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.pass2lead.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

Where are Netcat\\'s own network activity messages, such as when a connection occurs, sent?

A. Standard Error

B. Standard input

C. Standard Logfile

D. Standard Output

Correct Answer: A

Reference: http://www.sans.org/security-resources/sec560/netcat_cheat_sheet_v1.pdf

QUESTION 2

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 3

You are using the Nmap Scripting Engine and want detailed output of the script as it runs. Which option do you include in the command string?

A. Nmap --script-output -script-SSH-hostkey.nse 155.65.3.221 -p 22

B. Nmap --script-trace --script-ssh-hostkey.nse 155.65.3.221 -p 22

C. Nmap -script-verbose --scrlpr-ssh-hostkey.nse 155.65.3.221 -p 22

D. Nmap -v --script=ssh-hostkey.nse 155.65.3.221 -p 22

Correct Answer: C

QUESTION 4

In the DNS Zone transfer enumeration, an attacker attempts to retrieve a copy of the entire zone file for a domain from a DNS server. The information provided by the DNS zone can help an attacker gather user names, passwords, and other

valuable information. To attempt a zone transfer, an attacker must be connected to a DNS server that is the authoritative server for that zone. Besides this, an attacker can launch a Denial of Service attack against the zone\\'s DNS servers by

flooding them with a lot of requests. Which of the following tools can an attacker use to perform a DNS zone transfer?

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

A. NSLookup

B. Host

C. DSniff

D. Dig

Correct Answer: ABD

QUESTION 5

Fill in the blank with the appropriate word.

____is a port scanner that can also be used for the OS detection.

A. Nmap

Correct Answer: A

QUESTION 6

Which of the following is the JavaScript variable used to store a cookie?

A. Browsercookie

B. Windowcookie

C. Document cookie

D. Session cookie

Correct Answer: C

Reference: http://www.w3schools.com/js/js_cookies.asp

QUESTION 7

Which of the following Web authentication techniques uses a single sign-on scheme?

A. Basic authentication

B. Digest authentication

C. NTLM authentication

D. Microsoft Passport authentication

Correct Answer: D

QUESTION 8

You are concerned about war driving bringing hackers attention to your wireless network. What is the most basic step you can take to mitigate this risk?

A. Implement WEP

B. Implement WPA

C. Don\\'t broadcast SSID

D. Implement MAC filtering

Correct Answer: C

QUESTION 9

192.168.116.9 Is an IP address for www.scanned-server.com. Why are the results from the two scans, shown below, different?

```
user@desktop:~$ nmap 192.168.116.9

Starting Nmap 4.53 ( http://insecure.org ) at 2010-09-29 20:14 EDT
Interesting ports on 192.168.116.9:
Not shown: 1710 closed ports
PORT STATE SERVICE
80/tcp open http
139/tcp open netbios-ssn
445/tcp open microsoft-ds
8081/tcp open blackice-icecap

user@desktop:~$ nmap www.scanned-server.com
Starting Nmap 4.53 ( http://insecure.org ) at 2010-09-29 20:19 EDT
Interesting ports on 192.168.112.89:
Not shown: 1712 closed ports
PORT STATE SERVICE
80/tcp open http
443/tcp open https
```

A. John.pot

B. John conf

C. John.rec

D. John.ini

Correct Answer: C

QUESTION 10

What is the MOST important document to obtain before beginning any penetration testing?

A. Project plan

B. Exceptions document

C. Project contact list

D. A written statement of permission

Correct Answer: A

Reference:

Before starting a penetration test, all targets must be identified. These targets should be obtained from the customer during the initial questionnaire phase. Targets can be given in the form of specific IP addresses, network ranges, or domain

names by the customer. In some instances, the only target the customer provides is the name of the organization and expects the testers be able to identify the rest on their own. It is important to define if systems like firewalls and IDS/IPS or

networking equipment that are between the tester and the final target are also part of the scope. Additional elements such as upstream providers, and other 3rd party providers should be identified and defined whether they are in scope or not.

QUESTION 11

Fill in the blanks with the appropriate protocol.

CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) is an IEEE___ encryption protocol created to replace both TKIP and WEP.

A. 802.11i

Correct Answer: A

QUESTION 12

Which of the following United States laws protects stored electronic information?

A. Title 18, Section 1029

B. Title 18, Section 1362

C. Title 18, Section 2701

D. Title 18, Section 2510

Correct Answer: D

QUESTION 13

You are concerned about war driving bringing hackers attention to your wireless network. What is the most basic step you can take to mitigate this risk?

A. Implement WEP

B. Implement MAC filtering

C. Don\\'t broadcast SSID

D. Implement WPA

Correct Answer: C

QUESTION 14

Which of the following tools is used for vulnerability scanning and calls Hydra to launch a dictionary attack?

A. Whishker

B. Nmap

C. Nessus

D. SARA

Correct Answer: C

QUESTION 15

You work as a Network Administrator for Tech Perfect Inc. The company has a Windows Active Directory-based single domain single forest network. The functional level of the forest is Windows Server 2003. The company has recently provided laptops to its sales team members. You have configured access points in the network to enable a wireless network. The company\\'s security policy states that all users using laptops must use smart cards for authentication. Which of the following authentication techniques will you use to implement the security policy of the company?

A. IEEE 802.1X using EAP-TLS

B. IEEE 802.1X using PEAP-MS-CHAP

C. Pre-shared key

D. Open system

Correct Answer: A