CIW v5 Security Essentials

CIW 1D0-571

Version Demo

Total Demo Questions: 10

Total Premium Questions: 62

QUESTION NO: 1

Which of the following applications can help determine whether a denial-of-service attack is occurring against a network host?

A. The netstat command and a packet sniffer

B. The ps command and a network scanner

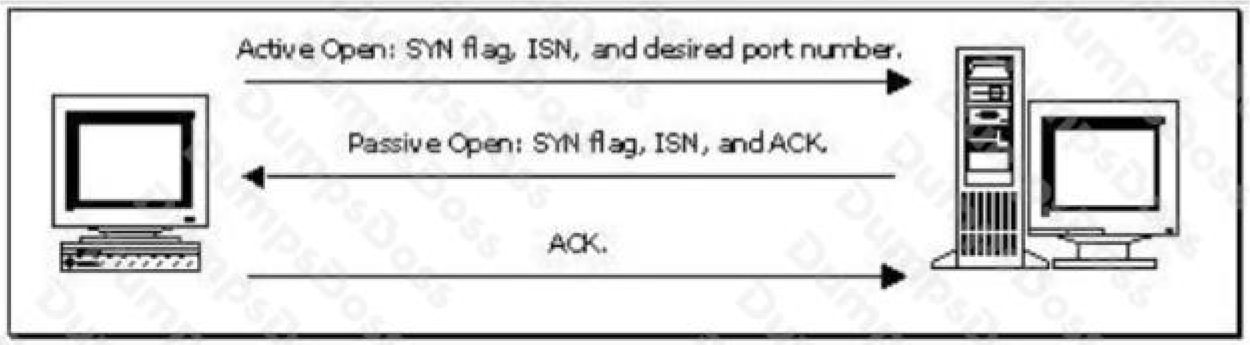
C. The ping command and User Manager

D. The iptables command and Windows desktop firewall

ANSWER: A

QUESTION NO: 2

Consider the following diagram:


Active Open: SYN flag, ISN, and desired port number.
Passive Open: SYN flag, ISN, and ACK.
ACK.

Which of the following best describes the protocol activity shown in the diagram, along with the most likely potential threat that accompanies this protocol?

A. The ICMP Time Exceeded message, with the threat of a denial-of-service attack

B. The SIP three-way handshake, with the threat of a buffer overflow

C. The TCP three-way handshake, with the threat of a man-in-the-middle attack

D. The DNS name query, with the threat of cache poisoning

ANSWER: C

QUESTION NO: 3

A distributed denial-of-service (DDOS) attack has occurred where both ICMP and TCP packets have crashed the company's Web server. Which of the following techniques will best help reduce the severity of this attack?

A. Filtering traffic at the firewall

B. Changing your ISP

C. Installing Apache Server rather than Microsoft IIS

D. Placing the database and the Web server on separate systems

ANSWER: A

QUESTION NO: 4

You are creating an information security policy for your company. Which of the following activities will help you focus on creating policies for the most important resources?

A. Auditing the firewall

B. Implementing non-repudiation

C. Logging users

D. Classifying systems

ANSWER: D

QUESTION NO: 5

Requests for Web-based resources have become unacceptably slow. You have been assigned to implement a solution that helps solve this problem. Which of the following would you recommend?

A. Enable stateful multi-layer inspection on the packet filter

B. Implement caching on the network proxy server

C. Enable authentication on the network proxy server

D. Implement a screening router on the network DMZ

ANSWER: B

QUESTION NO: 6

Which algorithm can use a 128-bit key, and has been adopted as a standard by various governments and corporations?

A. MARS

B. RC2

C. Advanced Encryption Standard (AES)

D. International Data Encryption Algorithm (IDEA)

ANSWER: C

QUESTION NO: 7

Consider the following series of commands from a Linux system: iptables -A input -p icmp -s 0/0 -d 0/0 -j REJECT Which explanation best describes the impact of the resulting firewall ruleset?

