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.leads4pass.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 needs to confirm the version number of a client\\'s web application server. Which of the following techniques should the penetration tester use?

A. SSL certificate inspection

B. URL spidering

C. Banner grabbing

D. Directory brute forcing

Correct Answer: C

Banner grabbing is a technique used to gather information about a service running on an open port, which often includes the version number of the application or server. Here\\'s why banner grabbing is the correct answer:

Banner Grabbing: It involves connecting to a service and reading the welcome banner or response, which typically includes version information. This is a direct method to identify the version number of a web application server. SSL Certificate

Inspection: While it can provide information about the server, it is not reliable for identifying specific application versions. URL Spidering: This is used for discovering URLs and resources within a web application, not for version identification.

Directory Brute Forcing: This is used to discover hidden directories and files, not for identifying version information.

References from Pentest:

Luke HTB: Shows how banner grabbing can be used to identify the versions of services running on a server.

Writeup HTB: Demonstrates the importance of gathering version information through techniques like banner grabbing during enumeration phases.

Conclusion:

Option C, banner grabbing, is the most appropriate technique for confirming the version number of a web application server.

QUESTION 2

A penetration tester gains access to a Windows machine and wants to further enumerate users with native operating system credentials. Which of the following should the tester use?

A. route.exe print

B. netstat.exe -ntp

C. net.exe commands

D. strings.exe -a

Correct Answer: C

To further enumerate users on a Windows machine using native operating system commands, the tester should use net.exe commands. The net command is a versatile tool that provides various network functionalities, including user

enumeration.

net.exe:

net user

uk.co.certification.simulator.questionpool.PList@a43cf82 net localgroup administrators

Enumerating Users:

Pentest References:

Using net.exe commands, the penetration tester can effectively enumerate user accounts and group memberships on the compromised Windows machine, aiding in further exploitation and privilege escalation.

QUESTION 3

Which of the following post-exploitation activities allows a penetration tester to maintain persistent access in a compromised system?

A. Creating registry keys

B. Installing a bind shell

C. Executing a process injection

D. Setting up a reverse SSH connection

Correct Answer: A

Maintaining persistent access in a compromised system is a crucial goal for a penetration tester after achieving initial access. Here\\'s an explanation of each option and why creating registry keys is the preferred method:

Creating registry keys (Answer: A):

Installing a bind shell (Option B):

Executing a process injection (Option C):

Setting up a reverse SSH connection (Option D):

Conclusion: Creating registry keys is the most effective method for maintaining persistent access in a compromised system, particularly in Windows environments, due to its stealthiness and reliability.

QUESTION 4

Which of the following is a term used to describe a situation in which a penetration tester bypasses physical access controls and gains access to a facility by entering at the same time as an employee?

A. Badge cloning

B. Shoulder surfing

C. Tailgating

D. Site survey

Correct Answer: C

Understanding Tailgating:

Methods to Prevent Tailgating:

Examples in Penetration Testing:

References from Pentesting Literature:

References:

Penetration Testing - A Hands-on Introduction to Hacking HTB Official Writeups

QUESTION 5

A penetration tester needs to evaluate the order in which the next systems will be selected for testing. Given the following output:

Hostname | IP address | CVSS 2.0 | EPSS

hrdatabase | 192.168.20.55 | 9.9 | 0.50

financesite | 192.168.15.99 | 8.0 | 0.01

legaldatabase | 192.168.10.2 | 8.2 | 0.60

fileserver | 192.168.125.7 | 7.6 | 0.90

Which of the following targets should the tester select next?

A. fileserver

B. hrdatabase

C. legaldatabase

D. financesite

Correct Answer: A

Given the output, the penetration tester should select the fileserver as the next target for testing, considering both CVSS and EPSS scores.

CVSS (Common Vulnerability Scoring System):

EPSS (Exploit Prediction Scoring System):

Evaluation:

Pentest References:

Prioritization: Balancing between severity (CVSS) and exploitability (EPSS) is crucial for effective vulnerability management. Risk Assessment: Evaluating both the impact and the likelihood of exploitation helps in making informed decisions

about testing priorities. By selecting the fileserver, which has a high EPSS score, the penetration tester focuses on a target that is more likely to be exploited, thereby addressing the most immediate risk.

