412-79V8 Q&As

EC-Council Certified Security Analyst (ECSA)

Pass EC-COUNCIL 412-79V8 Exam with 100% Guarantee

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

https://www.geekcert.com/412-79v8.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

James is testing the ability of his routers to withstand DoS attacks. James sends ICMP ECHO requests to the broadcast address of his network. What type of DoS attack is James testing against his network?

A. Smurf

B. Trinoo

C. Fraggle

D. SYN flood

Correct Answer: A

QUESTION 2

You are conducting a penetration test against a company and you would like to know a personal email address of John, a crucial employee. What is the fastest, cheapest way to find out John\\'s email address.

A. Call his wife and ask for his personal email account

B. Call a receptionist and ask for John Stevens\\' personal email account

C. Search in Google for his personal email ID

D. Send an email to John stating that you cannot send him an important spreadsheet attachment file to his business email account and ask him if he has any other email accounts

Correct Answer: D

QUESTION 3

Firewall and DMZ architectures are characterized according to its design. Which one of the following architectures is used when routers have better high-bandwidth data stream handling capacity?

A. Weak Screened Subnet Architecture

B. "Inside Versus Outside" Architecture

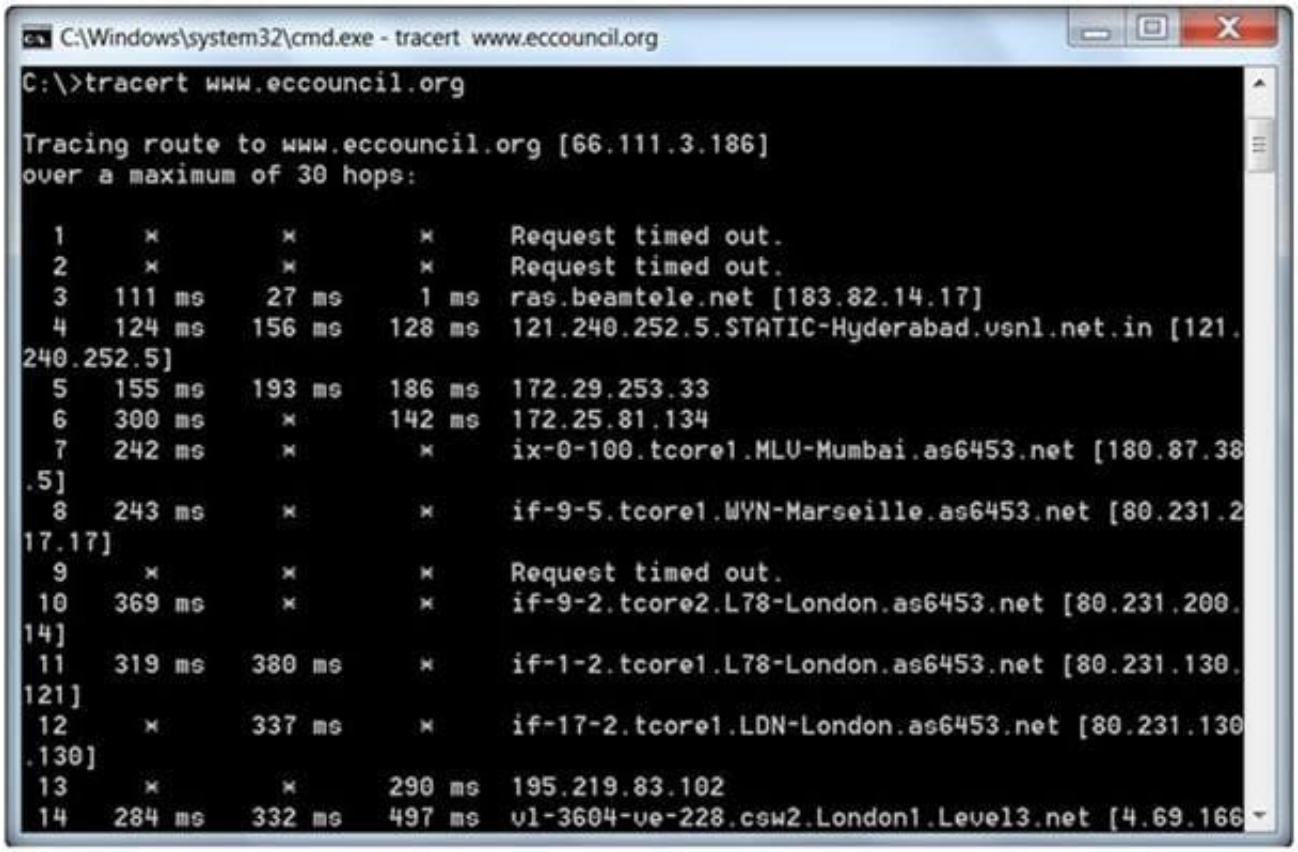
C. "Three-Homed Firewall" DMZ Architecture

D. Strong Screened-Subnet Architecture

Correct Answer: A

QUESTION 4

Traceroute is a computer network diagnostic tool for displaying the route (path) and measuring transit delays of packets across an Internet Protocol (IP) network. It sends a sequence of three Internet Control Message Protocol (ICMP) echo request packets addressed to a destination host. The time-to-live (TTL) value, also known as hop limit, is used in determining the intermediate routers being traversed towards the destination.



