CS0-001$^{Q\&As}$

CompTIA Cybersecurity Analyst

Pass CompTIA CS0-001 Exam with 100% Guarantee

QUESTION 1

The help desk has reported that users are reusing previous passwords when prompted to change them. Which of the following would be the MOST appropriate control for the security analyst to configure to prevent password reuse?

A. Implement mandatory access control on all workstations.

B. Implement role-based access control within directory services.

C. Deploy Group Policy Objects to domain resources.

D. Implement scripts to automate the configuration of PAM on Linux hosts.

E. Deploy a single-sing-on solution for both Windows and Linux hosts.

Correct Answer: C

QUESTION 2

Which of the following policies BEST explains the purpose of a data ownership policy?

A. The policy should describe the roles and responsibilities between users and managers, and the management of specific data types.

B. The policy should establish the protocol for retaining information types based on regulatory or business needs.

C. The policy should document practices that users must adhere to in order to access data on the corporate network or Internet.

D. The policy should outline the organization\\'s administration of accounts for authorized users to access the appropriate data.

Correct Answer: D

QUESTION 3

A security analyst has performed various scans and found vulnerabilities in several applications that affect production data. Remediation of all exploits may cause certain applications to no longer work. Which of the following activities would need to be conducted BEFORE remediation?

A. Fuzzing

B. Input validation

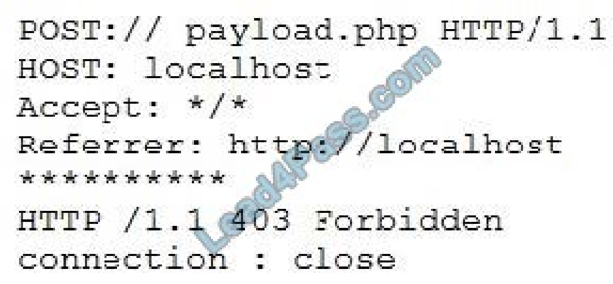
C. Change control

D. Sandboxing

Correct Answer: C

QUESTION 4

A cybersecurity analyst is reviewing log data and sees the output below:



```
POST:// payload.php HTTP/1.1
HOST: localhost
Accept: */*
Referrer: http://localhost
**********
HTTP /1.1 403 Forbidden
connection : close
```

Which of the following technologies MOST likely generated this log?

A. Stateful inspection firewall

B. Network-based intrusion detection system

C. Web application firewall

D. Host-based intrusion detection system

Correct Answer: C

QUESTION 5

A staff member reported that a laptop has degraded performance. The security analyst has investigated the issue and discovered that CPU utilization, memory utilization, and outbound network traffic are consuming the laptop\\'s resources. Which of the following is the BEST course of actions to resolve the problem?

A. Identify and remove malicious processes.

B. Disable scheduled tasks.

C. Suspend virus scan.

D. Increase laptop memory.

E. Ensure the laptop OS is properly patched.

Correct Answer: A

QUESTION 6

A technician is running an intensive vulnerability scan to detect which ports are open to exploit. During the scan, several network services are disabled and production is affected. Which of the following sources would be used to evaluate which network service was interrupted?

A. Syslog

B. Network mapping

C. Firewall logs

D. NIDS

Correct Answer: A

QUESTION 7

A computer at a company was used to commit a crime. The system was seized and removed for further analysis. Which of the following is the purpose of labeling cables and connections when seizing the computer system?

A. To capture the system configuration as it was at the time it was removed

B. To maintain the chain of custody

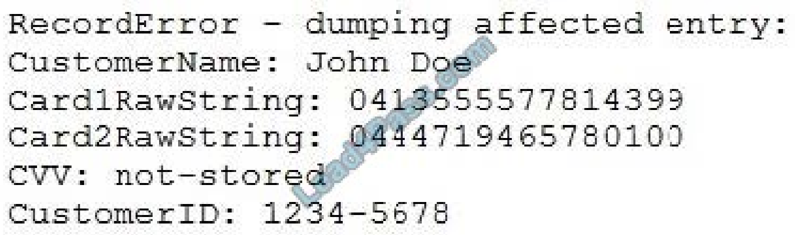
C. To block any communication with the computer system from attack

D. To document the model, manufacturer, and type of cables connected

Correct Answer: A

QUESTION 8

The Chief Information Security Officer (CISO) asks a security analyst to write a new SIEM search rule to determine if any credit card numbers are being written to log files. The CISO and security analyst suspect the following log snippet contains real customer card data:



```
RecordError - dumping affected entry:
CustomerName: John Doe
Card1RawString: 0413555577814399
Card2RawString: 0444719465780100
CVV: not-stored
CustomerID: 1234-5678
```

Which of the following expressions would find potential credit card numbers in a format that matches the log snippet?

