PT0-001 Q&As

CompTIA PenTest+ Exam

Pass CompTIA PT0-001 Exam with 100% Guarantee

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

https://www.passapply.com/pt0-001.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

After successfully enumerating users on an Active Directory domain controller using enum4linux a penetration tester wants to conduct a password-guessing attack Given the below output: Which of the following can be used to extract usernames from the above output prior to conducting the attack?

```
enum4linux_output.txt:
Starting enum4linux v0.8.2 ( https://labs.portcullis.co.uk/application/enum4linux/ ) on Mon Feb 5 11:36:22 2018

---- Users on 192.168.2.55 ----
index: 0x1 RID: 0x1f4 acb: 0x210 Account: Administrator Name: Built-in account for administering the computer/domain
index 0x2 RID: 0x3ee acb: 0x10 Account test Name: test Desc:
index 0x3 RID: 0x3ed acb: 0x215 Account: Guest Name: Guest Desc: Built-in account for guest access to the computer/domain
index 0x4: RID: 0x1f5 acb: 0x214 Account: Test_User Name:Test User Account: Desc:

user:[Administrator] rid:[0x1f4]
user:[test] rid:[0x3ee]
user:[Guest] rid:[0x3ed]
user:[Test_User] rid:[0x1f5]
```

A. cat enum41inux_output.txt > grep -v user I sed `s/\[//\\' I sed `s/\]//\\' 2> usernames.txt

B. grep user enuza41inux_output.txt I awk \\'{print $1}\\' | cut -d[-? I cut -d] -f1>; username.txt

C. grep -i rid v; usernames. txt

D. cut -d: -f2 enum41inux_output.txt | awk \\'{print S2}\\' I cut -d: -f1 > usernaraes.txt

Correct Answer: B

QUESTION 2

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 3

A penetration tester is able to move laterally throughout a domain with minimal roadblocks after compromising a single workstation. Which of the following mitigation strategies would be BEST to recommend in the report? (Select THREE).

A. Randomize local administrator credentials for each machine.

B. Disable remote logons for local administrators.

C. Require multifactor authentication for all logins.

D. Increase minimum password complexity requirements.

E. Apply additional network access control.

F. Enable full-disk encryption on every workstation.

G. Segment each host into its own VLAN.

Correct Answer: CDE

QUESTION 4

A penetration tester has compromised a system and wishes to connect to a port on it from the attacking machine to control the system Which of the following commands should the tester run on the compromised system?

A. nc looalhot 4423

B. nc -nvlp 4423 -?/bin/bash

C. nc 10.0.0.1 4423

D. nc 127.0.0.1 4423 -e /bin/bash

Correct Answer: B

QUESTION 5

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 6

When calculating the sales price of a penetration test to a client, which of the following is the MOST important aspect to understand?

A. The operating cost

B. The client\\'s budget

C. The required scope of work

D. The non-disclosure agreement

Correct Answer: C

QUESTION 7

A company performed an annual penetration test of its environment. In addition to several new findings, all of the previously identified findings persisted on the latest report.

Which of the following is the MOST likely reason?

A. Infrastructure is being replaced with similar hardware and software.

B. Systems administrators are applying the wrong patches.

C. The organization is not taking action to remediate identified findings.

D. The penetration testing tools were misconfigured.

Correct Answer: C

QUESTION 8

Which of the following documents BEST describes the manner in which a security assessment will be conducted?

A. BIA

B. SOW

C. SLA

D. MSA

Correct Answer: A

QUESTION 9

A penetration tester is attempting to scan a legacy web application using the scanner\\'s default scan settings. The scans continually result in the application becoming unresponsive. Which of the following can help to alleviate this issue?

A. Packet shaping

B. Flow control

C. Bandwidth limits

D. Query throttling

Correct Answer: A

QUESTION 10

A penetration tester notices that the X-Frame-Optjons header on a web application is not set. Which of the following would a malicious actor do to exploit this configuration setting?

A. Use path modification to escape the application\\'s framework.

B. Create a frame that overlays the application.

C. Inject a malicious iframe containing JavaScript.

D. Pass an iframe attribute that is malicious.

Correct Answer: C

QUESTION 11

Which of the following commands starts the Metasploit database?

A. msfconsole

B. workspace

C. msfvenom

D. db_init

E. db_connect

Correct Answer: A

References: https://www.offensive-security.com/metasploit-unleashed/msfconsole/

QUESTION 12

A security consultant is trying to attack a device with a previously identified user account.

```
Module options (exploit/windows/smb/psexec):

Name                  Current Setting                                                  Required
----                  ---------------                                                  --------
RHOST                 192.168.1.10                                                     yes
RPORT                 445                                                              yes
SERVICE_DESCRIPTION                                                                    no
SERVICE_DISPLAY_NAME                                                                   no
SERVICE_NAME                                                                           no
SHARE                 ADMIN$                                                           yes
SMBDOMAIN             ECorp                                                            no
SMBPASS               aad3b435b514004ccaad3b435b5140ee:gbh5n356b58700ggppd6m2439ep no
SMBUSER               Administrator                                                    no
```

Which of the following types of attacks is being executed?

A. Credential dump attack

B. DLL injection attack

C. Reverse shell attack

D. Pass the hash attack

Correct Answer: D

QUESTION 13

A penetration tester is performing a wireless penetration test. Which of the following are some vulnerabilities that might allow the penetration tester to easily and quickly access a WPA2-protected access point?

A. Deauthentication attacks against an access point can allow an opportunity to capture the four-way handshake, which can be used to obtain and crack the encrypted password.

B. Injection of customized ARP packets can generate many initialization vectors quickly, making it faster to crack the password, which can then be used to connect to the WPA2-protected access point.

C. Weak implementations of the WEP can allow pin numbers to be guessed quickly, which can then be used to retrieve the password, which can then be used to connect to the WEP-protected access point.

D. Rainbow tables contain all possible password combinations, which can be used to perform a brute-force password attack to retrieve the password, which can then be used to connect to the WPA2-protected access point.

Correct Answer: C

QUESTION 14

A penetration tester has gained access to a marketing employee\\'s device. The penetration tester wants to ensure that

if the access is discovered, control of the device can be regained. Which of the following actions should the penetration tester use to maintain persistence to the device? (Select TWO.)

A. Place an entry in HKLM\Software\Microsoft\CurrentVersion\Run to call au57d.ps1.

B. Place an entry in C:\windows\system32\drivers\etc\hosts for 12.17.20.10 badcomptia.com.

C. Place a script in C:\users\%username\local\appdata\roaming\temp\au57d.ps1.

D. Create a fake service in Windows called RTAudio to execute manually.

E. Place an entry for RTAudio in HKLM\CurrentControlSet\Services\RTAudio.

F. Create a schedule task to call C:\windows\system32\drivers\etc\hosts.

Correct Answer: AC

QUESTION 15

A penetration tester has performed a security assessment for a startup firm. The report lists a total of ten vulnerabilities, with five identified as critical. The client does not have the resources to immediately remediate all vulnerabilities. Under such circumstances, which of the following would be the BEST suggestion for the client?

A. Apply easy compensating controls for critical vulnerabilities to minimize the risk, and then reprioritize remediation.

B. Identify the issues that can be remediated most quickly and address them first.

C. Implement the least impactful of the critical vulnerabilities\\' remediations first, and then address other critical vulnerabilities

D. Fix the most critical vulnerability first, even if it means fixing the other vulnerabilities may take a very long lime.

Correct Answer: D