PT0-002 Q&As

CompTIA PenTest+ Certification Exam

Pass CompTIA PT0-002 Exam with 100% Guarantee

QUESTION 1

Which of the following is the BEST resource for obtaining payloads against specific network infrastructure products?

A. Exploit-DB

B. Metasploit

C. Shodan

D. Retina

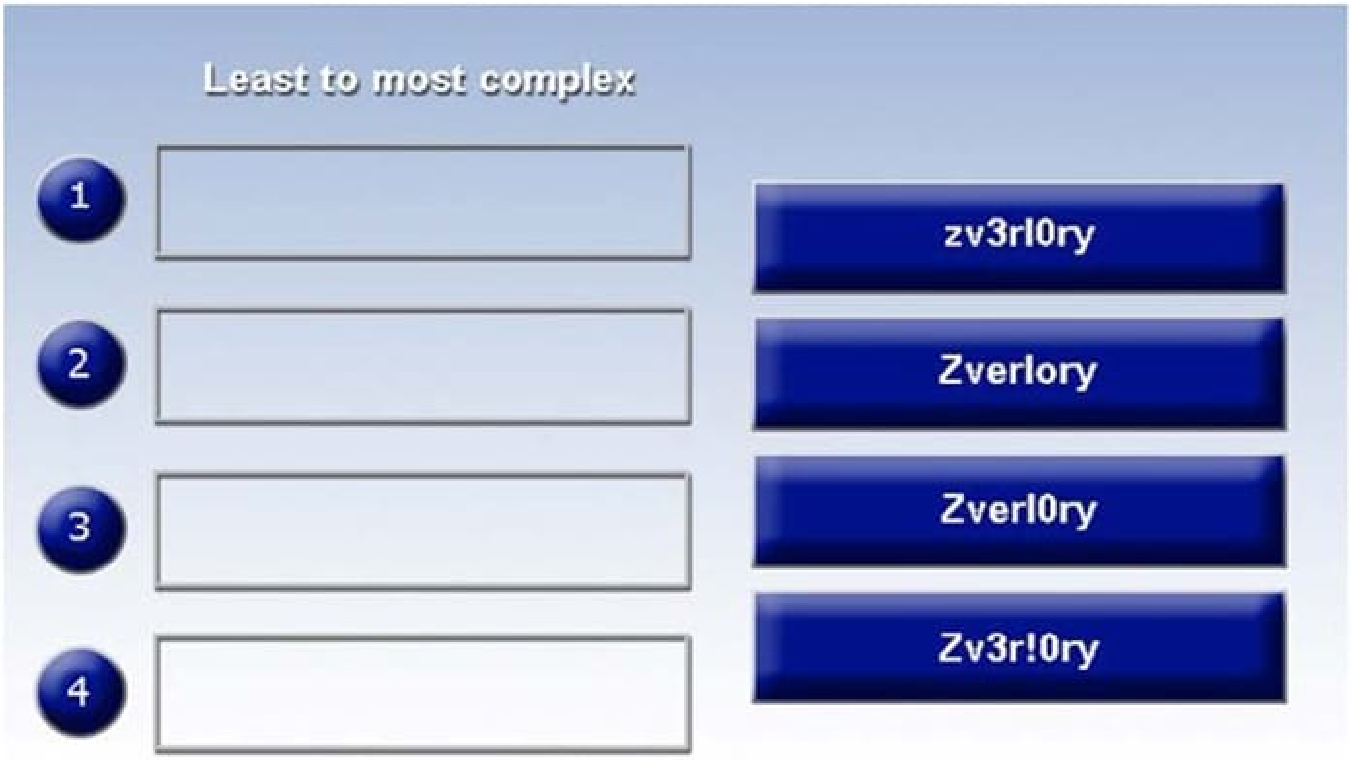
Correct Answer: A

"Exploit Database (ExploitDB) is a repository of exploits for the purpose of public security, and it explains what can be found on the database. The ExploitDB is a very useful resource for identifying possible weaknesses in your network and for staying up to date on current attacks occurring in other networks"

