PT0-002$^{\text{Q\&As}}$

CompTIA PenTest+ Certification Exam

QUESTION 1

A penetration tester managed to exploit a vulnerability using the following payload:

IF (1=1) WAIT FOR DELAY \\'0:0:15\\'

Which of the following actions would best mitigate this type ol attack?

A. Encrypting passwords

B. Parameterizing queries

C. Encoding output

D. Sanitizing HTML

Correct Answer: B

The payload used by the penetration tester is a type of blind SQL injection attack that delays the response of the database by 15 seconds if the condition is true. This can be used to extract information from the database by asking a series of true or false questions. To prevent this type of attack, the best practice is to use parameterized queries, which separate the user input from the SQL statement and prevent the injection of malicious code. Encrypting passwords, encoding output, and sanitizing HTML are also good security measures, but they do not directly address the SQL injection vulnerability. References: The Official CompTIA PenTest+ Study Guide (Exam PT0-002), Chapter 5: Attacks and Exploits, Section 5.2: Perform Network Attacks, Subsection: SQL Injection, p. 235-237 Blind SQL Injection | OWASP Foundation, Description and Examples sections Time-Based Blind SQL Injection Attacks, Introduction and Microsoft SQL Server sections

QUESTION 2

A penetration tester is testing a company\\'s public API and discovers that specific input allows the execution of arbitrary commands on the base operating system. Which of the following actions should the penetration tester take next?

A. Include the findings in the final report.

B. Notify the client immediately.

C. Document which commands can be executed.

D. Use this feature to further compromise the server.

Correct Answer: B

The Nmap command uses the Xmas scan technique, which sends packets with the FIN, PSH, and URG flags set. This is an attempt to bypass firewall rules and elicit a response from open ports. However, if the target responds with an RST packet, it means that the port is closed. Open ports will either ignore the Xmas scan packets or send back an ACK packet. Therefore, the information most likely indicates that all of the ports in the target range are closed. References: [Nmap Scan Types], [Nmap Port Scanning Techniques], [CompTIA PenTest+ Study Guide: Exam PT0-002, Chapter 4: Conducting Passive Reconnaissance, page 127]

QUESTION 3

Which of the following concepts defines the specific set of steps and approaches that are conducted during a penetration test?

A. Scope details

B. Findings

C. Methodology

D. Statement of work

Correct Answer: C

QUESTION 4

A mail service company has hired a penetration tester to conduct an enumeration of all user accounts on an SMTP server to identify whether previous staff member accounts are still active. Which of the following commands should be used to accomplish the goal?

A. VRFY and EXPN

B. VRFY and TURN

C. EXPN and TURN

D. RCPT TO and VRFY

Correct Answer: A

The VRFY and EXPN commands can be used to enumerate user accounts on an SMTP server, as they are used to verify the existence of users or mailing lists. VRFY (verify) asks the server to confirm that a given user name or address is valid. EXPN (expand) asks the server to expand a mailing list into its individual members. These commands can be used by a penetration tester to identify valid user names or e-mail addresses on the target SMTP server. Reference: https://hackerone.com/reports/193314

QUESTION 5

Which of the following assessment methods is MOST likely to cause harm to an ICS environment?

A. Active scanning

B. Ping sweep

C. Protocol reversing

D. Packet analysis

Correct Answer: A