Free Questions for SY0-601 by dumpssheet

Shared by Barr on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A company is looking to move completely to a remote work environment. The Chief Information Security Officer is concerned about the improper use of company-owned devices when employees are working from home. Which of the following could be implemented to ensure that devices are on the company-owned network?

Options:

A- Internet proxy

B- Always-on VPN

C- Split tunneling

D- OS firewall

Answer:

B

Explanation:

Always-on VPN is a feature that enables the active VPN profile to connect automatically on certain triggers, such as user sign-in, network change, or device screen on. This ensures that the devices are always on the company-owned network and protected by the company's security policies.Always-on VPN also prevents the devices from accessing the internet if the VPN connection is lost or interrupted

Question 2

Question Type: MultipleChoice

A security analyst discovers that a large number of employee credentials had been stolen and were being sold on the dark web. The analyst investigates and discovers that some hourly employee credentials were compromised, but salaried employee credentials were not affected.

Most employees clocked in and out while they were inside the building using one of the kiosks connected to the network. However, some clocked out and recorded their time after leaving to go home. Only those who clocked in and out while inside the building had credentials stolen. Each of the kiosks are on different floors, and there are multiple routers, since the business segments environments for certain business functions.

Hourly employees are required to use a website called acmetimekeeping.com to clock in and out. This website is accessible from the internet. Which of the following is the most likely reason for this compromise?

Options:

A- A brute-force attack was used against the time-keeping website to scan for common passwords.

B- A malicious actor compromised the time-keeping website with malicious code using an unpatched vulnerability on the site, stealing the credentials.

C- The internal DNS servers were poisoned and were redirecting acmetimekeeping.com to a malicious domain that intercepted the credentials and then passed them through to the real site.

D- ARP poisoning affected the machines in the building and caused the kiosks to send a copy of all the submitted credentials to a malicious machine.

Answer:

D

Explanation:

ARP poisoning is a technique by which an attacker sends spoofed ARP messages to alter routing on a local area network.It can be used to intercept, modify, or stop data frames, or launch other attacks3In this scenario, the attacker likely used ARP poisoning to associate their MAC address with the IP address of the time-keeping website, causing the kiosks to send a copy of all the submitted credentials to the attacker's machine.This explains why only the credentials of the employees who clocked in and out while inside the building were stolen, and why the compromise was not detected by the DNS servers or the website itself4

Question 3

Question Type: MultipleChoice

A company wants to ensure that all employees in a given department are trained on each job role to help with employee burnout and continuity of business operations in the event an employee leaves the company. Which of the following should the company implement?

Options:

A- Separation of duties

B- Job rotation

C- Mandatory vacations

D- Least privilege

Answer:

B

Explanation:

Job rotation is the practice of regularly transitioning employees between different job roles to ensure they gain exposure to various departments and skills.Job rotation can help with employee burnout by providing variety and challenge, and with continuity of business

operations by creating backups and cross-trained staff

Question 4

Question Type: MultipleChoice

A company has had several malware incidents that have been traced back to users accessing personal SaaS applications on the internet from the company network. The company has a policy that states users can only access business-related cloud applications from within the company network. Which of the following technical solutions should be used to enforce the policy?

Options:

A- Implement single sign-on using an identity provider.

B- Leverage a cloud access security broker.

C- Configure cloud security groups.

D- Install a virtual private cloud endpoint.

Answer:

B

Explanation:

A cloud access security broker (CASB) is a solution that sits between the users and the cloud service providers and enforces the organization's security policies for cloud app access and usage.A CASB can help the company prevent unauthorized access to personal SaaS applications and mitigate cloud security risks

Question 5

Question Type: MultipleChoice

Which of the following strengthens files stored in the /etc/shadow directory?

Options:

A- Key agreement

B- Digital signatures

C- Salting

D- Key stretching

Answer:

C

Explanation:

Salting is a technique that adds random data to the password before hashing it, making it more difficult to crack.Salting strengthens the files stored in the /etc/shadow directory, which contain the hashed passwords of the users.