During routing, each router reduces packets\\' TTL value by

A. 3

B. 1

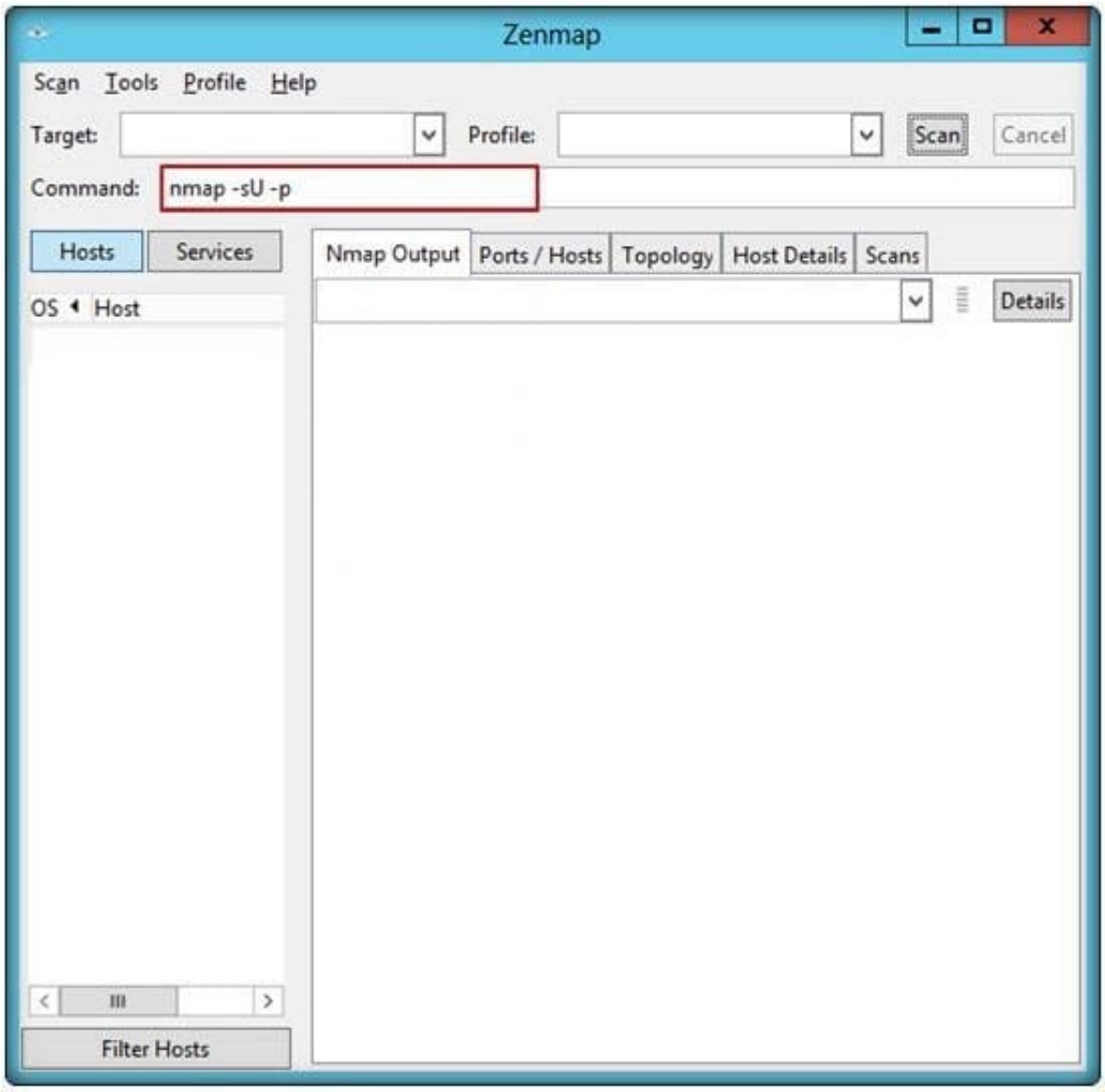
C. 4

D. 2

Correct Answer: B

QUESTION 5

John, the penetration tester in a pen test firm, was asked to find whether NTP services are opened on the target network (10.0.0.7) using Nmap tool.



Which one of the following Nmap commands will he use to find it?

A. nmap -sU p 389 10.0.0.7

B. nmap -sU p 123 10.0.0.7

C. nmap -sU p 161 10.0.0.7

D. nmap -sU p 135 10.0.0.7

Correct Answer: B