Free Questions for CS0-003 by braindumpscollection

Shared by Mcleod on 24-05-2024

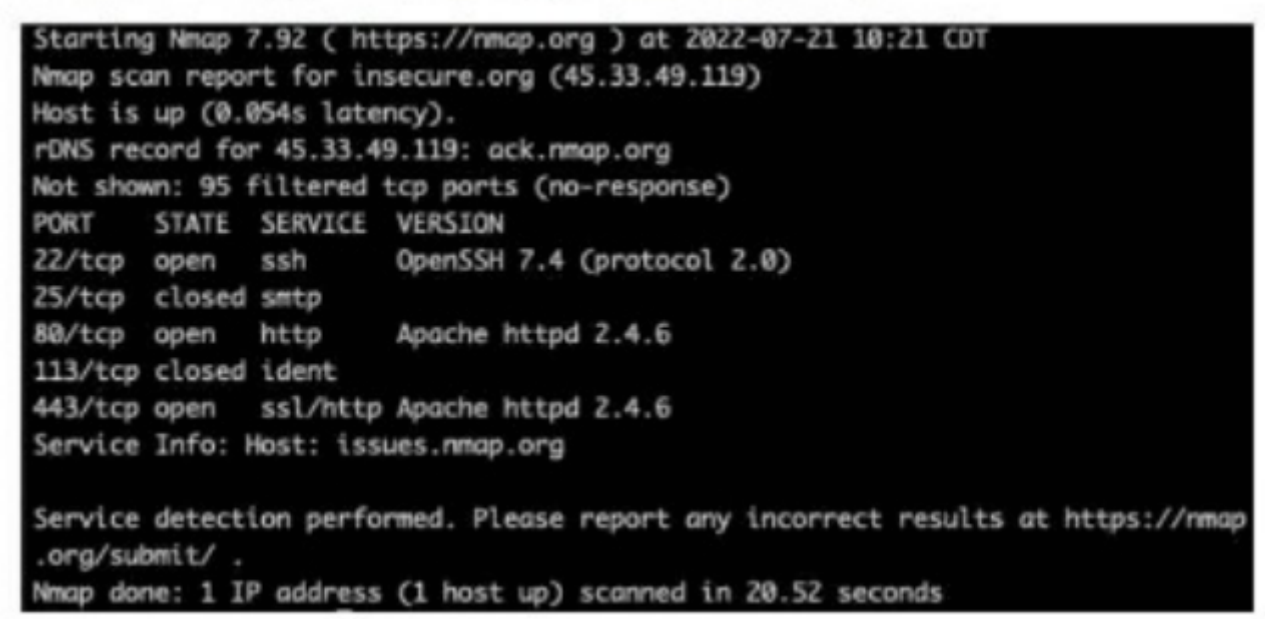
For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

An analyst investigated a website and produced the following:



```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-21 10:21 CDT
Nmap scan report for insecure.org (45.33.49.119)
Host is up (0.054s latency).
rDNS record for 45.33.49.119: ack.nmap.org
Not shown: 95 filtered tcp ports (no-response)
PORT    STATE  SERVICE  VERSION
22/tcp  open   ssh      OpenSSH 7.4 (protocol 2.0)
25/tcp  closed smtp
80/tcp  open   http     Apache httpd 2.4.6
113/tcp closed ident
443/tcp open   ssl/http Apache httpd 2.4.6
Service Info: Host: issues.nmap.org

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.52 seconds
```

Which of the following syntaxes did the analyst use to discover the application versions on this vulnerable website?

Options:

A- nmap -sS -T4 -F insecure.org

B- nmap -o insecure.org

C- nmap -sV -T4 -F insecure.org

D- nmap -A insecure.org

Answer:

C

Question 2

Question Type: MultipleChoice

An employee is no longer able to log in to an account after updating a browser. The employee usually has several tabs open in the browser. Which of the following attacks was most likely performed?

Options:

A- RFI

B- LFI

C- CSRF

D- XSS

Answer:

C

Explanation:

CSRF is an attack that forces an end user to execute unwanted actions on a web application in which they're currently authenticated. An attacker may trick the user into clicking a malicious link or submitting a forged form that performs an action on the user's behalf, such as changing their password or transferring funds. If the user has several tabs open in the browser, they may not notice the CSRF request or the resulting change in their account. Updating the browser may have cleared the user's cache or cookies, preventing them from logging in to their account after the CSRF attack.

