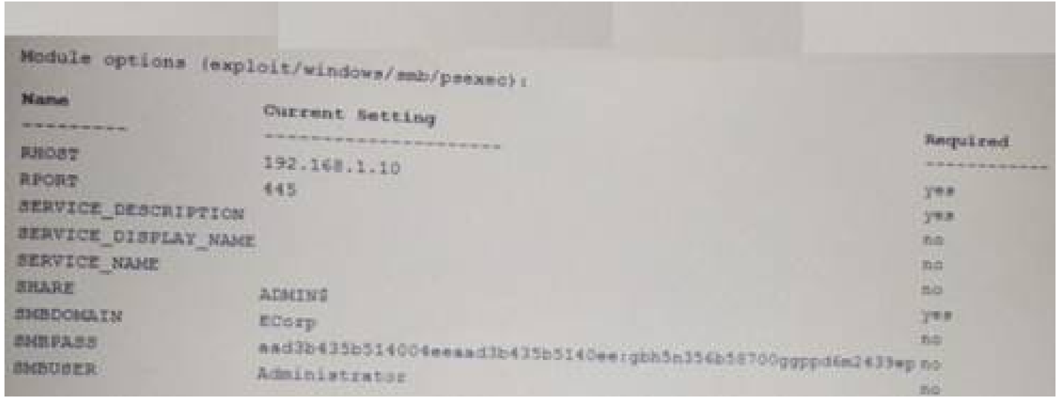
Exam Questions PT0-001

CompTIA PenTest+ Certification Exam

https://www.2passeasy.com/dumps/PT0-001/

NEW QUESTION 1
A security consultant is trying to attack a device with a previous 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                aad3b435b51404eeaad3b435b51404ee:gbh5n356b58700gppd6m2433ep             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

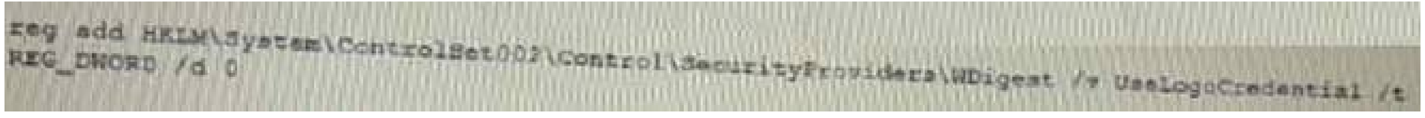
Answer: D

NEW QUESTION 2
A client is asking a penetration tester to evaluate a new web application for availability. Which of the following types of attacks should the tester use?

A. TCP SYN flood
B. SQL injection
C. xss
D. XMAS scan

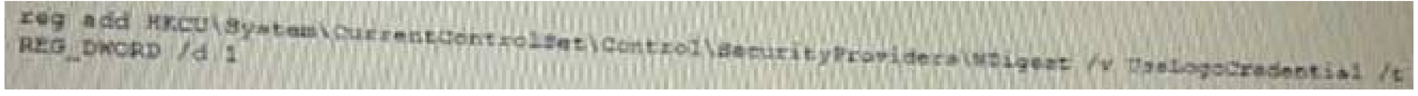
Answer: A

NEW QUESTION 3
During a penetration test, a tester runs a phishing campaign and receives a shell from an internal PC running Windows 10 OS. The tester wants to perform credential harvesting with Mimikazt. Which of the following registry changes would allow for credential caching in memory?
A)



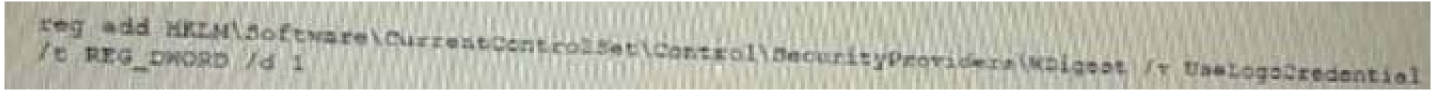
```
reg add HKLM\System\ControlSet002\Control\SecurityProviders\WDigest /v UseLogoCredential /t
REG_DWORD /d 0
```

B)



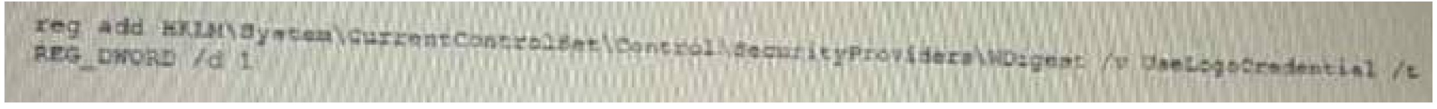
```
reg add HKCU\System\CurrentControlSet\Control\SecurityProviders\WDigest /v UseLogoCredential /t
REG_DWORD /d 1
```

C)



```
reg add HKLM\Software\CurrentControlSet\Control\SecurityProviders\WDigest /v UseLogoCredential
/t REG_DWORD /d 1
```

D)



```
reg add HKLM\System\CurrentControlSet\Control\SecurityProviders\WDigest /v UseLogoCredential /t
REG_DWORD /d 1
```

A. Option A
B. Option B
C. Option C
D. Option D

Answer: D

NEW QUESTION 4
In which of the following components is an explogted vulnerability MOST likely to affect multiple running application containers at once?