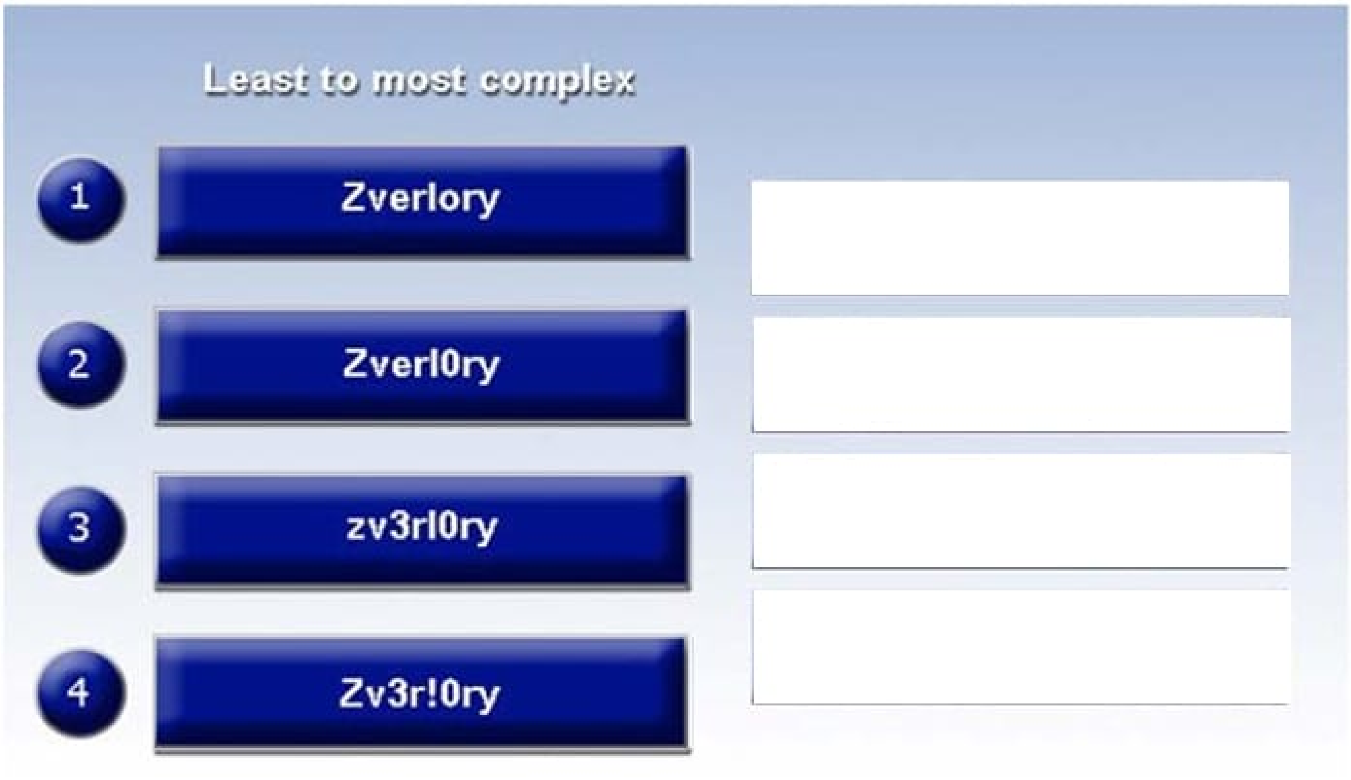
QUESTION 2

Place each of the following passwords in order of complexity from least complex (1) to most complex (4), based on the character sets represented Each password may be used only once.

Select and Place:



Correct Answer:



Least to most complex

1 Zverlory

2 Zverl0ry

3 zv3rl0ry

4 Zv3r!0ry

QUESTION 3

Penetration-testing activities have concluded, and the initial findings have been reviewed with the client. Which of the following best describes the NEXT step in the engagement?

