312-50V7 Q&As

Ethical Hacking and Countermeasures (CEHv7)

Pass EC-COUNCIL 312-50V7 Exam with 100% Guarantee

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

https://www.leads4pass.com/312-50v7.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

If an attacker\\'s computer sends an IPID of 31400 to a zombie (Idle Scanning) computer on an open port, what will be the response?

A. 31400

B. 31402

C. The zombie will not send a response

D. 31401

Correct Answer: B

QUESTION 2

Blane is a security analyst for a law firm. One of the lawyers needs to send out an email to a client but he wants to know if the email is forwarded on to any other recipients. The client is explicitly asked not to re-send the email since that would be a violation of the lawyer\\'s and client\\'s agreement for this particular case. What can Blane use to accomplish this?

A. He can use a split-DNS service to ensure the email is not forwarded on.

B. A service such as HTTrack would accomplish this.

C. Blane could use MetaGoofil tracking tool.

D. Blane can use a service such as ReadNotify tracking tool.

Correct Answer: D

QUESTION 3

NetBIOS over TCP/IP allows files and/or printers to be shared over the network. You are trying to intercept the traffic from a victim machine to a corporate network printer. You are attempting to hijack the printer network connection from your laptop by sniffing the wire. Which port does SMB over TCP/IP use?

A. 443

B. 139

C. 179

D. 445

Correct Answer: D

QUESTION 4

Which of the following is a component of a risk assessment?

A. Physical security

B. Administrative safeguards

C. DMZ

D. Logical interface

Correct Answer: B

QUESTION 5

Michael is a junior security analyst working for the National Security Agency (NSA) working primarily on breaking terrorist encrypted messages. The NSA has a number of methods they use to decipher encrypted messages including Government Access to Keys (GAK) and inside informants. The NSA holds secret backdoor keys to many of the encryption algorithms used on the Internet. The problem for the NSA, and Michael, is that terrorist organizations are starting to use custom-built algorithms or obscure algorithms purchased from corrupt governments. For this reason, Michael and other security analysts like him have been forced to find different methods of deciphering terrorist messages. One method that Michael thought of using was to hide malicious code inside seemingly harmless programs. Michael first monitors sites and bulletin boards used by known terrorists, and then he is able to glean email addresses to some of these suspected terrorists. Michael then inserts a stealth keylogger into a mapping program file readme.txt and then sends that as an attachment to the terrorist. This keylogger takes screenshots every 2 minutes and also logs all keyboard activity into a hidden file on the terrorist\\'s computer. Then, the keylogger emails those files to Michael twice a day with a built in SMTP server. What technique has Michael used to disguise this keylogging software?

A. Steganography

B. Wrapping

C. ADS

D. Hidden Channels

Correct Answer: C