A. Common libraries
B. Configuration files
C. Sandbox escape
D. ASLR bypass

Answer: D

NEW QUESTION 5
If a security consultant comes across a password hash that resembles the following b117 525b3454 7Oc29ca3dBaeOb556ba8
Which of the following formats is the correct hash type?

A. Kerberos
B. NetNTLMvl

C. NTLM
D. SHA-1

Answer: C

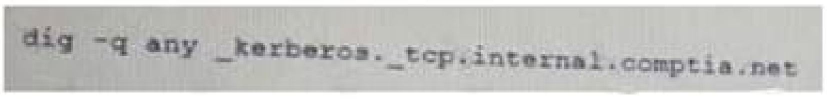
NEW QUESTION 6
A penetration tester was able to retrieve the initial VPN user domain credentials by phishing a member of the IT department. Afterward, the penetration tester obtained hashes over the VPN and easily cracked them using a dictionary attack Which of the following remediation steps should be recommended? (Select THREE)

A. Mandate all employees take security awareness training
B. Implement two-factor authentication for remote access
C. Install an intrusion prevention system
D. Increase password complexity requirements
E. Install a security information event monitoring solution.
F. Prevent members of the IT department from interactively logging in as administrators
G. Upgrade the cipher suite used for the VPN solution

Answer: BDG

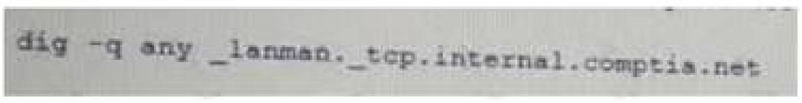
NEW QUESTION 7
An assessor begins an internal security test of the Windows domain internal. comptia. net. The assessor is given network access via DHCP, but is not given any network maps or target IP addresses. Which of the following commands can the assessor use to find any likely Windows domain controllers?

A)



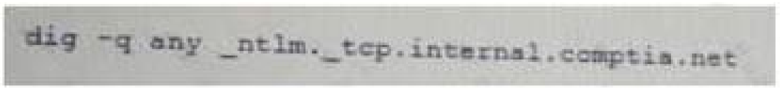
```
dig -q any _kerberos._tcp.internal.comptia.net
```

B)



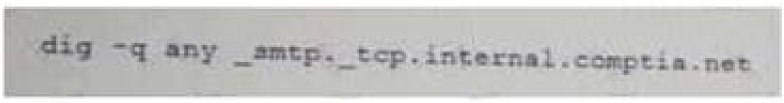
```
dig -q any _lanman._tcp.internal.comptia.net
```

C)



```
dig -q any _ntlm._tcp.internal.comptia.net
```

D)



```
dig -q any _smtp._tcp.internal.comptia.net
```

A. Option A
B. Option B
C. Option C
D. Option D

Answer: A

NEW QUESTION 8
While prioritizing findings and recommendations for an executive summary, which of the following considerations would De MOST valuable to the client?

A. Levels of difficulty to explogt identified vulnerabilities
B. Time taken to accomplish each step
C. Risk tolerance of the organization
D. Availability of patches and remediations

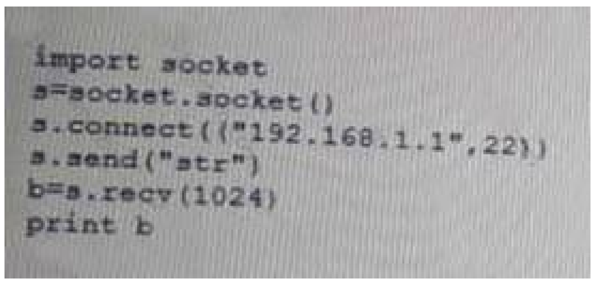
Answer: C

NEW QUESTION 9
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 explogt 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 maliciou

Answer: B

NEW QUESTION 10
Given the following Python script:



```
import socket
s=socket.socket()
s.connect(("192.168.1.1",22))
s.send("str")
b=s.recv(1024)
print b
```

Which of the following actions will it perform?