A. ^[0-9](16)$

B. (0-9) x 16

C. "1234-5678"

D. "04*"

Correct Answer: A

QUESTION 9

A technician receives an alert indicating an endpoint is beaconing to a suspect dynamic DNS domain. Which of the following countermeasures should be used to BEST protect the network in response to this alert? (Choose two.)

A. Set up a sinkhole for that dynamic DNS domain to prevent communication.

B. Isolate the infected endpoint to prevent the potential spread of malicious activity.

C. Implement an internal honeypot to catch the malicious traffic and trace it.

D. Perform a risk assessment and implement compensating controls.

E. Ensure the IDS is active on the network segment where the endpoint resides.

Correct Answer: AB

QUESTION 10

A security analyst has discovered that an outbound SFTP process is occurring at the same time of day for the past several days. At the time this was discovered, large amounts of business critical data were delivered. The authentication for this process occurred using a service account with proper credentials. The security analyst investigated the destination IP for this transfer and discovered that this new process is not documented in the change management log. Which of the following would be the BEST course of action for the analyst to take?

A. Investigate a potential incident.

B. Verify user permissions.

C. Run a vulnerability scan.

D. Verify SLA with cloud provider.

Correct Answer: A

QUESTION 11

A user received an invalid password response when trying to change the password. Which of the following policies could explain why the password is invalid?

A. Access control policy

B. Account management policy

C. Password policy

D. Data ownership policy

Correct Answer: C

QUESTION 12

Datacenter access is controlled with proximity badges that record all entries and exits from the datacenter.

The access records are used to identify which staff members accessed the data center in the event of equipment theft.

Which of the following MUST be prevented in order for this policy to be effective?

A. Password reuse

B. Phishing

C. Social engineering

D. Tailgating

Correct Answer: D

QUESTION 13

A Chief Executive Officer (CEO) wants to implement BYOD in the environment. Which of the following options should the security analyst suggest to protect corporate data on these devices? (Choose two.)

A. Disable VPN connectivity on the device.

B. Disable Bluetooth on the device.

C. Disable near-field communication on the device.

D. Enable MDM/MAM capabilities.

E. Enable email services on the device.

F. Enable encryption on all devices.

Correct Answer: DF

QUESTION 14

A network administrator is attempting to troubleshoot an issue regarding certificates on a secure website.

During the troubleshooting process, the network administrator notices that the web gateway proxy on the local network has signed all of the certificates on the local machine.

Which of the following describes the type of attack the proxy has been legitimately programmed to perform?

A. Transitive access

B. Spoofing

C. Man-in-the-middle

D. Replay

Correct Answer: C

QUESTION 15

The Chief Information Security Officer (CISO) has decided that all accounts with elevated privileges must use a longer, more complicated passphrase instead of a password. The CISO would like to formally document management\\'s intent to set this control level. Which of the following is the appropriate means to achieve this?

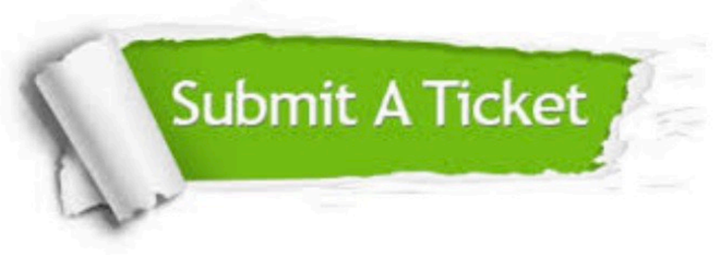
A. A control

B. A standard

C. A policy

D. A guideline

Correct Answer: C



Submit A Ticket