ECSAV10^Q&As^

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

Pass EC-COUNCIL ECSAV10 Exam with 100% Guarantee

QUESTION 1

Larry is an IT consultant who works for corporations and government agencies. Larry plans on shutting down the city\\'s network using BGP devices and Zombies? What type of Penetration Testing is Larry planning to carry out?

A. Internal Penetration Testing

B. Firewall Penetration Testing

C. DoS Penetration Testing

D. Router Penetration Testing

Correct Answer: C

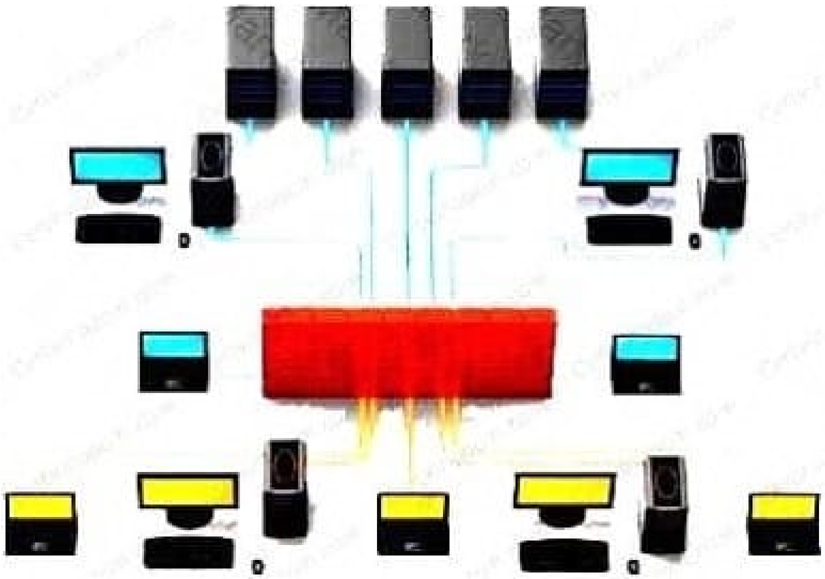
QUESTION 2

Information gathering is performed to:

i) Collect basic information about the target company and its network ii) Determine the operating system

used, platforms running, web server versions, etc.

iii) Find vulnerabilities and exploits



Which of the following pen testing tests yields information about a company\\'s technology infrastructure?

A. Searching for web page posting patterns

B. Analyzing the link popularity of the company\\'s website C. Searching for trade association directories

D. Searching for a company\\'s job postings

Correct Answer: D

QUESTION 3

A Demilitarized Zone (DMZ) is a computer host or small network inserted as a "neutral zone" between a company\\'s private network and the outside public network. Usage of a protocol within a DMZ environment is highly variable based on the specific needs of an organization. Privilege escalation, system is compromised when the code runs under root credentials, and DoS attacks are the basic weakness of which one of the following Protocol?

A. Lightweight Directory Access Protocol (LDAP)

B. Simple Network Management Protocol (SNMP)

C. Telnet

D. Secure Shell (SSH)

Correct Answer: D

QUESTION 4

As a security analyst you setup a false survey website that will require users to create a username and a strong password. You send the link to all the employees of the company. What information will you be able to gather?

A. The employees network usernames and passwords

B. The MAC address of the employees\\' computers

C. The IP address of the employees computers

D. Bank account numbers and the corresponding routing numbers

Correct Answer: C

QUESTION 5

Watson works as a Penetrating test engineer at Neo security services. The company found its wireless network operating in an unusual manner, with signs that a possible cyber attack might have happened. Watson was asked to resolve this problem. Watson starts a wireless penetrating test, with the first step of

discovering wireless networks by war-driving. After several thorough checks, he identifies that there is

some problem with rogue access points and resolves it. Identifying rogue access points involves a series

of steps.

Which of the following arguments is NOT valid when identifying the rogue access points?

A. If a radio media type used by any discovered AP is not present in the authorized list of media types, it is considered as a rogue AP

B. If any new AP which is not present in the authorized list of APs is detected, it would be considered as a rogue AP

C. If the radio channel used by any discovered AP is not present in the authorized list of channels, it is considered as a rogue AP

D. If the MAC of any discovered AP is present in the authorized list of MAC addresses, it would be considered as a rogue AP

Correct Answer: D