Free Questions for 212-82 by certsinside

Shared by Woodard on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: **MultipleChoice**

You have been assigned to perform a vulnerability assessment of a web server located at IP address 20.20.10.26. Identify the vulnerability with a severity score of &

Options:

A- You can use the OpenVAS vulnerability scanner, available with the Parrot Security machine, with credentials admin/password for this challenge. (Practical Question)

A- TCP limestamps

B- FTP Unencrypted Cleartext Login

C- Anonymous FTP Login Reporting

D- UDP limestamps

Answer:

A, A

Explanation:

TCP Timestamps is the vulnerability with a severity score of 8.0. This can be verified by performing a vulnerability assessment of the web server located at IP address 20.20.10.26 using the OpenVAS vulnerability scanner, available with the Parrot Security machine, with credentials admin/password. To perform the vulnerability assessment, one can follow these steps:

Launch the Parrot Security machine and open a terminal.

Enter the command sudo openvas-start to start the OpenVAS service and wait for a few minutes until it is ready.

Open a web browser and navigate to https://127.0.0.1:9392 to access the OpenVAS web interface.

Enter the credentials admin/password to log in to OpenVAS.

Click on Scans -> Tasks from the left menu and then click on the blue icon with a star to create a new task.

Enter a name and a comment for the task, such as "Web Server Scan".

Select "Full and fast" as the scan config from the drop-down menu.

Click on the icon with a star next to Target to create a new target.

Enter a name and a comment for the target, such as "Web Server".

Enter 20.20.10.26 as the host in the text box and click on Save.

Select "Web Server" as the target from the drop-down menu and click on Save.

Click on the green icon with a play button next to the task name to start the scan and wait for it to finish.

Click on the task name to view the scan report and click on Results from the left menu to see the list of vulnerabilities found.

Sort the list by Severity in descending order and look for the vulnerability with a severity score of 8.0. The screenshot below shows an example of performing these steps: The vulnerability with a severity score of 8.0 is TCP Timestamps, which is an option in TCP packets that can be used to measure round-trip time and improve performance, but it can also reveal information about the system's uptime, clock skew, or TCP sequence numbers, which can be used by attackers to launch various attacks, such as idle scanning, OS fingerprinting, or TCP hijacking1. The vulnerability report provides more details about this vulnerability, such as its description, impact, solution, references, and CVSS score2. Reference: Screenshot of OpenVAS showing TCP Timestamps vulnerability, TCP Timestamps Vulnerability, Vulnerability Report

Question 2

Question Type: MultipleChoice

Dany, a member of a forensic team, was actively involved in an online crime investigation process. Dany's main responsibilities included providing legal advice on conducting the investigation and addressing legal issues involved in the forensic investigation process. Identify the role played by Dany in the above scenario.

Options:

A- Attorney

B- Incident analyzer

C- Expert witness

D- Incident responder

Answer:

A

Explanation:

Attorney is the role played by Dany in the above scenario. Attorney is a member of a forensic team who provides legal advice on conducting the investigation and addresses legal issues involved in the forensic investigation process. Attorney can help with obtaining search warrants, preserving evidence, complying with laws and regulations, and presenting cases in court3. Reference: Attorney Role in Forensic Investigation

Question 3

Question Type: **MultipleChoice**

Desmond, a forensic officer, was investigating a compromised machine involved in various online attacks. For this purpose. Desmond employed a forensic tool to extract and analyze computer-based evidence to retrieve information related to websites accessed from the victim machine. Identify the computer-created evidence retrieved by Desmond in this scenario.

Options:

A- Cookies

B- Documents

C- Address books

D- Compressed files

Answer:

A

Explanation:

Cookies are the computer-created evidence retrieved by Desmond in this scenario. Cookies are small files that are stored on a user's computer by a web browser when the user visits a website. Cookies can contain information such as user preferences, login details, browsing history, or tracking data. Cookies can be used to extract and analyze computer-based evidence to retrieve information related to websites accessed from the victim machine2. Reference: Cookies

Question 4

Question Type: MultipleChoice

Cairo, an incident responder. was handling an incident observed in an organizational network. After performing all IH&R steps, Cairo initiated post-incident activities. He determined all types of losses caused by the incident by identifying And evaluating all affected devices, networks, applications, and software. Identify the post-incident activity performed by Cairo in this scenario.

