GPEN Q&As

GIAC Certified Penetration Tester

Pass GIAC GPEN Exam with 100% Guarantee

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

https://www.leads4pass.com/gpen.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

You want to run the nmap command that includes the host specification of 202.176.56-57.*. How many hosts will you scan?

A. 256

B. 512

C. 1024

D. 64

Correct Answer: B

QUESTION 2

You have compromised a Windows XP system and Injected the Meterpreter payload into the lsass process. While looking over the system you notice that there is a popular password management program on the system. When you attempt to access the file that contains the password you find it is locked. Further investigation reveals that it is locked by the passmgr process. How can you use the Meterpreter to get access to this file?

A. Use the getuid command to determine the user context the process is runningunder, then use the imp command to impersonate that user.

B. use the getpid command to determine the user context the process is runningunder, then use the Imp command to impersonate that user.

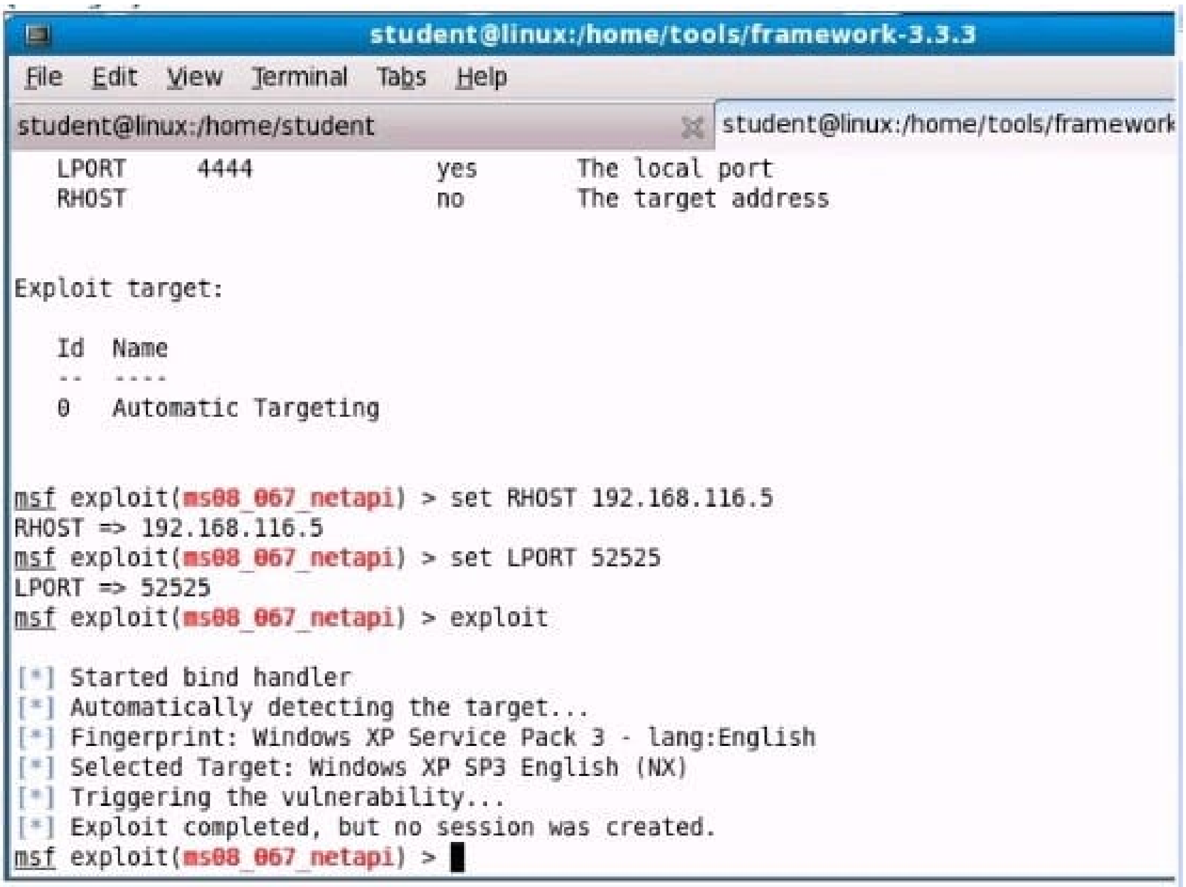
C. Use the execute command to the passmgr executable. That will give you access to the file.

D. Use the migrate command to jump to the passmgr process. That will give you accessto the file.

Correct Answer: C

QUESTION 3

Analyze the screenshot below. What event is depicted?


student@linux:/home/tools/framework-3.3.3
File Edit View Terminal Tabs Help
student@linux:/home/student
student@linux:/home/tools/framework

```
   LPORT     4444              yes       The local port
   RHOST                       no        The target address


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting


msf exploit(ms08_067_netapi) > set RHOST 192.168.116.5
RHOST => 192.168.116.5
msf exploit(ms08_067_netapi) > set LPORT 52525
LPORT => 52525
msf exploit(ms08_067_netapi) > exploit

[*] Started bind handler
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP Service Pack 3 - lang:English
[*] Selected Target: Windows XP SP3 English (NX)
[*] Triggering the vulnerability...
[*] Exploit completed, but no session was created.
msf exploit(ms08_067_netapi) >
```

A. An exploit that was attempted does not work against the target selected.

B. A payload was used that is not compatible with the chosen exploit.

C. The exploit is designed to work against the local host only.

D. The payload Is designed to create an interactive session.

Correct Answer: A

QUESTION 4

Which of the following tools can be used as a Linux vulnerability scanner that is capable of identifying operating systems and network services? Each correct answer represents a complete solution. Choose all that apply.

