SelectSingleNode("Response//TimeZone").InnerXml;
```

A. The file is redirecting users to a website that requests privilege escalations from the user.

B. The file is redirecting users to the website that is downloading ransomware to encrypt files.

C. The file is redirecting users to a website that harvests cookies and stored account information.

D. The file is redirecting users to a website that is determining users' geographic location.

Correct Answer: D

QUESTION 2

An analyst is alerted for a malicious file hash. After analysis, the analyst determined that an internal workstation is communicating over port 80 with an external server and that the file hash is associated with Duqu malware. Which tactics, techniques, and procedures align with this analysis?

A. Command and Control, Application Layer Protocol, Duqu

B. Discovery, Remote Services: SMB/Windows Admin Shares, Duqu

C. Lateral Movement, Remote Services: SMB/Windows Admin Shares, Duqu

D. Discovery, System Network Configuration Discovery, Duqu

Correct Answer: A

QUESTION 3

An engineer is investigating several cases of increased incoming spam emails and suspicious emails from the HR and service departments. While checking the event sources, the website monitoring tool showed several web scraping alerts overnight.

Which type of compromise is indicated?

A. phishing

B. dumpster diving

C. social engineering

D. privilege escalation

Correct Answer: C

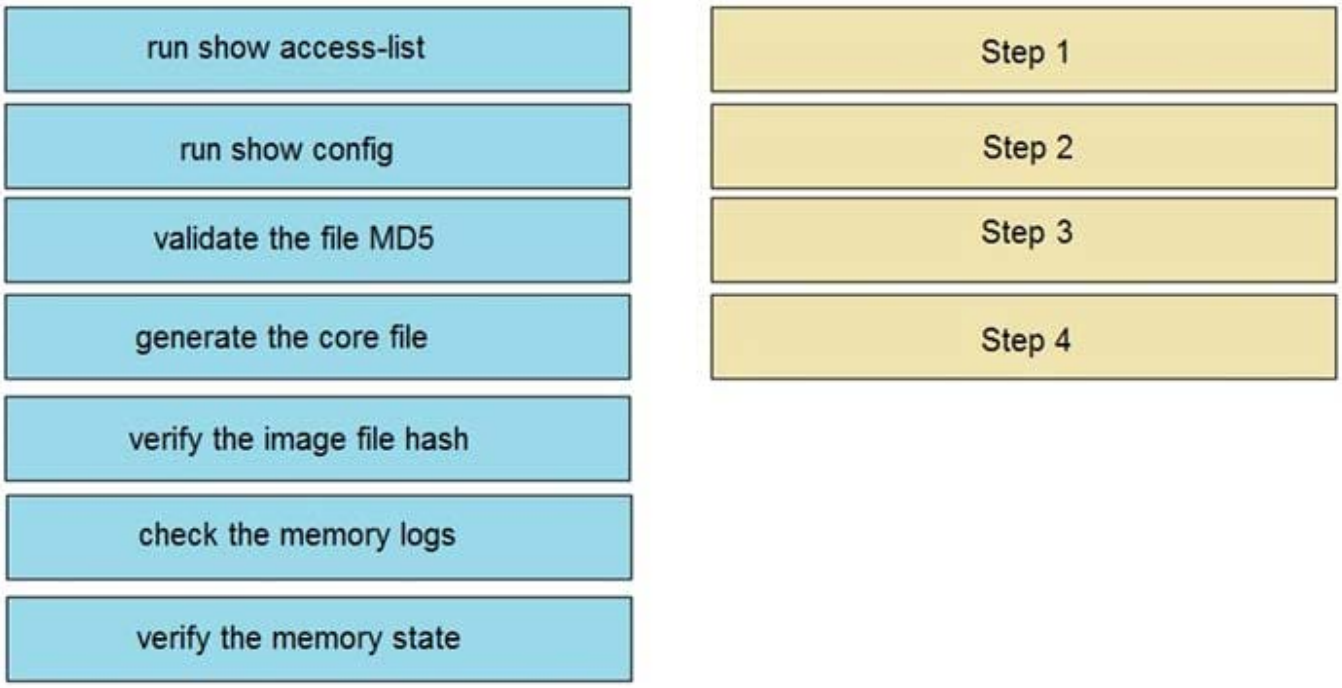
QUESTION 4

DRAG DROP

An organization lost connectivity to critical servers, and users cannot access business applications and internal websites. An engineer checks the network devices to investigate the outage and determines that all devices are functioning. Drag and drop the steps from the left into the sequence on the right to continue investigating this issue. Not all options are used.

