Vendor: CompTIA

Exam Code:PT0-001

Exam Name: CompTIA PenTest+ Exam

Version: Demo

QUESTION 1

A client has scheduled a wireless penetration test. Which of the following describes the scoping target information MOST likely needed before testing can begin?

A. The physical location and network ESSIDs to be tested

B. The number of wireless devices owned by the client

C. The client\\'s preferred wireless access point vendor

D. The bands and frequencies used by the client\\'s devices

Correct Answer: D

QUESTION 2

Which of the following CPU registers does the penetration tester need to overwrite in order to exploit a simple buffer overflow?

A. Stack pointer register

B. Index pointer register

C. Stack base pointer

D. Destination index register

Correct Answer: A

Reference: http://www.informit.com/articles/article.aspx?p=704311andseqNum=3

QUESTION 3

A penetration tester is planning to conduct a distributed dictionary attack on a government domain against the login portal. The tester will leverage multiple proxies to mask the origin IPs of the attack. Which of the following threat actors will be emulated?

A. APT

B. Hacktivist

C. Script kiddie

D. Insider threat

Correct Answer: A

Reference: https://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/

QUESTION 4

A recently concluded penetration test revealed that a legacy web application is vulnerable to SQL injection. Research indicates that completely remediating the vulnerability would require an architectural change, and the stakeholders are not in a position to risk the availability on the application. Under such circumstances, which of the following controls are low-effort, short-term solutions to minimize the SQL injection risk? (Choose two.)

A. Identify and eliminate inline SQL statements from the code.

B. Identify and eliminate dynamic SQL from stored procedures.

C. Identify and sanitize all user inputs.

D. Use a whitelist approach for SQL statements.

E. Use a blacklist approach for SQL statements.

F. Identify the source of malicious input and block the IP address.

Correct Answer: CD

QUESTION 5

During a penetration test a tester Identifies traditional antivirus running on the exploited server. Which of the following techniques would BEST ensure persistence in a post-exploitation phase?

