PT0-003 Q&As

CompTIA PenTest+

Pass CompTIA PT0-003 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/pt0-003.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

QUESTION 1

A penetration tester was contracted to test a proprietary application for buffer overflow vulnerabilities. Which of the following tools would be BEST suited for this task?

A. GDB

B. Burp Suite

C. SearchSpliot

D. Netcat

Correct Answer: A

GDB is a debugging tool that can be used to analyze and manipulate the memory of a running process, which is useful for finding and exploiting buffer overflow vulnerabilities. Burp Suite is a web application testing tool that does not directly test for buffer overflows. SearchSpliot is a database of known exploits that does not test for new vulnerabilities. Netcat is a network utility that can be used to send and receive data, but not to test for buffer overflows.

QUESTION 2

A penetration tester performs a service enumeration process and receives the following result after scanning a server using the Nmap tool: PORT STATE SERVICE

22/tcp open ssh 25/tcp filtered smtp

111/tcp open rpcbind

2049/tcp open nfs

Based on the output, which of the following services provides the best target for launching an attack?

A. Database

B. Remote access

C. Email

D. File sharing

Correct Answer: D

Based on the Nmap scan results, the services identified on the target server are as follows:

22/tcp open ssh:

25/tcp filtered smtp:

111/tcp open rpcbind:

2049/tcp open nfs:

Conclusion: The NFS service (2049/tcp) provides the best target for launching an attack. File sharing services like NFS often contain sensitive data and can be vulnerable to misconfigurations that allow unauthorized access or privilege

escalation.

QUESTION 3

A penetration tester attempts to run an automated web application scanner against a target URL. The tester validates that the web page is accessible from a different device. The tester analyzes the following HTTP request header logging output:

200; GET /login.aspx HTTP/1.1 Host: foo.com; User-Agent: Mozilla/5.0

200; GET /login.aspx HTTP/1.1 Host: foo.com; User-Agent: Mozilla/5.0

No response; POST /login.aspx HTTP/1.1 Host: foo.com; User-Agent: curl 200; POST /login.aspx HTTP/1.1 Host: foo.com; User-Agent: Mozilla/5.0

No response; GET /login.aspx HTTP/1.1 Host: foo.com; User-Agent: python Which of the following actions should the tester take to get the scans to work properly?

A. Modify the scanner to slow down the scan.

B. Change the source IP with a VPN.

C. Modify the scanner to only use HTTP GET requests.

D. Modify the scanner user agent.

Correct Answer: D

QUESTION 4

A penetration tester is conducting a vulnerability scan. The tester wants to see any vulnerabilities that may be visible from outside of the organization. Which of the following scans should the penetration tester perform?

A. SAST

B. Sidecar

C. Unauthenticated

D. Host-based

Correct Answer: C

To see any vulnerabilities that may be visible from outside of the organization, the penetration tester should perform an unauthenticated scan.

Unauthenticated Scan:

Comparison with Other Scans:

Pentest References:

By performing an unauthenticated scan, the penetration tester can identify vulnerabilities that an external attacker could exploit without needing any credentials or internal access.

QUESTION 5

Which of the following is the most efficient way to infiltrate a file containing data that could be sensitive?

A. Use steganography and send the file over FTP

B. Compress the file and send it using TFTP

C. Split the file in tiny pieces and send it over dnscat

D. Encrypt and send the file over HTTPS

Correct Answer: D

When considering efficiency and security for exfiltrating sensitive data, the chosen method must ensure data confidentiality and minimize the risk of detection. Here\\'s an analysis of each option:

Use steganography and send the file over FTP (Option A):

Compress the file and send it using TFTP (Option B):

Split the file in tiny pieces and send it over dnscat (Option C):

Encrypt and send the file over HTTPS (Answer: D):

Conclusion: Encrypting the file and sending it over HTTPS is the most efficient and secure method for exfiltrating sensitive data, ensuring both confidentiality and reducing the risk of detection.