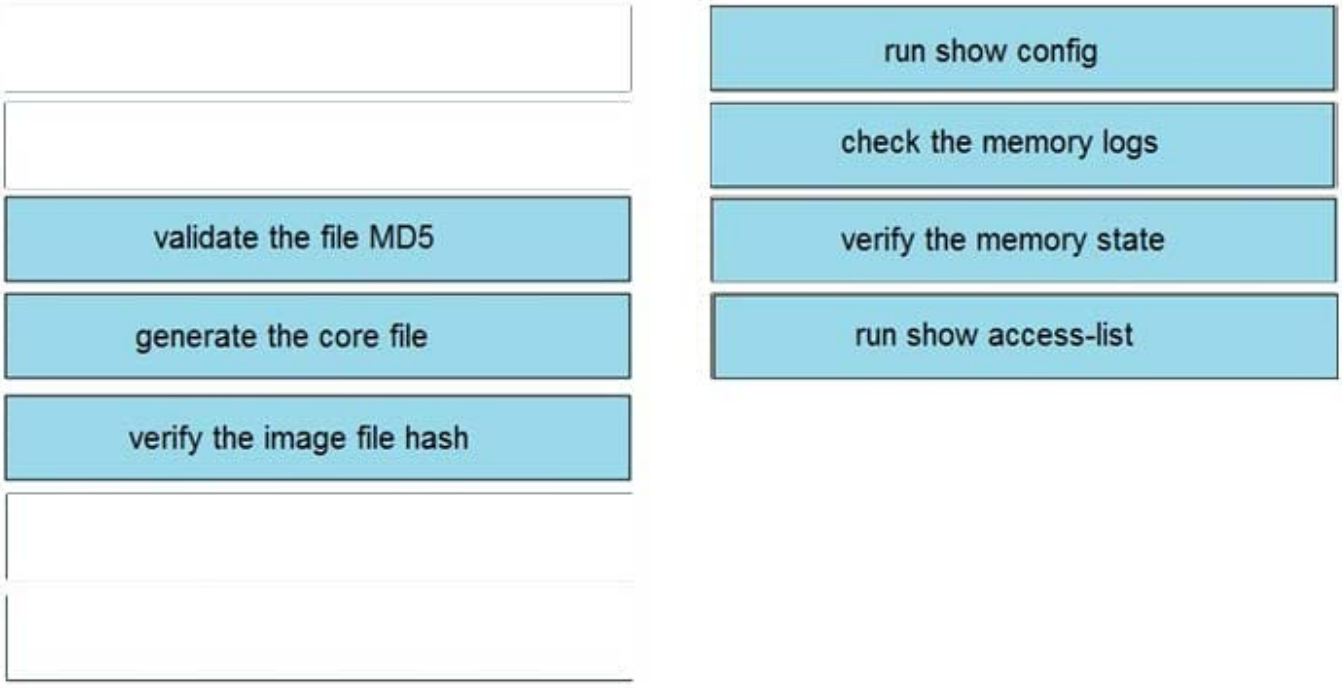
Select and Place:

Answer Area



Correct Answer:

Answer Area



QUESTION 5

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 6

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 7

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

Correct Answer: D

QUESTION 8

A logistic company must use an outdated application located in a private VLAN during the migration to new technologies. The IPS blocked and reported an unencrypted communication. Which tuning option should be applied to IPS?

A. Allow list only authorized hosts to contact the application\\'s IP at a specific port.

B. Allow list HTTP traffic through the corporate VLANS.

C. Allow list traffic to application\\'s IP from the internal network at a specific port.

D. Allow list only authorized hosts to contact the application\\'s VLAN.

Correct Answer: D

QUESTION 9

A company recently completed an internal audit and discovered that there is CSRF vulnerability in 20 of its hosted applications. Based on the audit, which recommendation should an engineer make for patching?

A. Identify the business applications running on the assets

B. Update software to patch third-party software

C. Validate CSRF by executing exploits within Metasploit

D. Fix applications according to the risk scores

Correct Answer: D

QUESTION 10

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 11

What is the impact of hardening machine images for deployment?

A. reduces the attack surface

B. increases the speed of patch deployment

C. reduces the steps needed to mitigate threats

D. increases the availability of threat alerts

Correct Answer: A

QUESTION 12

How is a SIEM tool used?

A. To collect security data from authentication failures and cyber attacks and forward it for analysis

B. To search and compare security data against acceptance standards and generate reports for analysis

C. To compare security alerts against configured scenarios and trigger system responses

D. To collect and analyze security data from network devices and servers and produce alerts

Correct Answer: D

Reference: https://www.varonis.com/blog/what-is-siem/

QUESTION 13

An organization had a breach due to a phishing attack. An engineer leads a team through the recovery phase of the incident response process. Which action should be taken during this phase?

A. Host a discovery meeting and define configuration and policy updates

B. Update the IDS/IPS signatures and reimage the affected hosts

C. Identify the systems that have been affected and tools used to detect the attack

D. Identify the traffic with data capture using Wireshark and review email filters

Correct Answer: C

QUESTION 14

An engineer implemented a SOAR workflow to detect and respond to incorrect login attempts and anomalous user behavior. Since the implementation, the security team has received dozens of false positive alerts and negative feedback from system administrators and privileged users. Several legitimate users were tagged as a threat and their accounts blocked, or credentials reset because of unexpected login times and incorrectly typed credentials.

How should the workflow be improved to resolve these issues?

A. Meet with privileged users to increase awareness and modify the rules for threat tags and anomalous behavior alerts

B. Change the SOAR configuration flow to remove the automatic remediation that is increasing the false positives and triggering threats

C. Add a confirmation step through which SOAR informs the affected user and asks them to confirm whether they made the attempts

D. Increase incorrect login tries and tune anomalous user behavior not to affect privileged accounts

Correct Answer: B

QUESTION 15

The physical security department received a report that an unauthorized person followed an authorized individual to enter a secured premise. The incident was documented and given to a security specialist to analyze. Which step should be taken at this stage?

A. Determine the assets to which the attacker has access

B. Identify assets the attacker handled or acquired

C. Change access controls to high risk assets in the enterprise

D. Identify movement of the attacker in the enterprise

Correct Answer: D

350-201 VCE Dumps 350-201 Study Guide 350-201 Exam Questions