CompTIA

CS0-002

CompTIA CySA+ Certification 2021

http://killexams.com/pass4sure/exam-detail/CS0-002
Question: 178 Topic 1
A security analyst working in the SOC recently discovered instances in which hosts visited a specific set of domains and IPs and became infected with malware. Which of the following is the MOST appropriate action to take in this situation?

- A. Implement an IPS signature for the malware and update the blacklisting for the associated domains and IPs
- B. Implement an IPS signature for the malware and another signature request to block all the associated domains and IPs
- C. Implement a change request to the firewall setting to not allow traffic to and from the IPs and domains
- D. Implement an IPS signature for the malware and a change request to the firewall setting to not allow traffic to and from the origin IPs subnets and second-level domains

Answer: D

Question: 179 Topic 1
The help desk notified a security analyst that emails from a new email server are not being sent out. The new email server was recently added to the existing ones. The analyst runs the following command on the new server:
nslookup -type=txt exampledomain.org

"v=spf1 ip4:72.56.48.0/26 -all"

Given the output, which of the following should the security analyst check NEXT?

- A. The DNS name of the new email server
- B. The version of SPF that is being used
- C. The IP address of the new email server
- D. The DMARC policy

Answer: A

Question: 180 Topic 1
Which of the following should a database administrator implement to BEST protect data from an untrusted server administrator?

- A. Data deidentification
- B. Data encryption
- C. Data masking
- D. Data minimization

Answer: B

Question: 181 Topic 1
A forensic analyst took an image of a workstation that was involved in an incident. To BEST ensure the image is not tampered with, the analyst should use:

- A. hashing
- B. backup tapes
- C. a legal hold
- D. chain of custody

Answer: D

Question: 182 Topic 1
An organization wants to mitigate against risks associated with network reconnaissance. ICMP is already blocked at the firewall; however, a penetration testing team has been able to perform reconnaissance against the organization’s network and identify active hosts. An analyst sees the following output from a packet capture:

192.168.2.3 (eth0 192.168.2.3): NO FLAGS are set, 40 headers + 0 data bytes
len=46 ip=192.168.2.3 ttl=64 id=12345 sport=0 flags=RA seq=0 win=0 rtt=0.4ms

Which of the following phrases from the output provides information on how the testing team is successfully getting around the ICMP firewall rule?

- A. flags=RA indicates the testing team is using a Christmas tree attack
B. ttl=64 indicates the testing team is setting the time to live below the firewall's threshold.
C. 0 data bytes indicates the testing team is crafting empty ICMP packets.
D. NO FLAGS are set indicates the testing team is using hping.

Answer: D

Question: 183 Topic 1

A security analyst is investigating malicious traffic from an internal system that attempted to download proxy avoidance as identified from the firewall logs, but the destination IP is blocked and not captured. Which of the following should the analyst do?

A. Shut down the computer
B. Capture live data using Wireshark
C. Take a snapshot
D. Determine if DNS logging is enabled
E. Review the network logs

Answer: B

Question: 184 Topic 1

An organization is assessing risks so it can prioritize its mitigation actions. Following are the risks and their probability and impact:

<table>
<thead>
<tr>
<th>Risk</th>
<th>Probability of occurrence</th>
<th>Cost of occurrence</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>50%</td>
<td>$120,000</td>
</tr>
<tr>
<td>B</td>
<td>10%</td>
<td>$300,000</td>
</tr>
<tr>
<td>C</td>
<td>20%</td>
<td>$100,000</td>
</tr>
<tr>
<td>D</td>
<td>80%</td>
<td>$50,000</td>
</tr>
</tbody>
</table>

Which of the following is the order of priority for risk mitigation from highest to lowest?

A. A, B, C, D
B. A, D, B, C
C. B, C, A, D
D. C, B, D, A
E. D, A, C, B

Answer: B

Question: 185 Topic 1

The Chief Information Officer (CIO) of a large healthcare institution is concerned about all machines having direct access to sensitive patient information. Which of the following should the security analyst implement to BEST mitigate the risk of sensitive data exposure?

A. A cloud access service broker system
B. NAC to ensure minimum standards are met
C. MFA on all workstations
D. Network segmentation

Answer: D

Question: 186 Topic 1

A Chief Information Security Officer (CISO) is concerned developers have too much visibility into customer data. Which of the following controls should be implemented to BEST address these concerns?

A. Data masking
B. Data loss prevention
C. Data minimization
D. Data sovereignty

Answer: A

Question: 187 Topic 1

A security analyst is supporting an embedded software team. Which of the following is the BEST recommendation to ensure proper error handling at runtime?

A. Perform static code analysis
B. Require application fuzzing
C. Enforce input validation
D. Perform a code review

Answer: B

Question: 188 Topic 1
Which of the following MOST accurately describes an HSM?

- A. An HSM is a low-cost solution for encryption
- B. An HSM can be networked based or a removable USB
- C. An HSM is slower at encrypting than software
- D. An HSM is explicitly used for MFA

**Answer:** B

Question: 189 Topic 1

A company is moving from the use of web servers hosted in an internal datacenter to a containerized cloud platform. An analyst has been asked to identify indicators of compromise in the containerized environment. Which of the following would BEST indicate a running container has been compromised?

- A. A container from an approved software image has drifted
- B. An approved software orchestration container is running with root privileges
- C. A container from an approved software image has stopped responding
- D. A container from an approved software image fails to start

**Answer:** A

Question: 190 Topic 1

A cybersecurity analyst is investigating a potential incident affecting multiple systems on a company’s internal network. Although there is a negligible impact to performance, the following symptoms are present on each of the affected systems:

- ‘Existence of a new and unexpected svchost.exe process
- Persistent, outbound TCP/IP connections to an unknown external host with routine keep-alives transferred
- DNS query logs showing successful name resolution for an Internet-resident dynamic DNS domain

If this situation remains unresolved, which of the following will MOST likely occur?

- A. The affected hosts may participate in a coordinated DDoS attack upon command
- B. An adversary may leverage the affected hosts to reconfigure the company’s router ACLs
- C. Key files on the affected hosts may become encrypted and require ransom payment for unlock
- D. The adversary may attempt to perform a man-in-the-middle attack

**Answer:** A

Question: 191 Topic 1

Massivelog.log has grown to 40GB on a Windows server. At this size, local tools are unable to read the file, and it cannot be moved off the virtual server where it is located. Which of the following lines of PowerShell script will allow a user to extract the last 10,000 lines of the log for review?

- A. tail -10000 Massivelog.log > extract.txt
- B. info tail n -10000 Massivelog.log | extract.txt;
- C. get content './Massivelog.log' Last 10000 | extract.txt
- D. get-content './Massivelog.log' Last 10000 > extract.txt;

**Answer:** D

Question: 192 Topic 1

Which of the following are components of the intelligence cycle? (Choose two.)

- A. Collection
- B. Normalization
- C. Response
- D. Analysis
- E. Correction
- F. Dissension

**Answer:** AD

Question: 193 Topic 1

A financial institution business unit plans to deploy a new technology in a manner that violates existing information security standards. Which of the following actions should the Chief Information Security Officer (CISO) take to manage any type of violation?

- A. Enforce the existing security standards and controls
- B. Perform a risk analysis and qualify the risk with legal
- C. Perform research and propose a better technology
- D. Enforce the standard permits

**Answer:** B
For More exams visit https://killexams.com/vendors-exam-list

Kill your exam at First Attempt….Guaranteed!