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.certbus.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

Which of the following tools can be used to perform Windows password cracking, Windows enumeration, and VoIP session sniffing?

A. L0phtcrack

B. John the Ripper

C. Cain

D. Pass-the-hash toolkit

Correct Answer: C

QUESTION 2

You have received a file named new.com in your email as an attachment. When you execute this file in your laptop, you get the following message:

\\'EICAR-STANDARD-ANTIVIRUS-TEST-FILE!\\'

When you open the file in Notepad, you get the following string:

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

What step will you take as a countermeasure against this attack?

A. Immediately shut down your laptop.

B. Do nothing.

C. Traverse to all of your drives, search new.com files, and delete them.

D. Clean up your laptop with antivirus.

Correct Answer: B

QUESTION 3

A client with 7200 employees in 14 cities (all connected via high speed WAN connections) has suffered a major external security breach via a desktop which cost them more than SI 72.000 and the loss of a high profile client. They ask you to perform a desktop vulnerability assessment to identify everything that needs to be patched. Using Nessus you find tens of thousands of vulnerabilities that need to be patched. In the report you find workstations running several Windows OS versions and service pack levels, anti-virus software from multiple vendors several major browser versions and different versions of Acrobat Reader. Which of the following recommendations should you provide with the report?

A. The client should standardize their desktop software

B. The client should eliminate workstations to reduce workload

C. The client should hire more people to catch up on patches

D. The client should perform monthly vulnerability assessments

Correct Answer: A

Both A and C are costly and time-consuming, but once standardization is achieved, future patch management costs can be controlled. On the other hand, a strategy that relies on the number of people will continue to be costly.

QUESTION 4

Which of the following characters will you use to check whether an application is vulnerable to an SQL injection attack?

A. Single quote (\\')

B. Semi colon (;)

C. Double quote (")

D. Dash (-)

Correct Answer: A

QUESTION 5

Which of the following tools is spyware that makes Windows clients send their passwords as clear text?

A. Pwddump2

B. SMBRelay

C. KrbCrack

D. C2MYAZZ

Correct Answer: D

QUESTION 6

Which of the following best describes a client side exploit?

A. Attack of a client application that retrieves content from the network

B. Attack that escalates user privileged to root or administrator

C. Attack of a service listening on a client system

D. Attack on the physical machine

Correct Answer: A

The correct answer is A. The first command creates a backdoor shell as a service. It is being started on TCP 2222 using cmd.exe. The second command verifies the service is created and its status. Here\\'s why the other answers are incorrect:

B. The first part of the answer is correct in that it creates a backdoor shell as a service. However, it incorrectly states that it is being started on UDP 2222. The command provided specifies the "-p 2222" flag, which indicates a TCP port rather than a UDP port.

C. This answer is incorrect because it misinterprets the purpose of the ncservice. It is not designed to stop any instance of nc.exe. Instead, it creates a backdoor shell as a service, as stated in answer A.

D. This answer has the commands\\' purposes switched. The first command is not verifying the service\\'s status; it is creating the backdoor shell. The second command is incomplete and does not provide enough information to determine its purpose.

QUESTION 7

Which of following tasks can be performed when Nikto Web scanner is using a mutation technique? Each correct answer represents a complete solution. Choose all that apply.

A. Guessing for password file names.

B. Sending mutation payload for Trojan attack.

C. Testing all files with all root directories.

D. Enumerating user names via Apache.

Correct Answer: ACD

QUESTION 8

You work as a Penetration Tester for the Infosec Inc. Your company takes the projects of security auditing. Recently, your company has assigned you a project to test the security of the we-aresecure. com Website. The we-are-secure.com Web server is using Linux operating system. When you port scanned the we-are-secure.com Web server, you got that TCP port 23, 25, and 53 are open. When you tried to telnet to port 23, you got a blank screen in response. When you tried to type the dir, copy, date, del, etc. commands you got only blank spaces or underscores symbols on the screen. What may be the reason of such unwanted situation?

A. The we-are-secure.com server is using honeypot.

B. The we-are-secure.com server is using a TCP wrapper.

C. The telnet service of we-are-secure.com has corrupted.

D. The telnet session is being affected by the stateful inspection firewall.

Correct Answer: B

QUESTION 9

Which of the following tools monitors the radio spectrum for the presence of unauthorized, rogue access points and the use of wireless attack tools?

A. IDS

B. Firewall

C. Snort

D. WIPS

Correct Answer: D

QUESTION 10

Which of the following is an open source Web scanner?

A. Nikto

B. GFI LANguird

C. NetRecon

D. Internet scanner

Correct Answer: A

QUESTION 11

You are conducting a penetration test for a private contractor located in Singapore. The scope extends to all internal hosts controlled by the company, you have gathered necessary hold-harmless and nondisclosure agreements. Which action by your group can incur criminal liability under Chapter 50a, Computer Misuse Act?

A. Exploiting vulnerable web services on internal hosts

B. Attempts at social engineering employees via telephone calls

C. Testing denial-of-service tolerance of the communications provider

D. Cracking password hashes on the corporate domain server

Correct Answer: D

QUESTION 12

Which of the following statements are true about firewalking?

Each correct answer represents a complete solution. Choose all that apply.

A. To use firewalking, the attacker needs the IP address of the last known gateway before the firewall and the IP address of a host located behind the firewall.

B. Firewalking works on the UDP packets.

C. In this technique, an attacker sends a crafted packet with a TTL value that is set to expire one hop past the firewall.

D. A malicious attacker can use firewalking to determine the types of ports/protocols that can bypass the firewall.

Correct Answer: ACD

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. NetStumbler

B. Tcpdump

C. Kismet

D. Ettercap

Correct Answer: A

QUESTION 14

A penetration tester wishes to stop the Windows Firewall process on a remote host running Windows Vista She issues the following commands:

```
C:\Documents and Settings\Owner>net use Z: \\fileserver\shared
/user:Administrator
The command completed successfully.

C:\Documents and Settings\Owner>Z:

Z:\>sc stop MpsSvc
[SC] ControlService FAILED 1062:

The service has been stopped.

Z:\>
```

A check of the remote host indicates that Windows Firewall is still running. Why did the command fail?

A. The kernel prevented the command from being executed.

B. The user does not have the access level needed to stop the firewall.

C. The sc command needs to be passed the IP address of the target.

D. The remote server timed out and did not complete the command.

Correct Answer: C

QUESTION 15

John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He wants to perform a stealth scan to discover open ports and applications running on the We-are-secure server. For this purpose, he wants to initiate scanning with the IP address of any third party. Which of the following scanning techniques will John use to accomplish his task?

A. UDP

B. TCP SYN/ACK

C. IDLE

D. RPC

Correct Answer: C