Pass2Lead

https://Pass2Lead.com

312-50 Q&As

Ethical Hacker Certified

Pass EC-COUNCIL 312-50 Exam with 100% Guarantee

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

https://www.pass2lead.com/312-50.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

QUESTION 1

What is Hunt used for?

A. Hunt is used to footprint networks

B. Hunt is used to sniff traffic

C. Hunt is used to hack web servers

D. Hunt is used to intercept traffic i.e. man-in-the-middle traffic

E. Hunt is used for password cracking

Correct Answer: D

Hunt can be used to intercept traffic. It is useful with telnet, ftp, and others to grab traffic between two computers or to hijack sessions.

QUESTION 2

How does a denial-of-service attack work?

A. A hacker tries to decipher a password by using a system, which subsequently crashes the network

B. A hacker attempts to imitate a legitimate user by confusing a computer or even another person

C. A hacker prevents a legitimate user (or group of users) from accessing a service

D. A hacker uses every character, word, or letter he or she can think of to defeat authentication

Correct Answer: C

In computer security, a denial-of-service attack (DoS attack) is an attempt to make a computer resource unavailable to its intended users. Typically the targets are high-profile web servers, and the attack attempts to make the hosted web pages unavailable on the Internet. It is a computer crime that violates the Internet proper use policy as indicated by the Internet Architecture Board (IAB).

QUESTION 3

Bill has successfully executed a buffer overflow against a Windows IIS web server. He has been able to spawn an interactive shell and plans to deface the main web page. He first attempts to use the "Echo" command to simply overwrite index.html and remains unsuccessful. He then attempts to delete the page and achieves no progress. Finally, he tries to overwrite it with another page again in vain.

What is the probable cause of Bill\\'s problem?

A. The system is a honeypot.

B. There is a problem with the shell and he needs to run the attack again.

C. You cannot use a buffer overflow to deface a web page.

D. The HTML file has permissions of ready only.

Correct Answer: D

The question states that Bill had been able to spawn an interactive shell. By this statement we can tell that the buffer overflow and its corresponding code was enough to spawn a shell. Any shell should make it possible to change the webpage. So we either don\\'t have sufficient privilege to change the webpage (answer D) or it\\'s a honeypot (answer A). We think the preferred answer is D

QUESTION 4

You have retrieved the raw hash values from a Windows 2000 Domain Controller. Using social engineering, you come to know that they are enforcing strong passwords. You understand that all users are required to use passwords that are at least 8 characters in length. All passwords must also use 3 of the 4 following categories: lower case letters, capital letters, numbers and special characters.

With your existing knowledge of users, likely user account names and the possibility that they will choose the easiest passwords possible, what would be the fastest type of password cracking attack you can run against these hash values and still get results?

A. Online Attack

B. Dictionary Attack

C. Brute Force Attack

D. Hybrid Attack

Correct Answer: D

A dictionary attack will not work as strong passwords are enforced, also the minimum length of 8 characters in the password makes a brute force attack time consuming. A hybrid attack where you take a word from a dictionary and exchange a number of letters with numbers and special characters will probably be the fastest way to crack the passwords.

QUESTION 5

Which Type of scan sends a packets with no flags set ? Select the Answer

A. Open Scan

B. Null Scan

C. Xmas Scan

D. Half-Open Scan

Correct Answer: B

The types of port connections supported are:

Latest 312-50 Dumps   312-50 Practice Test   312-50 Study Guide