Question 3

Question Type: **MultipleChoice**

Which of the following best explains the importance of communicating with staff regarding the official public communication plan related to incidents impacting the organization?

Options:

A- To establish what information is allowed to be released by designated employees

B- To designate an external public relations firm to represent the organization

C- To ensure that all news media outlets are informed at the same time

D- To define how each employee will be contacted after an event occurs

Answer:

A

Explanation:

Communicating with staff about the official public communication plan is important to avoid unauthorized or inaccurate disclosure of information that could harm the organization's reputation, security, or legal obligations. It also helps to ensure consistency and clarity of the messages delivered to the public and other stakeholders.

https://resources.sei.cmu.edu/asset_files/Handbook/2021_002_001_651819.pdf

Question 4

Question Type: MultipleChoice

Which of the following is the most appropriate action a security analyst to take to effectively identify the most security risks associated with a locally hosted server?

Options:

A- Run the operating system update tool to apply patches that are missing.

B- Contract an external penetration tester to attempt a brute-force attack.

C- Download a vendor support agent to validate drivers that are installed.

D- Execute a vulnerability scan against the target host.

Answer:

D

Explanation:

A vulnerability scan is a process of identifying and assessing the security weaknesses of a system or network. A vulnerability scan can help a security analyst to effectively identify the most security risks associated with a locally hosted server, such as missing patches, misconfigurations, outdated software, or exposed services. A vulnerability scan can also provide recommendations on how to remediate the identified vulnerabilities and improve the security posture of the server12 Reference: 1: What is a Vulnerability Scan? | Definition and Examples 2: Securing a server: risks, challenges and best practices - Vaadata

Question 5

Question Type: MultipleChoice

A security analyst is performing an investigation involving multiple targeted Windows malware binaries. The analyst wants to gather intelligence without disclosing information to the attackers. Which of the following actions would allow the analyst to achieve the objective?

Options:

A- Upload the binary to an air-gapped sandbox for analysis.

B- Send the binaries to the antivirus vendor.

C- Execute the binaries on an environment with internet connectivity.

D- Query the file hashes using VirusTotal.

Answer:

A

Explanation:

An air-gapped sandbox is a virtual machine or a physical device that is isolated from any network connection. This allows the analyst to safely execute the malware binaries and observe their behavior without risking any communication with the attackers or any damage to other systems. Uploading the binary to an air-gapped sandbox is the best option to gather intelligence without disclosing information to the attackers12 Reference: 1: Dynamic Analysis of a Windows Malicious Self-Propagating Binary 2: GitHub - mikesiko/PracticalMalwareAnalysis-Labs: Binaries for the book Practical Malware Analysis

Question 6

Question Type: MultipleChoice

The SOC received a threat intelligence notification indicating that an employee's credentials were found on the dark web. The user's web and log-in activities were reviewed for malicious or anomalous connections, data uploads/downloads, and exploits. A review of the controls confirmed multifactor

authentication was enabled. Which of the following should be done first to mitigate impact to the business networks and assets?

Options:

A- Perform a forced password reset.

B- Communicate the compromised credentials to the user.

C- Perform an ad hoc AV scan on the user's laptop.

D- Review and ensure privileges assigned to the user's account reflect least privilege.

E- Lower the thresholds for SOC alerting of suspected malicious activity.

Answer:

A

Explanation:

The first and most urgent step to mitigate the impact of compromised credentials on the dark web is to perform a forced password reset for the affected user. This will prevent the cybercriminals from using the stolen credentials to access the company's network and systems. Multifactor authentication is a good security measure, but it is not foolproof and can be bypassed by sophisticated attackers. Therefore, changing the password as soon as possible is the best practice to reduce the risk of a data breach or other cyber attack123 Reference: 1: How to monitor the dark web for compromised employee credentials 2: How to prevent corporate credentials ending up on the dark web 3: Data Breach Prevention: Identifying Leaked Credentials on the Dark Web