GPEN Q&As

GIAC Certified Penetration Tester

Pass GIAC GPEN Exam with 100% Guarantee

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

When attempting to crack a password using Rainbow Tables, what is the output of the reduction function?

A. A new potential chain

B. A new potential table

C. A new potential password

D. A new potential hash

Correct Answer: D

Reference: http://en.wikipedia.org/wiki/Rainbow_table

QUESTION 3

Which of the following is NOT a Back orifice plug-in?

A. BOSOCK32

B. STCPIO

C. BOPeep

D. Beast

Correct Answer: D

QUESTION 4

You have gained shell on a Windows host and want to find other machines to pivot to, but the rules of engagement state that you can only use tools that are already available. How could you find other machines on the target network?

A. Use the "ping" utility to automatically discover other hosts

B. Use the "ping" utility in a for loop to sweep the network.

C. Use the "edit" utility to read the target\\'s HOSTS file.

D. Use the "net share" utility to see who is connected to local shared drives.

Correct Answer: B

The correct answer is B. Use the "ping" utility in a for loop to sweep the network.

Here\\'s why the other answers are incorrect:

A. While the "ping" utility can be used to check the connectivity between two hosts, it doesn\\'t automatically discover other hosts. It requires you to input specific IP addresses.

C. The "edit" utility is a text editor, and reading the target\\'s HOSTS file would only provide you with a list of specific hostnames and their corresponding IP addresses that have been manually added to the file. This may not include all the machines on the target network.

D. The "net share" utility displays information about shared resources on a Windows host. Although it can show you who is connected to local shared drives, it does not actively discover other machines on the network. By using a for loop with the "ping" utility, you can systematically test a range of IP addresses on the target network, allowing you to find other machines that respond to the pings.

QUESTION 5

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