

QUESTION 1 OF 5

If you send a SYN to an open port what is the correct response?

Choose only ONE best answer.

☐ A SYN

☐ B ACK

☐ C FIN

☒ D SYN/ACK



This answer is correct.

QUESTION 2 OF 5

Which of the following is the most reliable type of scan?

Choose only ONE best answer.

☐ A SYN

☐ B Passive

☐ C FIN

☒ D Connect



This answer is correct.

QUESTION 3 OF 5

From a port scanning you identified that port 88 is open. What does this tell you?

Choose only ONE best answer.

☐ A The target system uses Telnet

☒ B The target system uses Kerberos authentication



☐ C The target system uses SMB

☐ D The target system uses SNMP

This answer is correct.

QUESTION 4 OF 5

Trying to identify machines on a target network is called?

Choose only ONE best answer.

A Enumeration 

B Scanning

C Checking

D Assessing

This answer is correct.

QUESTION 2 OF 5

Julie has been hired to perform a penetration test on xyz.com. She begins by looking at IP address ranges owned by the company and details of domain name registration. She then goes to news groups and financial websites to see whether any of the company's sensitive information or technical details are online. What is Julie doing?

Choose only ONE best answer.

A Passive Information Gathering 

B Active Information Gathering

C Attack Phase

D Vulnerability Mapping

This answer is correct.