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.geekcert.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

Bryce the bad boy is purposely sending fragmented ICMP packets to a remote target. The tool size of this ICMP packet once reconstructed is over 65,536 bytes. From the information given, what type of attack is Bryce attempting to perform?

A. Smurf

B. Fraggle

C. SYN Flood

D. Ping of Death

Correct Answer: D

A ping of death (abbreviated "POD") is a type of attack on a computer that involves sending a malformed or otherwise malicious ping to a computer. A ping is normally 64 bytes in size (or 84 bytes when IP header is considered); many computer systems cannot handle a ping larger than the maximum IP packet size, which is 65,535 bytes. Sending a ping of this size can crash the target computer. Traditionally, this bug has been relatively easy to exploit. Generally, sending a 65,536 byte ping packet is illegal according to networking protocol, but a packet of such a size can be sent if it is fragmented; when the target computer reassembles the packet, a buffer overflow can occur, which often causes a system crash.

QUESTION 2

You have successfully brute forced basic authentication configured on a Web Server using Brutus hacking tool. The username/password is "Admin" and "Bettlemani@". You logon to the system using the brute forced password and plant

backdoors and rootkits.

After downloading various sensitive documents from the compromised machine, you proceed to clear the log files to hide your trace..

Which event log located at C:\Windows\system32\config contains the trace of your brute force attempts?

A. AppEvent.Evt

B. SecEvent.Evt

C. SysEvent.Evt

D. WinEvent.Evt

Correct Answer: B

The Security Event log (SecEvent.Evt) will contain all the failed logins against the system.

QUESTION 3

Name two software tools used for OS guessing.(Choose two.

A. Nmap

B. Snadboy

C. Queso

D. UserInfo

E. NetBus

Correct Answer: AC

Nmap and Queso are the two best-known OS guessing programs. OS guessing software has the ability to look at peculiarities in the way that each vendor implements the RFC\\'s. These differences are compared with its database of known OS fingerprints. Then a best guess of the OS is provided to the user.

QUESTION 4

Sandra is conducting a penetration test for ABC.com. She knows that ABC.com is using wireless networking for some of the offices in the building right down the street. Through social engineering she discovers that they are using 802.11g.

Sandra knows that 802.11g uses the same 2.4GHz frequency range as 802.11b. Using NetStumbler and her 802.11b wireless NIC, Sandra drives over to the building to map the wireless networks. However, even though she repositions

herself around the building several times, Sandra is not able to detect a single AP.

What do you think is the reason behind this?

A. Netstumbler does not work against 802.11g.

B. You can only pick up 802.11g signals with 802.11a wireless cards.

C. The access points probably have WEP enabled so they cannot be detected.

D. The access points probably have disabled broadcasting of the SSID so they cannot be detected.

E. 802.11g uses OFDM while 802.11b uses DSSS so despite the same frequency and 802.11b card cannot see an 802.11g signal.

F. Sandra must be doing something wrong, as there is no reason for her to not see the signals.

Correct Answer: D

Netstumbler can not detect networks that do not respond to broadcast requests.

QUESTION 5

A digital signature is simply a message that is encrypted with the public key instead of the private key.

A. True

B. False

Correct Answer: B

Digital signatures enable the recipient of information to verify the authenticity of the information\\'s origin, and also verify that the information is intact. Thus, public key digital signatures provide authentication and data integrity. A digital signature also provides non-repudiation, which means that it prevents the sender from claiming that he or she did not actually send the information. Instead of encrypting information using someone else\\'s public key, you encrypt it with your private key. If the information can be decrypted with your public key, then it must have originated with you.