ECSAV10$^{Q\&As}$

EC-Council Certified Security Analyst (ECSA) v10 : Penetration Testing

Pass EC-COUNCIL ECSAV10 Exam with 100% Guarantee

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

https://www.leads4pass.com/ecsav10.html

100% Passing Guarantee
100% Money Back Assurance

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

- Instant Download After Purchase
- 100% Money Back Guarantee
- 365 Days Free Update
- 800,000+ Satisfied Customers

SATISFACTION GUARANTEED 100% SATISFACTION GUARANTEED

QUESTION 1

Sandra, a wireless network auditor, discovered her client is using WEP. To prove the point that the WEP encryption is very weak, she wants to decrypt some WEP packets. She successfully captured the WEP data packets, but could not reach the content as the data is encrypted.

Which of the following will help Sandra decrypt the data packets without knowing the key?

A. Fragmentation Attack

B. Chopchop Attack

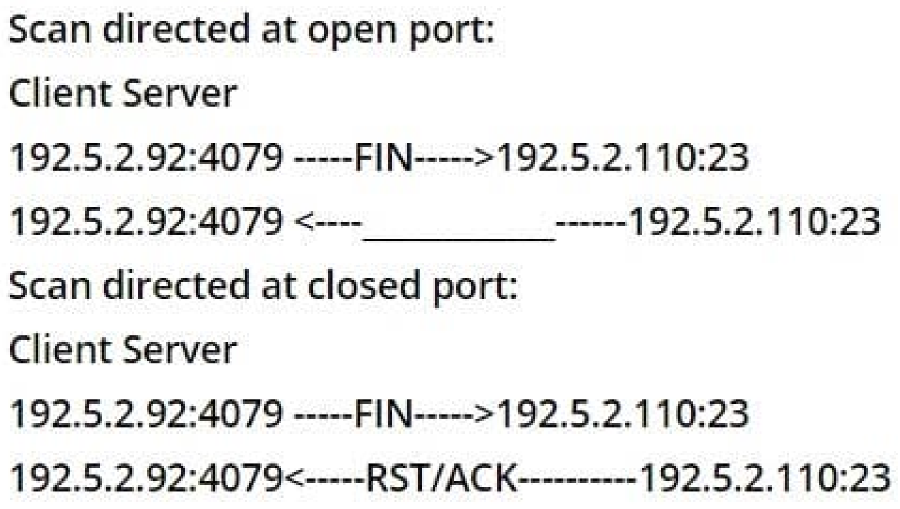
C. ARP Poisoning Attack

D. Packet injection Attack

Correct Answer: B

QUESTION 2

As a part of the pen testing process, James performs a FIN scan as given below:



Scan directed at open port:

Client Server

192.5.2.92:4079 -----FIN----->192.5.2.110:23

192.5.2.92:4079 <----____________------192.5.2.110:23

Scan directed at closed port:

Client Server

192.5.2.92:4079 -----FIN----->192.5.2.110:23

192.5.2.92:4079<-----RST/ACK---------192.5.2.110:23

What will be the response if the port is open?

A. No response

B. FIN/RST

C. FIN/ACK

D. RST

Correct Answer: A

QUESTION 3

Peter works as a lead penetration tester in a security service firm named Xsecurity. Recently, Peter was assigned a white-box pen test assignment testing the security of an IDS system deployed by a client. During the preliminary information gathering, Peter discovered the TTL to reach the IDS system from his end is 30. Peter created a Trojan and fragmented it in to 1-character packets using the Colasoft packet builder tool. He then used a packet flooding utility to bombard the IDS with these fragmented packets with the destination address of a target host behind the IDS whose TTL is 35. What is Peter trying to achieve?

A. Peter is trying to bypass the IDS system using a Trojan

B. Peter is trying to bypass the IDS system using the broadcast address

C. Peter is trying to bypass the IDS system using the insertion attack

D. Peter is trying to bypass the IDS system using inconsistent packets

Correct Answer: D

QUESTION 4

ABC bank, a UK-based bank hired Anthony, to perform a penetration test for the bank. Anthony began performing lookups on the bank\\'s DNS servers, reading news articles online about the bank, performing competitive intelligence gathering, watching what times the bank employees come and go, and searching the bank\\'s job postings. What phase of the penetration testing is Anthony currently in?

A. Attack phase

B. Post-attack phase

C. Pre-attack phase

D. Remediation phase

Correct Answer: C

QUESTION 5

While scanning a server, you found rpc, nfs and mountd services running on it. During the investigation, you were told that NFS Shares were mentioned in the /etc/exports list of the NFS server. Based on this information, which among the following commands would you issue to view the NFS Shares running on the server?

A. showmount

B. nfsenum

C. mount

D. rpcinfo

Correct Answer: A