A. Shell binary placed in C \windowsttemp

B. Modified daemons

C. New user creation

D. Backdoored executaWes

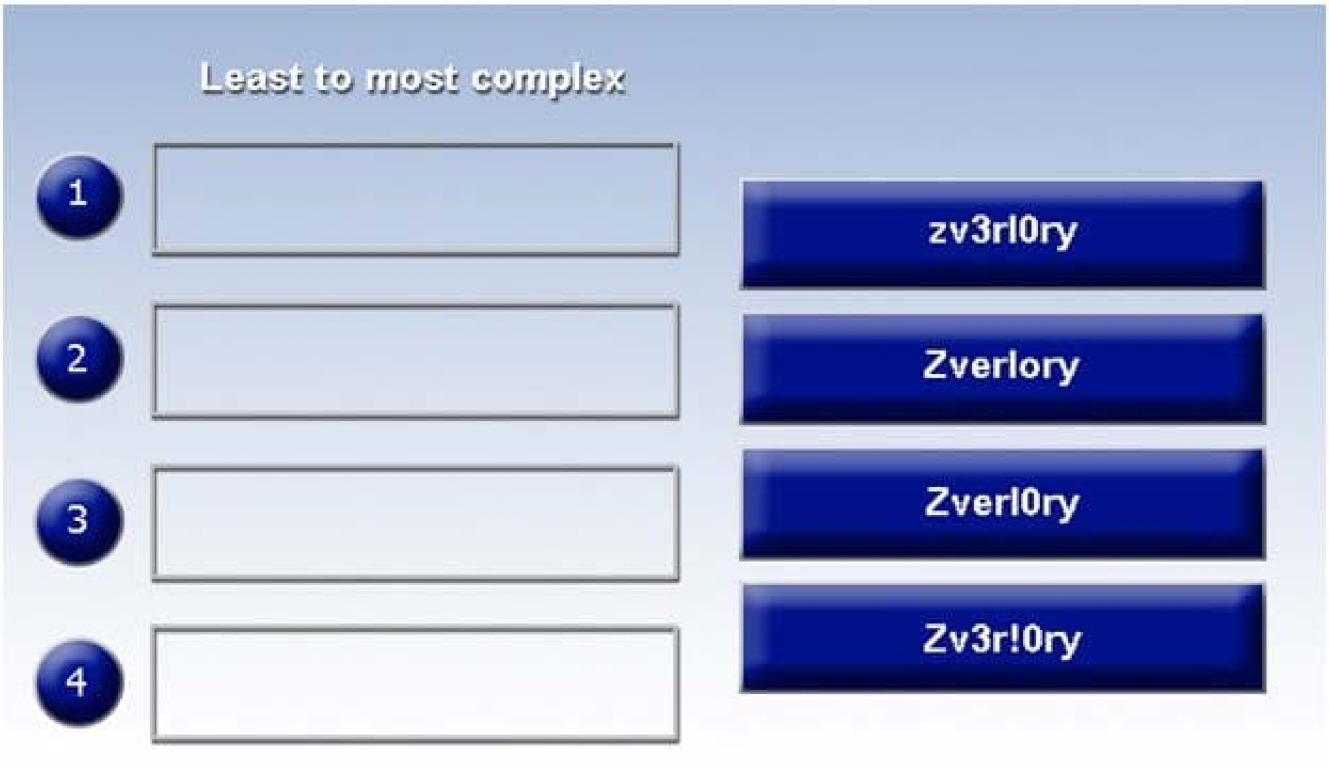
Correct Answer: B

QUESTION 6

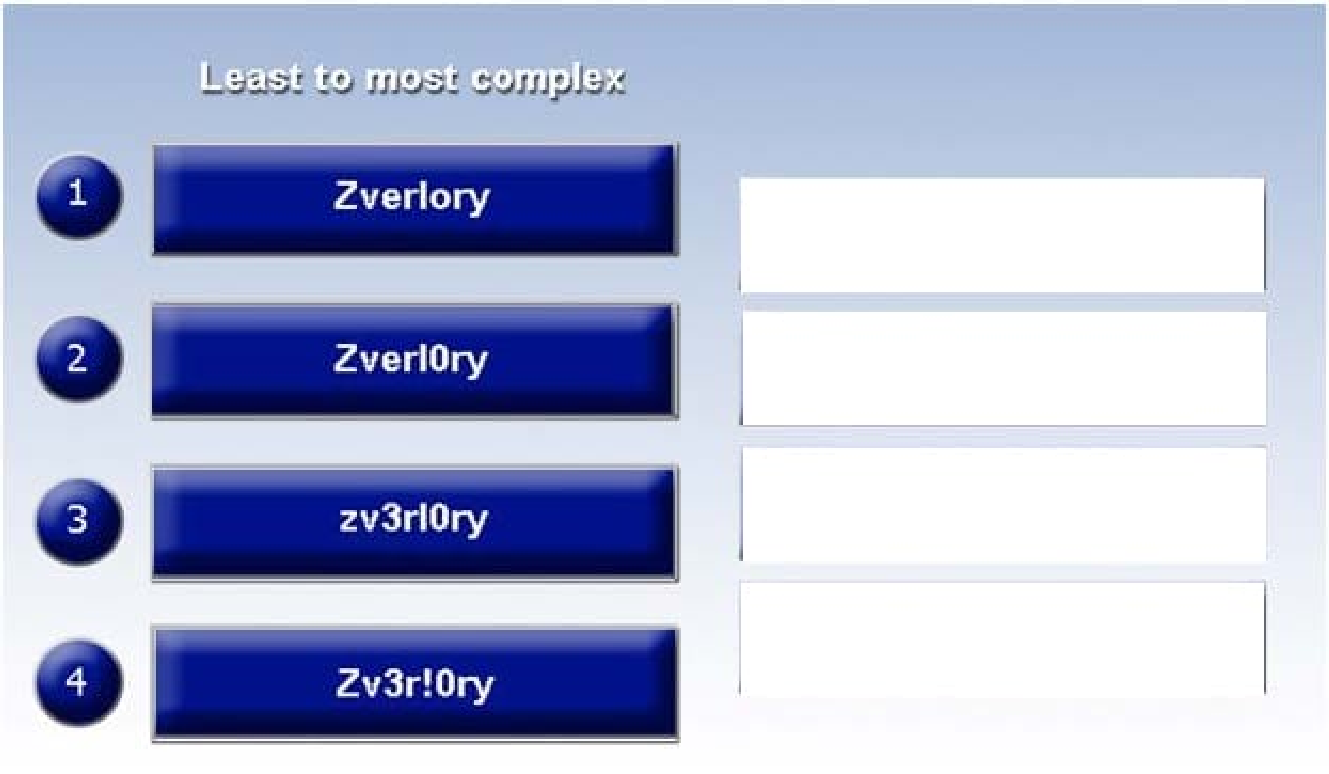
DRAG DROP

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 7

A penetration tester found a network with NAC enabled Which of the following commands can be used to bypass the NAC?

A. macchanger

B. sslbump

C. iptafcles

D. proxychains

Correct Answer: A

QUESTION 8

Which of the following BEST protects against a rainbow table attack?

A. Increased password complexity

B. Symmetric encryption

C. Cryptographic salting

D. Hardened OS configurations

Correct Answer: A

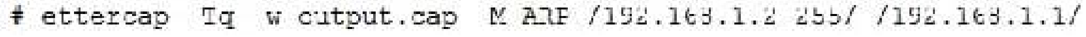
Reference: https://www.sciencedirect.com/topics/computer-science/rainbow-table

---

QUESTION 9

A penetration tester is performing a remote internal penetration test by connecting to the testing system from the Internet via a reverse SSH tunnel. The testing system has been placed on a general user subnet with an IP address of

192.168.1.13 and a gateway of 192.168.1.1. Immediately after running the command below, the penetration tester\\'s SSH connection to the testing platform drops:



```
# ettercap  Tq  w output.cap  M ARP /192.168.1.2 255/ /192.168.1.1/
```

Which of the following ettercap commands should the penetration tester use in the future to perform ARP spoofing while maintaining a reliable connection?