A. ARP spoofing
B. Port scanner
C. Reverse shell
D. Banner grabbing

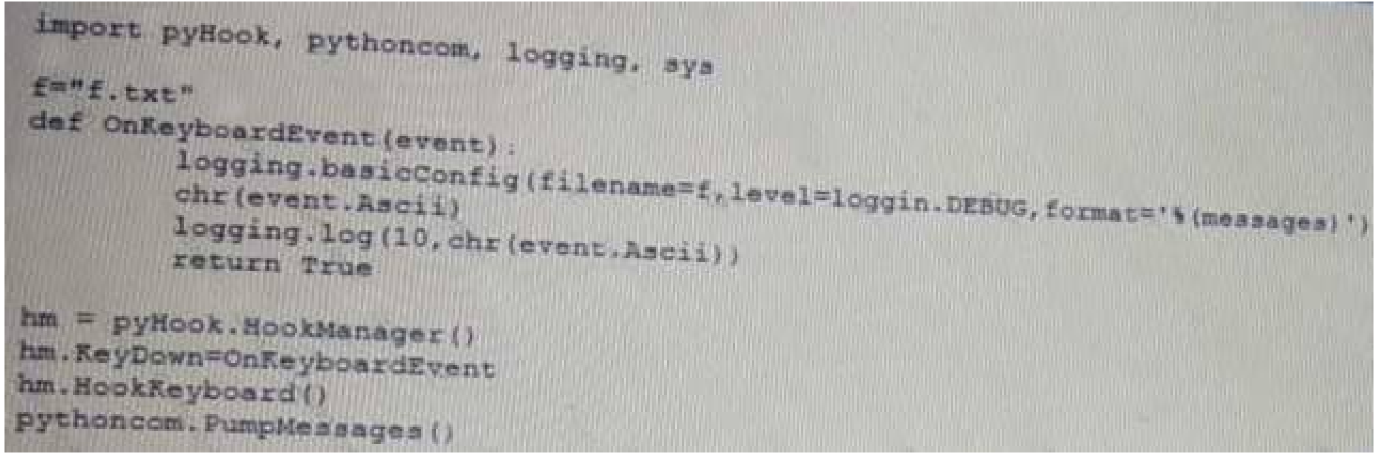
Answer: A

NEW QUESTION 10
A penetration tester runs the following from a compromised box 'python -c -import pty;Pty.sPawn("/bin/bash").' Which of the following actions is the tester taking?

A. Removing the Bash history
B. Upgrading the shell
C. Creating a sandbox
D. Capturing credentials

Answer: A

NEW QUESTION 12
Given the following script:



```
import pyHook, pythoncom, logging, sys
f="f.txt"
def OnKeyboardEvent(event):
        logging.basicConfig(filename=f,level=loggin.DEBUG,format='%(messages)')
        chr(event.Ascii)
        logging.log(10,chr(event.Ascii))
        return True

hm = pyHook.HookManager()
hm.KeyDown=OnKeyboardEvent
hm.HookKeyboard()
pythoncom.PumpMessages()
```

Which of the following BEST describes the purpose of this script?

A. Log collection
B. Event logging
C. Keystroke monitoring
D. Debug message collection

Answer: C

NEW QUESTION 14
Which of the following has a direct and significant impact on the budget of the security assessment?

A. Scoping
B. Scheduling
C. Compliance requirement
D. Target risk

Answer: A

NEW QUESTION 15
During an internal network penetration test, a tester recovers the NTLM password hash tor a user known to have full administrator privileges on a number of target systems Efforts to crack the hash and recover the plaintext password have been unsuccessful Which of the following would be the BEST target for continued exploglation efforts?

A. Operating system Windows 7 Open ports: 23, 161
B. Operating system Windows Server 2016 Open ports: 53, 5900
C. Operating system Windows 8 1Open ports 445, 3389
D. Operating system Windows 8 Open ports 514, 3389

Answer: C

NEW QUESTION 18
A client requests that a penetration tester emulate a help desk technician who was recently laid off. Which of the following BEST describes the abilities of the threat actor?

A. Advanced persistent threat
B. Script kiddie
C. Hacktivist
D. Organized crime

Answer: A

NEW QUESTION 22
Joe, a penetration tester, is asked to assess a company's physical security by gaining access to its corporate office. Joe ism looking for a method that will enable him to enter the building during business hours or when there are no employee on-site. Which of the following would be MOST effective in accomplishing this?

A. Badge cloning
B. Lock picking
C. Tailgating
D. Piggybacking

Answer: A

NEW QUESTION 23
Which of the following CPU register does the penetration tester need to overwrite in order to explogt a simple butter overflow?

A. Stack pointer register
B. Index pointer register
C. Stack base pointer
D. Destination index register

Answer: D

NEW QUESTION 27
A penetration test was performed by an on-staff technicians junior technician. During the test, the technician discovered the application could disclose an SQL table with user account and password information. Which of the following is the MOST effective way to notify management of this finding and its importance?