A. Acceptance by the client and sign-off on the final report

B. Scheduling of follow-up actions and retesting

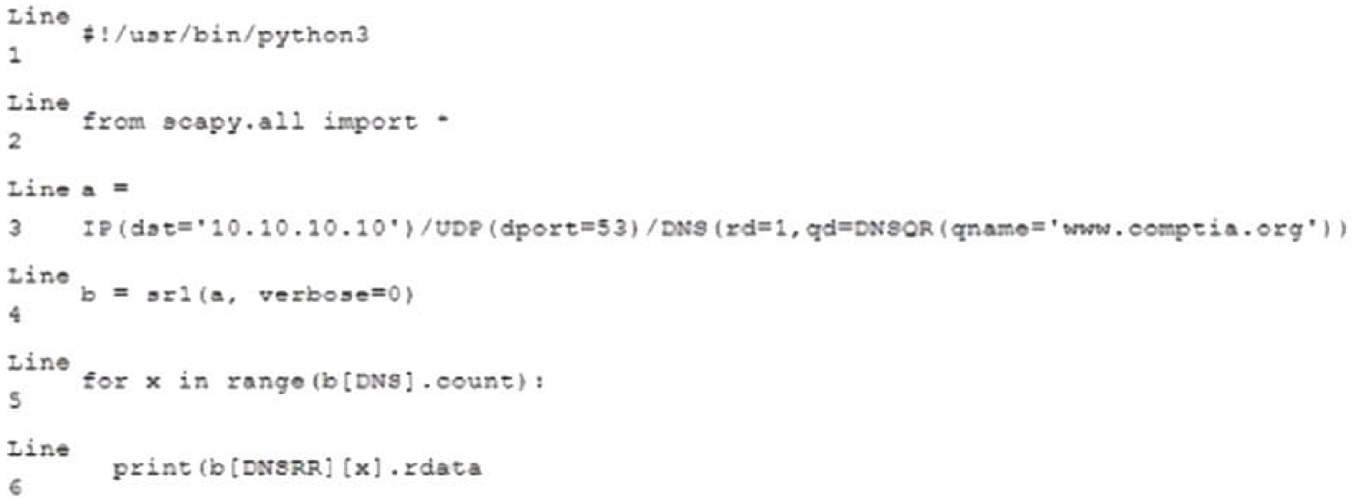
C. Attestation of findings and delivery of the report

D. Review of the lessons learned during the engagement

Correct Answer: C

QUESTION 4

Given the following script:



```
Line 1  #!/usr/bin/python3
Line 2  from scapy.all import *
Line 3  a = IP(dst='10.10.10.10')/UDP(dport=53)/DNS(rd=1,qd=DNSQR(qname='www.comptia.org'))
Line 4  b = sr1(a, verbose=0)
Line 5  for x in range(b[DNS].count):
Line 6      print(b[DNSRR][x].rdata
```

Which of the following BEST characterizes the function performed by lines 5 and 6?

A. Retrieves the start-of-authority information for the zone on DNS server 10.10.10.10

B. Performs a single DNS query for www.comptia.org and prints the raw data output

C. Loops through variable b to count the results returned for the DNS query and prints that count to screen

D. Prints each DNS query result already stored in variable b

Correct Answer: D

QUESTION 5

A penetration tester opened a reverse shell on a Linux web server and successfully escalated privileges to root. During the engagement, the tester noticed that another user logged in frequently as root to perform work tasks.

To avoid disrupting this user\\'s work, which of the following is the BEST option for the penetration tester to maintain root-level persistence on this server during the test?

A. Add a web shell to the root of the website.

B. Upgrade the reverse shell to a true TTY terminal.

C. Add a new user with ID 0 to the /etc/passwd file.

D. Change the password of the root user and revert after the test.

Correct Answer: C

The best option for the penetration tester to maintain root-level persistence on this server during the test is to add a new user with ID 0 to the /etc/passwd file. This will allow the penetration tester to use the same user account as the other user, but with root privileges, meaning that it won\\'t disrupt the other user\\'s work. This can be done by adding a new line with the username and the numerical user ID 0 to the /etc/passwd file. For example, if the username for the other user is "johndoe", the line to add would be "johndoe:x:0:0:John Doe:/root:/bin/bash". After the user is added, the penetration tester can use the "su" command to switch to the new user and gain root privileges.

QUESTION 6

A penetration tester is cleaning up and covering tracks at the conclusion of a penetration test. Which of the following should the tester be sure to remove from the system? (Choose two.)

A. Spawned shells

B. Created user accounts

C. Server logs

D. Administrator accounts

E. Reboot system

F. ARP cache

Correct Answer: AB

Removing shells: Remove any shell programs installed when performing the pentest.

Removing tester-created credentials: Be sure to remove any user accounts created during the pentest. This includes backdoor accounts. Removing tools: Remove any software tools that were installed on the customer\\'s systems that were

used to aid in the exploitation of systems.

QUESTION 7

A consulting company is completing the ROE during scoping. Which of the following should be included in the ROE?

A. Cost ofthe assessment

B. Report distribution

C. Testing restrictions

D. Liability

Correct Answer: B

QUESTION 8

A company hired a penetration-testing team to review the cyber-physical systems in a manufacturing plant. The team immediately discovered the supervisory systems and PLCs are both connected to the company intranet. Which of the following assumptions, if made by the penetration-testing team, is MOST likely to be valid?