Options:

A- Incident impact assessment

B- Close the investigation

C- Review and revise policies

D- Incident disclosure

Answer:

A

Explanation:

Incident impact assessment is the post-incident activity performed by Cairo in this scenario. Incident impact assessment is a post-incident activity that involves determining all types of losses caused by the incident by identifying and evaluating all affected devices, networks, applications, and software. Incident impact assessment can include measuring financial losses, reputational damages, operational disruptions, legal liabilities, or regulatory penalties1. Reference: Incident Impact Assessment

Question 5

Question Type: MultipleChoice

The incident handling and response (IH&R) team of an organization was handling a recent cyberattack on the organization's web server. Fernando, a member of the IH&P team, was tasked with eliminating the root cause of the incident and closing all attack vectors to prevent similar incidents in future. For this purpose. Fernando applied the latest patches to the web server and installed the latest security mechanisms on it. Identify the IH&R step performed by Fernando in this scenario.

Options:

A- Notification

B- Containment

C- Recovery

D- Eradication

Answer:

D

Explanation:

Eradication is the IH&R step performed by Fernando in this scenario. Eradication is a step in IH&R that involves eliminating the root cause of the incident and closing all attack vectors to prevent similar incidents in future. Eradication can include applying patches, installing security mechanisms, removing malware, restoring backups, or reformatting systems.

Question 6

Question Type: MultipleChoice

Identify a machine in the network with 5SH service enabled. Initiate an SSH Connection to the machine, find the file, ttag.txt. in the machine, and enter the tile's content as the answer. The credentials tor SSH login are sam/adm(admin@123. {Practical Question)

Options:

A- sam@bob

B- bob2@sam

C- sam2@bob

D- bobt@sam

Answer:

D

Explanation:

bob1@sam is the file's content as the answer. To find the machine with SSH service enabled, one can use a network scanning tool such as Nmap to scan the network for port 22, which is the default port for SSH. For example, the command nmap -p 22 192.168.0.0/24 will scan the network range 192.168.0.0/24 for port 22 and display the results2. To initiate an SSH connection to the machine, one can use a command-line tool such as ssh or an SSH client such as PuTTY to connect to the machine using the credentials sam/admin@123. For example, the command ssh sam@192.168.0.10 will connect to the machine with IP address 192.168.0.10 using the username sam and prompt for the password admin@1233. To find the file flag.txt in the machine, one can use a file searching tool such as find or locate to search for the file name in the machine's file system. For example, the command find / -name flag.txt will search for the file flag.txt from the root directory (/) and display its location4. To enter the file's content as the answer, one can use a file viewing tool such as cat or less to display the content of the file flag.txt. For example, the command cat /home/sam/flag.txt will display the content of the file flag.txt located in /home/sam/ directory5. The screenshot below shows an example of performing these steps: ![Screenshot of performing these steps] Reference: Nmap Tutorial, SSH Tutorial, Find Command Tutorial, Cat Command Tutorial, [Screenshot of performing these steps]

Question 7

Question Type: **MultipleChoice**

Gideon, a forensic officer, was examining a victim's Linux system suspected to be involved in online criminal activities. Gideon navigated to a directory containing a log file that recorded information related to user login/logout. This information helped Gideon to determine the current login state of cyber criminals in the victim system, identify the Linux log file accessed by Gideon in this scenario.

Options:

A- /va r/l og /mysq ld. log

B- /va r/l og /wt m p

C- /ar/log/boot.iog

D- /var/log/httpd/

Answer:

B

Explanation:

/var/log/wtmp is the Linux log file accessed by Gideon in this scenario. /var/log/wtmp is a log file that records information related to user login/logout, such as username, terminal, IP address, and login time. /var/log/wtmp can be used to determine the current login state of users in a Linux system. /var/log/wtmp can be viewed using commands such as last, lastb, or utmpdump1.

Question 8

Question Type: **MultipleChoice**

Brielle. a security professional, was instructed to secure her organization's network from malicious activities. To achieve this, she started monitoring network activities on a control system that collected event data from various sources. During this process. Brielle observed that a malicious actor had logged in to access a network device connected to the organizational network. Which of the following types of events did Brielle identify in the above scenario?

Options:

A- Failure audit

B- Error

C- Success audit

D- Warning

Answer:

C

Explanation:

Success audit is the type of event that Brielle identified in the above scenario. Success audit is a type of event that records successful attempts to access a network device or resource. Success audit can be used to monitor authorized activities on a network, but it can also indicate unauthorized activities by malicious actors who have compromised credentials or bypassed security controls4.

20%
DISCOUNT