A. Cheops

B. Fport

C. Elsave

D. Cheops-ng

Correct Answer: AD

QUESTION 5

You run the following PHP script:

What is the use of the mysql_real_escape_string() function in the above script. Each correct answer represents a complete solution. Choose all that apply

A. It escapes all special characters from strings $_POST["name"] and $_POST["password"].

B. It escapes all special characters from strings $_POST["name"] and $_POST["password"] except \\' and ".

C. It can be used to mitigate a cross site scripting attack.

D. It can be used as a countermeasure against a SQL injection attack.

Correct Answer: AD

QUESTION 6

You are pen testing a network and have shell access to a machine via Netcat. You try to use ssh to access another machine from the first machine. What is the expected result?

A. The ssh connection will succeed If you have root access on the intermediate machine

B. The ssh connection will fail

C. The ssh connection will succeed

D. The ssh connection will succeed if no password required

Correct Answer: C

QUESTION 7

Which of the following is the default port value of beast Trojan?

A. 6666

B. 2222

C. 3333

D. 1111

Correct Answer: A

QUESTION 8

While reviewing traffic from a tcpdump capture, you notice the following commands being sent from a remote system to one of your web servers:

```
C:\>sc winternet.host.com create ncservice binpath- "c:\tools\ c.exe -l -p 2222 -e cmd.exe"
```

```
C:\>sc vJnternet.host.com query ncservice.
```

What is the intent of the commands?

A. The first command creates a backdoor shell as a service. It is being started on TCP2222 using cmd.exe. The second command verifies the service is created and itsstatus.

B. The first command creates a backdoor shell as a service. It is being started on UDP2222 using cmd.exe. The second command verifies the service is created and itsstatus.

C. This creates a service called ncservice which is linked to the cmd.exe command andits designed to stop any instance of nc.exe being run. The second command verifiesthe service is created and its status.

D. The first command verifies the service is created and its status. The secondcommand creates a backdoor shell as a service. It is being started on TCP 2222connected to cmd.exe.

Correct Answer: C

QUESTION 9

Which of the following scanning methods is most accurate and reliable, although it is easily detectable and hence avoided by a hacker?

A. TCP FIN

B. TCP half-open

C. TCP SYN/ACK

D. Xmas Tree

Correct Answer: C

QUESTION 10

John works as a professional Ethical Hacker. He has been assigned a project to test the security of www.we-are-secure.com. He successfully performs a brute force attack on the We-are-secure server. Now, he suggests some countermeasures to avoid such brute force attacks on the We-aresecure server. Which of the following are countermeasures against a brute force attack? Each correct answer represents a complete solution. Choose all that apply.

A. The site should increase the encryption key length of the password.

B. The site should restrict the number of login attempts to only three times.

C. The site should force its users to change their passwords from time to time.

D. The site should use CAPTCHA after a specific number of failed login attempts.

Correct Answer: BD

QUESTION 11

Which of the following is the second half of the LAN manager Hash?

A. 0xAAD3B435B51404BB

B. 0xAAD3B435B51404CC

C. 0xAAD3B435B51404EE

D. 0xAAD3B435B51404AA

Correct Answer: C

QUESTION 12

You have forgotten your password of an online shop. The web application of that online shop asks you to enter your email so that they can send you a new password. You enter your email you@gmail.com\\' and press the submit button. The

Web application displays the server error.

What can be the reason of the error?

A. The remote server is down.

B. You have entered any special character in email.

C. Your internet connection is slow.

D. Email entered is not valid.

Correct Answer: B

QUESTION 13

Which of the following is a Windows-based tool that is used for the detection of wireless LANs using the IEEE 802.11a, 802.11b, and 802.11g standards and also detects wireless networks marking their relative position with a GPS?

A. Kismet

B. NetStumbler

C. Ettercap

D. Tcpdump

Correct Answer: B

QUESTION 14

Which of the following is a tool for SSH and SSL MITM attacks?

A. Ettercap

B. Cain

C. Dsniff

D. AirJack

Correct Answer: C

QUESTION 15

John works as a professional Ethical Hacker. He has been assigned a project to test the security of www.we-are-secure.com. He performs Web vulnerability scanning on the We-are-secure server. The output of the scanning test is as follows: C:\whisker.pl -h target_IP_address -- whisker / v1.4.0 / rain forest puppy / www.wiretrip.net -- = - = - = - = - = = Host: target_IP_address = Server: Apache/1.3.12 (Win32) ApacheJServ/1.1 mod_ssl/2.6.4 OpenSSL/0.9.5a mod_perl/1.22

+ 200 OK: HEAD /cgi-bin/printenv John recognizes /cgi-bin/printenv vulnerability (\\'Printenv\\' vulnerability) in the We_are_secure server. Which of the following statements about \\'Printenv\\' vulnerability are true? Each correct answer represents a complete solution. Choose all that apply.

A. \\'Printenv\\' vulnerability maintains a log file of user activities on the Website, which may be useful for the attacker.

B. The countermeasure to \\'printenv\\' vulnerability is to remove the CGI script.

C. This vulnerability helps in a cross site scripting attack.

D. With the help of \\'printenv\\' vulnerability, an attacker can input specially crafted links and/or other malicious scripts.

Correct Answer: BCD

[Latest GPEN Dumps](https://www.leads4pass.com/gpen.html) [GPEN VCE Dumps](https://www.leads4pass.com/gpen.html) [GPEN Exam Questions](https://www.leads4pass.com/gpen.html)