Question 6

Question Type: MultipleChoice

Which of the following is best to use when determining the severity of a vulnerability?

Options:

A- CVE

B- OSINT

C- SOAR

D- CVSS

Answer:

D

Explanation:

CVSS, or Common Vulnerability Scoring System, is a standard method for assessing the severity of software vulnerabilities based on various metrics and factors. CVE, or Common Vulnerabilities and Exposures, is a list of publicly disclosed vulnerabilities, but does not provide a severity score. OSINT, or Open Source Intelligence, is the collection and analysis of publicly available information, which may or may not be relevant to a specific vulnerability. SOAR, or Security Orchestration, Automation and Response, is a set of tools and processes that automate and streamline security operations and incident response.

Question 7

Question Type: **MultipleChoice**

The primary goal of the threat-hunting team at a large company is to identify cyberthreats that the SOC has not detected. Which of the following types of data would the threat-hunting team primarily use to identify systems that are exploitable?

Options:

A- Vulnerability scan

B- Packet capture

C- Threat feed

D- User behavior

Answer:

A

Explanation:

A vulnerability scan is a type of data that can identify systems that are exploitable by detecting known weaknesses and misconfigurations in the software and hardware. Packet capture, threat feed, and user behavior are types of data that can help identify malicious activities or indicators of compromise, but not necessarily the systems that are vulnerable to exploitation.

Question 8

Question Type: MultipleChoice

A security analyst is investigating a malware incident at a company The malware is accessing a command-and-control website at www.comptia.com. All outbound internet traffic is logged to a syslog server and stored in /logfiles/messages Which of the following commands would be best for the analyst to use on the syslog server to search for recent traffic to the command-and-control website?

Options:

A- head -500 www. compt ia.com | grep /logfiles/messages

B- cat /logfiles/messages I tail -500 www.comptia.com

C- tail -500 /logfiles/messages I grep www.cornptia.com

D- grep -500 /logfiles/messages I cat www.comptia.cctn

Answer:

C

Explanation:

tail is a Linux command that can be used to display the last part of a file. grep is a Linux command that can be used to search for a pattern in a file or input. The pipe symbol (|) is used to connect two commands and pass the output of one command as the input of another command. The best command for the analyst to use on the syslog server to search for recent traffic to the command-and-control website is tail -500 /logfiles/messages | grep www.comptia.com. This command would display the last 500 lines of the /logfiles/messages file and filter them by the pattern www.comptia.com, which is the domain name of the command-and-control website. This way, the

analyst can see any syslog messages that contain the domain name of the malicious website and investigate them further.2122[23]Reference:CompTIA Security+ SY0-601 Certification Study Guide, Chapter 11: Explaining Digital Forensics Concepts, page 498;tail (Unix) - Wikipedia;grep - Wikipedia; [How To Use grep Command In Linux / UNIX - nixCraft]

Question 9

Question Type: MultipleChoice

A systems administrator is auditing all company servers to ensure they meet the minimum security baseline While auditing a Linux server the systems administrator observes the /etc/ahadow file has permissions beyond the baseline recommendation. Which of the following commands should the systems administrator use to resolve this issue?

Options:

A- chmod

B- grep

C- dd

D- passwd

Answer:

A

Explanation:

chmod is a Linux command that can be used to change or modify the permissions of files and directories. The /etc/shadow file is a system file that stores the encrypted passwords of user accounts in Linux. The /etc/shadow file should have restricted permissions to prevent unauthorized access or modification of the passwords. The recommended permissions for the /etc/shadow file are read/write for root user only (600). If the systems administrator observes that the /etc/shadow file has permissions beyond the baseline recommendation, they can use the chmod command to resolve this issue by setting the appropriate permissions for the file. For example, chmod 600 /etc/shadow would set the permissions of the /etc/shadow file to read/write for root user only.181920Reference:CompTIA Security+ SY0-601 Certification Study Guide, Chapter 9: Implementing Identity and Access Management Controls, page 404;chmod - Wikipedia;Linux /etc/shadow file - nixCraft;How to Change File Permissions in Linux - Linuxize