A. Document Ihe findtngs with an executive summary, recommendations, and screenshots of the web apphcation disclosure.
B. Connect to the SQL server using this information and change the password to one or two noncritical accounts to demonstrate a proof-of-concept to management.
C. Notify the development team of the discovery and suggest that input validation be implementedon the web application's SQL query strings.
D. Request that management create an RFP to begin a formal engagement with a professional penetration testing company.

Answer: B

NEW QUESTION 32
A penetration tester has been asked to conduct OS fingerprinting with Nmap using a companyprovide text file that contain a list of IP addresses.
Which of the following are needed to conduct this scan? (Select TWO).

A. -O
B. _iL
C. _sV
D. -sS
E. -oN
F. -oX

Answer: EF

NEW QUESTION 36
Which of Ihe following commands would allow a penetration tester to access a private network from the Internet in Metasplogt?

A. set rhost 192.168.1.10
B. run autoroute -a 192.168.1.0/24
C. db_nm«p -iL /tmp/privatehoots . txt
D. use auxiliary/servet/aocka^a

Answer: D

NEW QUESTION 40
A tester has captured a NetNTLMv2 hash using Responder Which of the following commands will allow the tester to crack the hash using a mask attack?

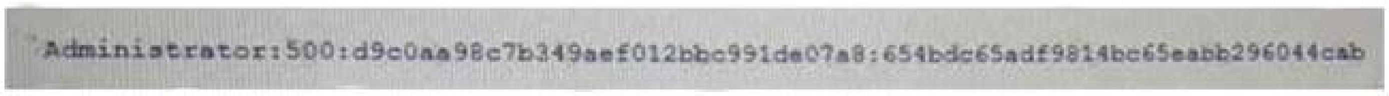
A. hashcat -m 5600 -r rulea/beat64.rule hash.txt wordliat.txt
B. hashcax -m 5€00 hash.txt
C. hashc&t -m 5600 -a 3 haah.txt ?a?a?a?a?a?a?a?a
D. hashcat -m 5600 -o reaulta.txt hash.txt wordliat.txt

Answer: A

NEW QUESTION 43
A penetration tester successfully explogts a Windows host and dumps the hashes Which of the following hashes can the penetration tester use to perform a pass-

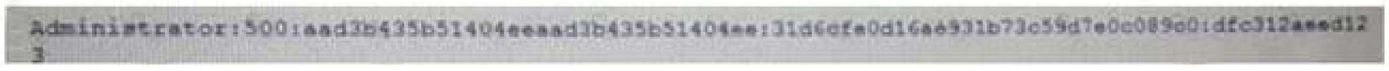
the-hash attack?

A)



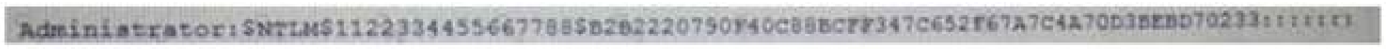
```
Administrator:500:d9c0aa98c7b349aef012bbc991de07a8:654bdc65adf9814bc65eabb296044cab
```

B)



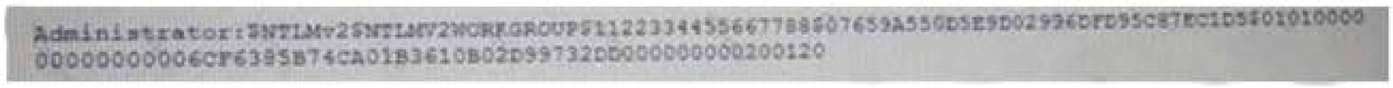
```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:dfc312aeed12
3
```

C)



```
Administrator:$NTLM$1122334455667788$B2B2220790F40C88BCFF347C652F67A7C4A70D3BEBD70233:::::
```

D)



```
Administrator:$NTLMv2$NTLMV2WORKGROUP$1122334455667788$07659A550D5E9D02996DFD95C87EC1D5$01010000
00000000006CF6385B74CA01B3610B02D99732DD000000000200120
```

A. Option A
B. Option B
C. Option C
D. Option D

Answer: D

NEW QUESTION 47

A tester has determined that null sessions are enabled on a domain controller. Which of the following attacks can be performed to leverage this vulnerability?

A. RID cycling to enumerate users and groups
B. Pass the hash to relay credentials
C. Password brute forcing to log into the host
D. Session hijacking to impersonate a system account

Answer: C

NEW QUESTION 49

A penetration tester ran the following Nmap scan on a computer nmap -sV 192.168.1.5
The organization said it had disabled Telnet from its environment However, the results of the Nmap scan show port 22 as closed and port 23 as open to SSH
Which of the following is the BEST explanation for what happened?

A. The organization failed to disable Telnet.
B. Nmap results contain a false positive for port 23.
C. Port 22 was filtered.
D. The service is running on a non-standard por

Answer: A

NEW QUESTION 51

......