A. Individuals on remote networks will no longer be able to use SSH to control internal network resources.

B. Internal hosts will not be able to ping each other using ICMP.

C. Stateful multi-layer inspection has been enabled.

D. Individuals on remote networks will not be able to use ping to troubleshoot connections.

ANSWER: D

QUESTION NO: 8

You have implemented a service on a Linux system that allows a user to read and edit resources. What is the function of this service?

A. Authentication

B. Data integrity

C. Access control

D. Intrusion detection

ANSWER: C

QUESTION NO: 9

Which of the following errors most commonly occurs when responding to a security breach?

A. Shutting down network access using the firewall, rather than the network router

B. Adhering to the company policy rather than determining actions based on the IT manager's input

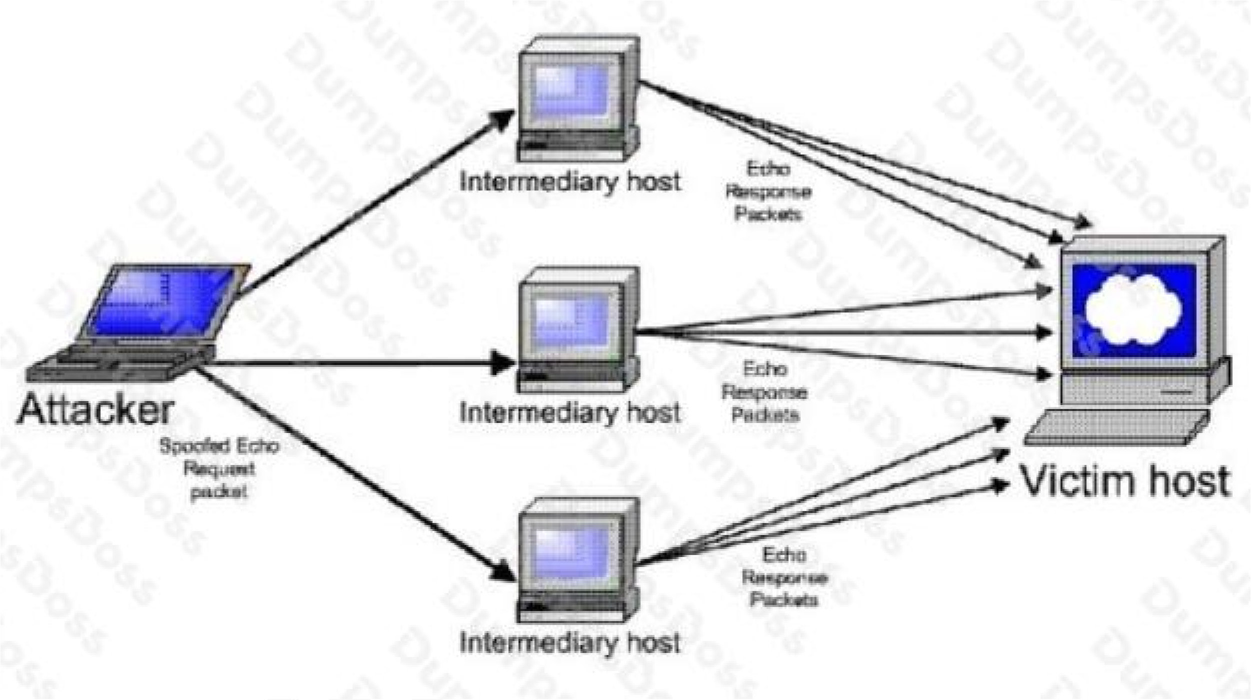
C. Making snap judgments based on emotions, as opposed to company policy

D. Taking too much time to document the attack

ANSWER: C

QUESTION NO: 10

Consider the following diagram:



Which type of attack is occurring?

A. Polymorphic virus-based attack

B. Denial-of-service attack

C. Distributed denial-of-service attack

D. Man-in-the-middle attack using a packet sniffer

ANSWER: C