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

Jenny a well known hacker scanning to remote host of 204.4.4.4 using nmap. She got the scanned output but she saw that 25 port states is filtered. What is the meaning of filtered port State?

A. Can Accessible

B. Filtered by firewall

C. Closed

D. None of above

Correct Answer: B

The state is either open, filtered, closed, or unfiltered. Filtered means that a firewall, filter, or other network obstacle is blocking the port so that Nmap cannot tell whether it is open or closed.

QUESTION 2

John is using tokens for the purpose of strong authentication. He is not confident that his security is considerably strong.

In the context of Session hijacking why would you consider this as a false sense of security?

A. The token based security cannot be easily defeated.

B. The connection can be taken over after authentication.

C. A token is not considered strong authentication.

D. Token security is not widely used in the industry.

Correct Answer: B

A token will give you a more secure authentication, but the tokens will not help against attacks that are directed against you after you have been authenticated.

QUESTION 3

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: D

QUESTION 4

Say that "abigcompany.com" had a security vulnerability in the javascript on their website in the past. They recently fixed the security vulnerability, but it had been there for many months. Is there some way to 4go back and see the code for that error? Select the best answer.

A. archive.org

B. There is no way to get the changed webpage unless you contact someone at the company

C. Usenet

D. Javascript would not be in their html so a service like usenet or archive wouldn\\'t help you

Correct Answer: A

Archive.org is a website that periodically archives internet content. They have archives of websites over many years. It could be used to go back and look at the javascript as javascript would be in the HTML code.

QUESTION 5

Which of the following is an attack in which a secret value like a hash is captured and then reused at a later time to gain access to a system without ever decrypting or decoding the hash.

A. Replay Attacks

B. Brute Force Attacks

C. Cryptography Attacks

D. John the Ripper Attacks

Correct Answer: A

A replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an adversary who intercepts the data and retransmits it.