A. PLCs will not act upon commands injected over the network.

B. Supervisors and controllers are on a separate virtual network by default.

C. Controllers will not validate the origin of commands.

D. Supervisory systems will detect a malicious injection of code/commands.

Correct Answer: C

QUESTION 9

A penetration tester completed an assessment, removed all artifacts and accounts created during the test, and presented the findings to the client. Which of the following happens NEXT?

A. The penetration tester conducts a retest.

B. The penetration tester deletes all scripts from the client machines.

C. The client applies patches to the systems.

D. The client clears system logs generated during the test.

Correct Answer: C

QUESTION 10

In the process of active service enumeration, a penetration tester identifies an SMTP daemon running on one of the target company\\'s servers.

Which of the following actions would BEST enable the tester to perform phishing in a later stage of the assessment?

A. Test for RFC-defined protocol conformance.

B. Attempt to brute force authentication to the service.

C. Perform a reverse DNS query and match to the service banner.

D. Check for an open relay configuration.

Correct Answer: D

SMTP is a protocol associated with mail servers. Therefore, for a penetration tester, an open relay configuration can be exploited to launch phishing attacks.

QUESTION 11

A company hired a penetration tester to do a social-engineering test against its employees. Although the tester did not find any employees\\' phone numbers on the company\\'s website, the tester has learned the complete phone catalog was published there a few months ago.

In which of the following places should the penetration tester look FIRST for the employees numbers?

A. Web archive

B. GitHub

C. File metadata

D. Underground forums

Correct Answer: A

QUESTION 12

In an unprotected network file repository, a penetration tester discovers a text file containing usernames and passwords in cleartext and a spreadsheet containing data for 50 employees, including full names, roles, and serial numbers. The tester realizes some of the passwords in the text file follow the format: . Which of the following would be the best action for the tester to take NEXT with this information?

A. Create a custom password dictionary as preparation for password spray testing.

B. Recommend using a password manage/vault instead of text files to store passwords securely.

C. Recommend configuring password complexity rules in all the systems and applications.

D. Document the unprotected file repository as a finding in the penetration-testing report.

Correct Answer: D

QUESTION 13

Which of the following tools would BEST allow a penetration tester to capture wireless handshakes to reveal a Wi-Fi password from a Windows machine?

A. Wireshark

B. EAPHammer

C. Kismet

D. Aircrack-ng

Correct Answer: D

The BEST tool to capture wireless handshakes to reveal a Wi-Fi password from a Windows machine is Aircrack-ng. Aircrack-ng is a suite of tools used to assess the security of wireless networks. It starts by capturing wireless network packets [1], then attempts to crack the network password by analyzing them [1]. Aircrack-ng supports FMS, PTW, and other attack types, and can also be used to generate keystreams for WEP and WPA-PSK encryption. It is capable of running on Windows, Linux, and Mac OS X. The BEST tool to capture wireless handshakes to reveal a Wi-Fi password from a Windows machine is Aircrack-ng. Aircrack-ng is a suite of tools used to assess the security of wireless networks. It starts by capturing wireless network packets [1], then attempts to crack the network password by analyzing them [1]. Aircrack-ng supports FMS, PTW, and other attack types, and can also be used to generate keystreams for WEP and WPAPSK encryption. It is capable of running on Windows, Linux, and Mac OS X.

QUESTION 14

A red team completed an engagement and provided the following example in the report to describe how the team gained access to a web server:

x\\' OR role LIKE \\'%admin%

Which of the following should be recommended to remediate this vulnerability?

A. Multifactor authentication

B. Encrypted communications

C. Secure software development life cycle

D. Parameterized queries

Correct Answer: D

QUESTION 15

A penetration tester obtained the following results after scanning a web server using the dirb utility:

```
...

GENERATED WORDS: 4612

---- Scanning URL: http://10.2.10.13/---

+

 http://10.2.10.13/about (CODE:200|SIZE:1520)

+

 http://10.2.10.13/home.html (CODE:200|SIZE:214)

+

 http://10.2.10.13/index.html (CODE:200|SIZE:214)

+

 http://10.2.10.13/info (CODE:200|SIZE:214)

...

DOWNLOADED: 4612 FOUND: 4
```

Which of the following elements is MOST likely to contain useful information for the penetration tester?

A.

index.html

B.

about

C.

info

D.

home.html

Correct Answer: B