QUESTION 6

During a vulnerability scanning phase, a penetration tester wants to execute an Nmap scan using custom NSE scripts stored in the following folder:

/home/user/scripts

Which of the following commands should the penetration tester use to perform this scan?

A. nmap resume "not intrusive"

B. nmap script default safe

C. nmap script /home/user/scripts

D. nmap -load /home/user/scripts

Correct Answer: C

The Nmap command in the question aims to use custom NSE scripts stored in a specific folder. The correct syntax for this option is to use the script argument followed by the path to the folder. The other commands are either invalid, use the wrong argument, or do not specify the folder path. References: Best PenTest+ certification study resources and training materials, CompTIA PenTest+ PT0-002 Cert Guide, 101 Labs -- CompTIA PenTest+: Hands-on Labs for the PT0-002 Exam

QUESTION 7

A penetration tester needs to confirm the version number of a client\\'s web application server. Which of the following techniques should the penetration tester use?

A. SSL certificate inspection

B. URL spidering

C. Banner grabbing

D. Directory brute forcing

Correct Answer: C

Banner grabbing is a technique used to obtain information about a network service, including its version number, by connecting to the service and reading the response.

Understanding Banner Grabbing:

Manual Banner Grabbing:

Step-by-Step Explanationtelnet target_ip 80

uk.co.certification.simulator.questionpool.PList@58886243 nc target_ip 80

Automated Banner Grabbing:

nmap -sV target_ip

Benefits:

References from Pentesting Literature:

References:

Penetration Testing - A Hands-on Introduction to Hacking HTB Official Writeups

---

QUESTION 8

A security engineer is trying to bypass a network IPS that isolates the source when the scan exceeds 100 packets per minute. The scope of the scan is to identify web servers in the 10.0.0.0/16 subnet.

Which of the following commands should the engineer use to achieve the objective in the least amount of time?

A. nmap -T3 -p 80 10.0.0.0/16 -- max-hostgroup 100

B. nmap -TO -p 80 10.0.0.0/16

C. nmap -T4 -p 80 10.0.0.0/16 -- max-rate 60

D. nmap -T5 -p 80 10.0.0.0/16 -- min-rate 80

Correct Answer: C

The nmap -T4 -p 80 10.0.0.0/16 -- max-rate 60 command is used to scan the 10.0.0.0/16 subnet for web servers (port 80) at a maximum rate of 60 packets per minute. The -T4 option sets the timing template to "aggressive", which speeds up the scan. The -- max-rate option limits the number of packets sent per second, helping to bypass the network IPS that isolates the source when the scan exceeds 100 packets per minute12.

QUESTION 9

Which of the following BEST describes why a client would hold a lessons-learned meeting with the penetration-testing team?

A. To provide feedback on the report structure and recommend improvements

B. To discuss the findings and dispute any false positives

C. To determine any processes that failed to meet expectations during the assessment

D. To ensure the penetration-testing team destroys all company data that was gathered during the test

Correct Answer: C

QUESTION 10

While conducting a peer review for a recent assessment, a penetration tester finds the debugging mode is still enabled for the production system. Which of the following is most likely responsible for this observation?

A. Configuration changes were not reverted.

B. A full backup restoration is required for the server.

C. The penetration test was not completed on time.

D. The penetration tester was locked out of the system.

Correct Answer: A

Debugging Mode:

Common Causes:

Best Practices:

References from Pentesting Literature:

References:

Penetration Testing - A Hands-on Introduction to Hacking HTB Official Writeups

QUESTION 11

A Chief Information Security Officer wants to evaluate the security of the company\\'s e- commerce application.

Which of the following tools should a penetration tester use FIRST to obtain relevant information from the application without triggering alarms?

