312-50Q&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.passapply.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

QUESTION 1

Exhibit:

Based on the following extract from the log of a compromised machine, what is the hacker really trying to steal?

A. har.txt

B. SAM file

C. wwwroot

D. Repair file

Correct Answer: B

He is actually trying to get the file har.txt but this file contains a copy of the SAM file.

QUESTION 2

How would you describe a simple yet very effective mechanism for sending and receiving unauthorized information or data between machines without alerting any firewalls and IDS\\'s on a network?

A. Covert Channel

B. Crafted Channel

C. Bounce Channel

D. Deceptive Channel

Correct Answer: A

A covert channel is described as: "any communication channel that can be exploited by a process to transfer information in a manner that violates the systems security policy." Essentially, it is a method of communication that is not part of an actual computer system design, but can be used to transfer information to users or system processes that normally would not be allowed access to the information.

QUESTION 3

What is the most common vehicle for social engineering attacks?

A. Email

B. Direct in person

C. Local Area Networks

D. Peer to Peer Networks

Correct Answer: B

All social engineering techniques are based on flaws in human logic known as cognitive biases.

QUESTION 4

Which of the following systems would not respond correctly to an nmap XMAS scan?

A. Windows 2000 Server running IIS 5

B. Any Solaris version running SAMBA Server

C. Any version of IRIX

D. RedHat Linux 8.0 running Apache Web Server

Correct Answer: A

When running a XMAS Scan, if a RST packet is received, the port is considered closed, while no response means it is open|filtered. The big downside is that not all systems follow RFC 793 to the letter. A number of systems send RST responses to the probes regardless of whether the port is open or not. This causes all of the ports to be labeled closed. Major operating systems that do this are Microsoft Windows, many Cisco devices, BSDI, and IBM OS/400.

QUESTION 5

Jack Hacker wants to break into company\\'s computers and obtain their secret double fudge cookie recipe. Jacks calls Jane, an accountant at company pretending to be an administrator from company. Jack tells Jane that there has been a problem with some accounts and asks her to verify her password with him "just to double check our records". Jane does not suspect anything amiss, and parts with her password. Jack can now access company\\'s computers with a valid user name and password, to steal the cookie recipe.

What kind of attack is being illustrated here? (Choose the best answer)

A. Reverse Psychology

B. Reverse Engineering

C. Social Engineering

D. Spoofing Identity

E. Faking Identity

Correct Answer: C

This is a typical case of pretexting. Pretexting is the act of creating and using an invented scenario (the pretext) to persuade a target to release information or perform an action and is usually done over the telephone.