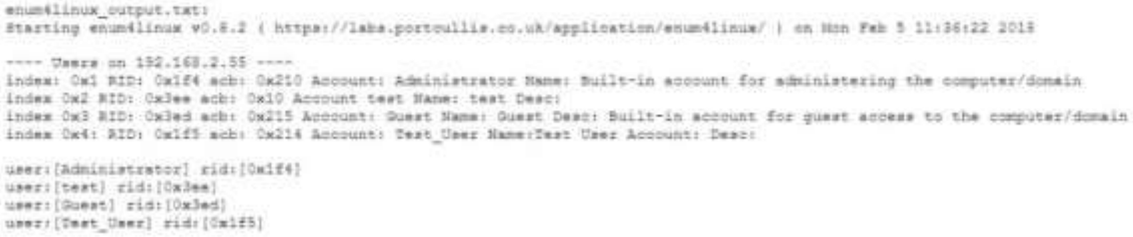
- **Vendor:** CompTIA
- **Exam Code:** PT0-001
- **Exam Name:** CompTIA PenTest+ Exam
- **New Updated Questions from Braindump2go (Updated in Nov./2020)**

Visit Braindump2go and Download Full Version PT0-001 Exam Dumps

QUESTION 159
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:



```
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]
```

Which of the following can be used to extract usernames from the above output prior to conducting the attack?

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< enura.41inux_output. txt' | cut -d: -? i cut -d] -f1>; usernames. txt
D. cut -d: -f2 enum41inux_output.txt | awk '{print S2}' I cut -d: -f1 > usernaraes.txt

Answer: B

QUESTION 160
Joe, a penetration tester, was able to exploit a web application behind a firewall He is trying to get a reverse shell back to his machine but the firewall blocks the outgoing traffic Ports for which of the following should the security consultant use to have the HIGHEST chance to bypass the firewall?

A. HTTP
B. SMTP
C. FTP
D. DNS

Answer: A

QUESTION 161
A penetration tester is performing an annual security assessment for a repeat client The tester finds indicators of previous compromise Which of the following would be the most logical steps to follow NEXT?

A. Report the incident to the tester's immediate manager and follow up with the client immediately
B. Report the incident to the clients Chief Information Security Officer (CISO) immediately and alter the terms of engagement accordingly
C. Report the incident to the client's legal department and then follow up with the client's security

operations team

D. Make note of the anomaly, continue with the penetration testing and detail it in the final report

Answer: A

QUESTION 162

A file contains several hashes. Which of the following can be used in a pass-the-hash attack?

A. NTLMv2
B. Kerberos
C. NTLMv1
D. LMv2
E. NTLM

Answer: B

QUESTION 163

A penetration tester must assess a web service. Which of the following should the tester request during the scoping phase?

A. XSD
B. After-hours contact escalation
C. WSDLfile
D. SOAP project file

Answer: C

QUESTION 164

A penetration tester is exploiting the use of default public and private community strings Which of the following protocols is being exploited?

A. SMTP
B. DNS
C. SNMP
D. HTTP

Answer: A

QUESTION 165

A consultant is identifying versions of Windows operating systems on a network Which of the following Nmap commands should the consultant run?

A. nmap -T4 -v -sU -iL /tmp/list.txt -Pn --script smb-system-info
B. nmap -T4 -v -iL /tmp/list .txt -Pn --script smb-os-disccvery
C. nmap -T4 -v -6 -iL /tmp/liat.txt -Pn --script smb-os-discovery -p 135-139
D. nmap -T4 -v --script smb-system-info 192.163.1.0/24

Answer: B

QUESTION 166

A penetration tester is using the Onesixtyone tool on Kali Linux to try to exploit the SNMP protocol on a target that has SNMP enabled Which of the following types of attacks is the penetration tester performing?

A. Buffer overflow attack

B. Man-in-the-middle attack
C. Dictionary-based attack
D. Name resolution attack

Answer: C

QUESTION 167
A web server is running PHP, and a penetration tester is using LFI to execute commands by passing parameters through the URL. This is possible because server logs were poisoned to execute the PHP system ( ) function. Which of the following would retrieve the contents of the passwd file?

A. "&CMD_cat /etc/passwd--&id-34"
B. "&CMD=cat / etc/passwd%&id= 34"
C. "&CMD=cat ../../../../etc/passwd7id=34'
D. "&system(CMD) "cat /etc/passed&id=34"

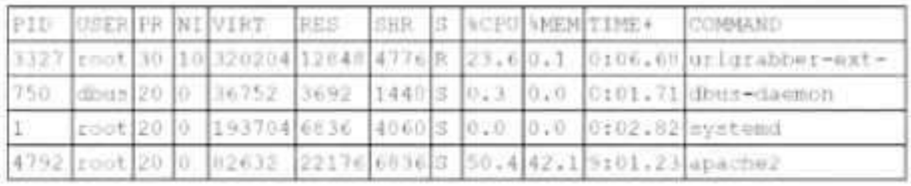
Answer: A

QUESTION 168
When conducting reconnaissance against a target, which of the following should be used to avoid directory communicating with the target?

A. Nmap tool
B. Maltego community edition
C. Nessus vulnerability scanner
D. OpenVAS
E. Melasploit

Answer: B

QUESTION 169
A penetration tester generates a report for a host-based vulnerability management agent that is running on a production web server to gather a list of running processes. The tester receives the following information.



PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
3327	root	30	10	320204	12648	4776	R	23.6	0.1	0:06.68	urlgrabber-ext-
750	dbus	20	0	36752	3692	1440	S	0.3	0.0	0:01.71	dbus-daemon
1	root	20	0	193704	6836	4060	S	0.0	0.0	0:02.82	systemd
4792	root	20	0	82632	22176	6836	S	50.4	42.1	9:01.23	apache2

\

Which of the following processes MOST likely demonstrates a lack of best practices?

A. apache2
B. dbus-daemon
C. systemd
D. urlgrabber-ext

Answer: B