A. # sudo ettercap –Tq –w output.cap –M ARP /192.168.1.0/ /192.168.1.255/

B. # proxychains ettercap –Tq –w output.cap –M ARP /192.168.1.13/ /192.168.1.1/

C. # ettercap –Tq –w output.cap –M ARP 00:00:00:00:00:00//80 FF:FF:FF:FF:FF:FF//80

D. # ettercap —safe-mode –Tq –w output.cap –M ARP /192.168.1.2–255/ /192.168.1.13/

E. # ettercap –Tq –w output.cap –M ARP /192.168.1.2–12;192.168.1.14–255/ /192.168.1.1/

Correct Answer: A

QUESTION 10

A penetration tester obtained access to an internal host of a given target. Which of the following is the BEST tool to retrieve the passwords of users of the machine exploiting a well-knows architecture flaw of the Windows OS?

A. Mimikatz

B. John the Ripper

C. RainCrack

D. Hashcat

Correct Answer: A

QUESTION 11

When considering threat actor scoping prior to an engagement, which of the following characteristics makes an APT challenging to emulate?

A. Development of custom zero-day exploits and tools

B. Leveraging the dark net for non-attribution

C. Tenacity and efficacy of social engineering attacks

D. Amount of bandwidth available for DoS attacks

Correct Answer: C

QUESTION 12

Which of the following is an example of a spear phishing attack?

A. Targeting an executive with an SMS attack

B. Targeting a specific team with an email attack

C. Targeting random users with a USB key drop

D. Targeting an organization with a watering hole attack

Correct Answer: A

Reference: https://www.comparitech.com/blog/information-security/spear-phishing/