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.leads4pass.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

In an attempt to secure his 802.11b wireless network, Ulf decides to use a strategic antenna positioning. He places the antenna for the access points near the center of the building. For those access points near the outer edge of the building he uses semi-directional antennas that face towards the building\\'s center. There is a large parking lot and outlying filed surrounding the building that extends out half a mile around the building. Ulf figures that with this and his placement of antennas, his wireless network will be safe from attack.

Which of the following statements is true?

A. With the 300 feet limit of a wireless signal, Ulf\\'s network is safe.

B. Wireless signals can be detected from miles away, Ulf\\'s network is not safe.

C. Ulf\\'s network will be safe but only of he doesn\\'t switch to 802.11a.

D. Ulf\\'s network will not be safe until he also enables WEP.

Correct Answer: D

QUESTION 2

You are scanning the target network for the first time. You are able to detect few convention open ports. While attempting to perform conventional service identification by connecting to the open ports, the scan yields either bad or no result. As you are unsure of the protocols in use, you want to discover as many different protocols as possible. Which of the following scan options can help you achieve this?

A. Nessus sacn with TCP based pings

B. Netcat scan with the switches

C. Nmap scan with the P (ping scan) switch

D. Nmap with the O (Raw IP Packets switch

Correct Answer: D

-sO IP protocol scans: This method is used to determine which IP protocols are supported on a host. The technique is to send raw IP packets without any further protocol header to each specified protocol on the target machine. If we receive an ICMP protocol unreachable message, then the protocol is not in use. Otherwise we assume it is open. Note that some hosts (AIX, HP-UX, Digital UNIX) and firewalls may not send protocol unreachable messages.

QUESTION 3

Sara is using the nslookup command to craft queries to list all DNS information (such as Name Servers, host names, MX records, CNAME records, glue records (delegation for child Domains), zone serial number, TimeToLive (TTL) records, etc) for a Domain. What do you think Sara is trying to accomplish? Select the best answer.

A. A zone harvesting

B. A zone transfer

C. A zone update

D. A zone estimate

Correct Answer: B

The zone transfer is the method a secondary DNS server uses to update its information from the primary DNS server. DNS servers within a domain are organized using a master-slave method where the slaves get updated DNS information from the master DNS. One should configure the master DNS server to allow zone transfers only from secondary (slave) DNS servers but this is often not implemented. By connecting to a specific DNS server and successfully issuing the ls d domain-name > file-name you have initiated a zone transfer.

QUESTION 4

John is a keen administrator, and has followed all of the best practices as he could find on securing his Windows Server. He has renamed the Administrator account to a new name that he is sure cannot be easily guessed. However, there are people who already attempt to compromise his newly renamed administrator account.

How is it possible for a remote attacker to decipher the name of the administrator account if it has been renamed?

A. The attacker used the user2sid program.

B. The attacker used the sid2user program.

C. The attacker used nmap with the V switch.

D. The attacker guessed the new name.

Correct Answer: B

User2sid.exe can retrieve a SID from the SAM (Security Accounts Manager) from the local or a remote machine Sid2user.exe can then be used to retrieve the names of all the user accounts and more. These utilities do not exploit a bug but call the functions LookupAccountName and LookupAccountSid respectively. What is more these can be called against a remote machine without providing logon credentials save those needed for a null session connection.

QUESTION 5

Kevin is an IT security analyst working for Emerson Time Makers, a watch manufacturing company in Miami. Kevin and his girlfriend Katy recently broke up after a big fight. Kevin believes that she was seeing another person. Kevin, who has an online email account that he uses for most of his mail, knows that Katy has an account with that same company. Kevin logs into his email account online and gets the following URL after successfully logged in: http:// www.youremailhere.com/ mail.asp? mailbox=KevinandSmith=121%22 Kevin changes the URL to: http://www.youremailhere.com/mail.asp? mailbox=KatyandSanchez=121%22 Kevin is trying to access her email account to see if he can find out any information. What is Kevin attempting here to gain access to Katy\\'s mailbox?

A. This type of attempt is called URL obfuscation when someone manually changes a URL to try and gain unauthorized access

B. By changing the mailbox\\'s name in the URL, Kevin is attempting directory transversal

C. Kevin is trying to utilize query string manipulation to gain access to her email account

D. He is attempting a path-string attack to gain access to her mailbox

Correct Answer: C