A. SQLmap

B. DirBuster

C. w3af

D. OWASP ZAP

Correct Answer: C

W3AF, the Web Application Attack and Audit Framework, is an open source web application security scanner that includes directory and filename bruteforcing in its list of capabilities.

QUESTION 12

Which of the following should a penetration tester attack to gain control of the state in the HTTP protocol after the user is logged in?

A. HTTPS communication

B. Public and private keys

C. Password encryption

D. Sessions and cookies

Correct Answer: D

QUESTION 13

A penetration tester finished a security scan and uncovered numerous vulnerabilities on several hosts. Based on the targets\\' EPSS and CVSS scores, which of the following targets is the most likely to get attacked?

Host | CVSS | EPSS

Target 1 | 4 | 0.6

Target 2 | 2 | 0.3

Target 3 | 1 | 0.6 Target 4 | 4.5 | 0.4

A. Target 1: CVSS Score = 4 and EPSS Score = 0.6

B. Target 2: CVSS Score = 2 and EPSS Score = 0.3

C. Target 3: CVSS Score = 1 and EPSS Score = 0.6

D. Target 4: CVSS Score = 4.5 and EPSS Score = 0.4

Correct Answer: A

Based on the CVSS (Common Vulnerability Scoring System) and EPSS (Exploit Prediction Scoring System) scores, Target 1 is the most likely to get attacked.

CVSS:

EPSS:

Analysis:

Pentest References:

Vulnerability Prioritization: Using CVSS and EPSS scores to prioritize vulnerabilities based on severity and likelihood of exploitation. Risk Assessment: Understanding the balance between impact (CVSS) and exploit likelihood (EPSS) to

identify the most critical targets for remediation or attack. By focusing on Target 1, which has a balanced combination of severity and exploitability, the penetration tester can address the most likely target for attacks based on the given scores.

QUESTION 14

A penetration tester downloaded the following Perl script that can be used to identify vulnerabilities in network switches. However, the script is not working properly.

Which of the following changes should the tester apply to make the script work as intended?

A. Change line 2 to $ip= 10.192.168.254;

B. Remove lines 3, 5, and 6.

C. Remove line 6.

D. Move all the lines below line 7 to the top of the script.

Correct Answer: B

https://www.asc.ohio-state.edu/lewis.239/Class/Perl/perl.html Example script:

#!/usr/bin/perl

$ip=$argv[1];

attack($ip);

sub attack {

print("x");

}

QUESTION 15

A penetration tester presents the following findings to stakeholders:

Control | Number of findings | Risk | Notes

Encryption | 1 | Low | Weak algorithm noted

Patching | 8 | Medium | Unsupported systems

System hardening | 2 | Low | Baseline drift observed

Secure SDLC | 10 | High | Libraries have vulnerabilities

Password policy | 0 | Low | No exceptions noted

Based on the findings, which of the following recommendations should the tester make? (Select two).

A. Develop a secure encryption algorithm.

B. Deploy an asset management system.

C. Write an SDLC policy.

D. Implement an SCA tool.

E. Obtain the latest library version.

F. Patch the libraries.

Correct Answer: DE

Based on the findings, the focus should be on addressing vulnerabilities in libraries and ensuring their security. Here\\'s why options D and E are correct:

Implement an SCA Tool:

Obtain the Latest Library Version:

Other Options Analysis:

Develop a Secure Encryption Algorithm: This is not practical or necessary given that the issue is with the use of a weak algorithm, not the need to develop a new one. Deploy an Asset Management System: While useful, this is not directly

related to the identified high-risk issue of vulnerable libraries. Write an SDLC Policy: While helpful, the more immediate and effective actions involve implementing tools and processes to manage and update libraries.

References from Pentest:

Horizontall HTB: Demonstrates the importance of managing software dependencies and using tools to identify and mitigate vulnerabilities in libraries. Writeup HTB: Highlights the need for keeping libraries updated to ensure application

security and mitigate risks.

Conclusion:

Options D and E, implementing an SCA tool and obtaining the latest library version, are the most appropriate recommendations to address the high-risk finding related to vulnerable libraries in the Secure SDLC process.