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:

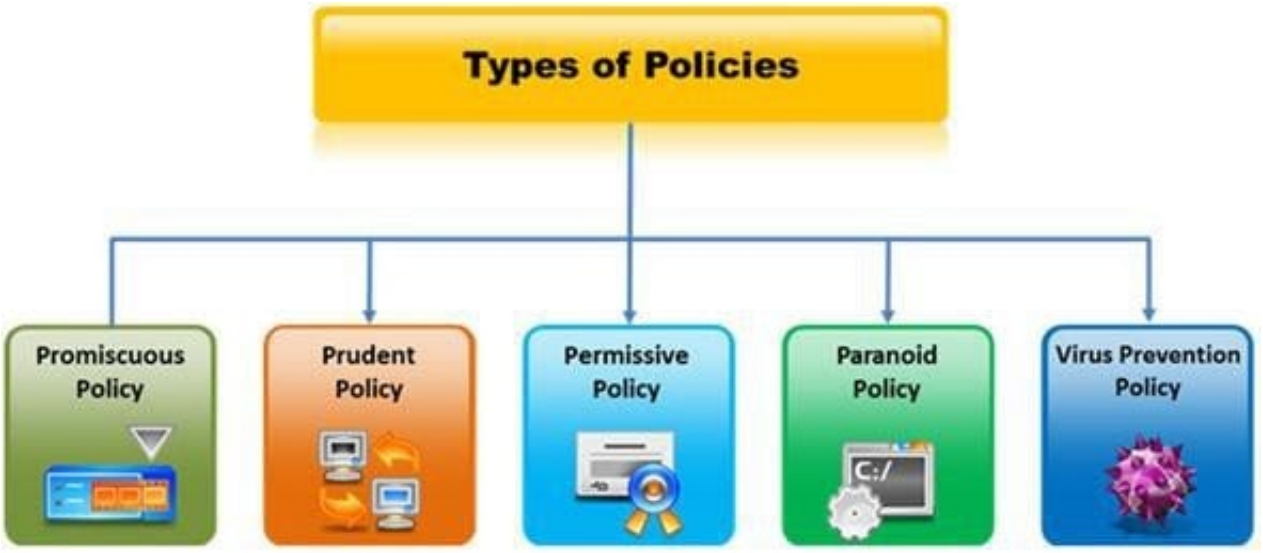
https://www.leads4pass.com/412-79v8.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Which type of security policy applies to the below configuration? i)Provides maximum security while allowing known, but necessary, dangers ii)All services are blocked; nothing is allowed iii)Safe and necessary services are enabled individually iv)Non-essential services and procedures that cannot be made safe are NOT allowed v)Everything is logged



A. Paranoid Policy

B. Prudent Policy

C. Permissive Policy

D. Promiscuous Policy

Correct Answer: B

QUESTION 2

Which of the following is NOT generally included in a quote for penetration testing services?

A. Type of testing carried out

B. Type of testers involved

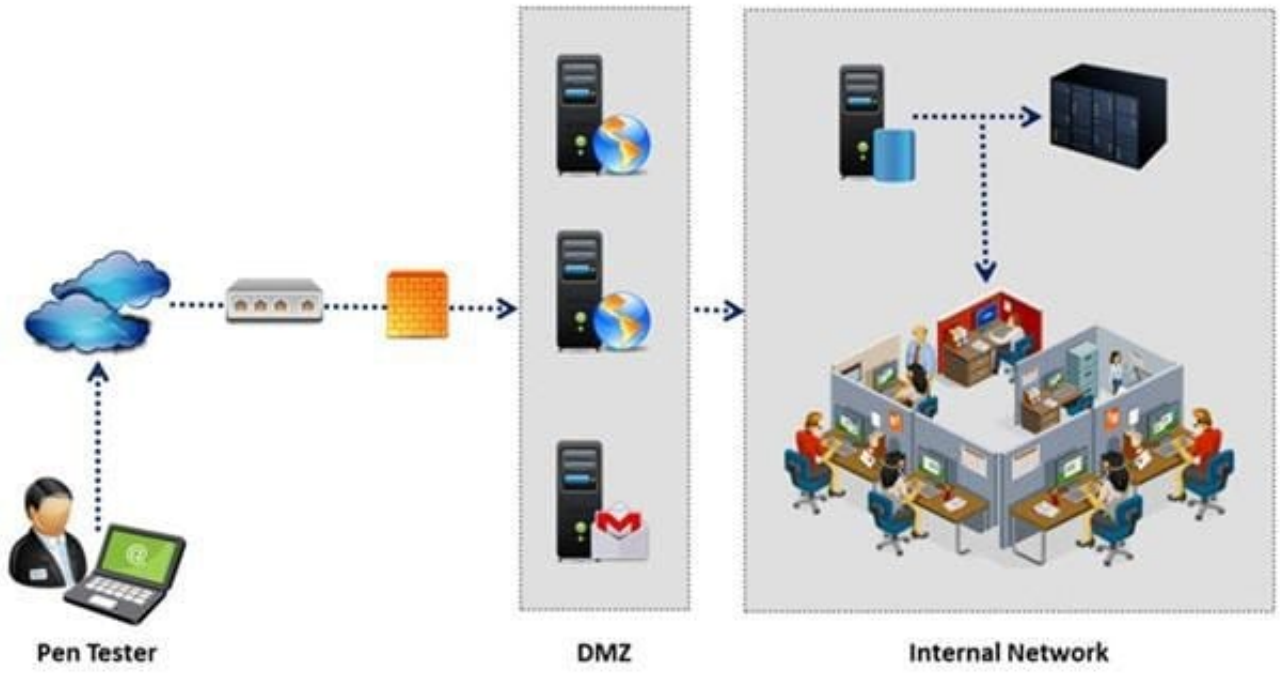
C. Budget required

D. Expected timescale required to finish the project

Correct Answer: B

QUESTION 3

An external intrusion test and analysis identify security weaknesses and strengths of the client\\'s systems and networks as they appear from outside the client\\'s security perimeter, usually from the Internet. The goal of an external intrusion test and analysis is to demonstrate the existence of known vulnerabilities that could be exploited by an external attacker.



During external penetration testing, which of the following scanning techniques allow you to determine a port\\'s state without making a full connection to the host?

A. XMAS Scan

B. SYN scan

C. FIN Scan

D. NULL Scan

Correct Answer: B

QUESTION 4

Which of the following is the range for assigned ports managed by the Internet Assigned Numbers Authority (IANA)?

A. 3001-3100

B. 5000-5099

C. 6666-6674

D. 0 1023

Correct Answer: D

QUESTION 5

Which of the following acts is a proprietary information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards and applies to all entities involved in payment card processing?

A. PIPEDA

B. PCI DSS

C. Human Rights Act 1998

D. Data Protection Act 1998

Correct Answer: B

QUESTION 6

Which of the following is an application alert returned by a web application that helps an attacker guess a valid username?

A. Invalid username or password

B. Account username was not found

C. Incorrect password

D. Username or password incorrect

Correct Answer: C

QUESTION 7

Which of the following protocol\\'s traffic is captured by using the filter tcp.port==3389 in the Wireshark tool?

A. Reverse Gossip Transport Protocol (RGTP)

B. Real-time Transport Protocol (RTP)

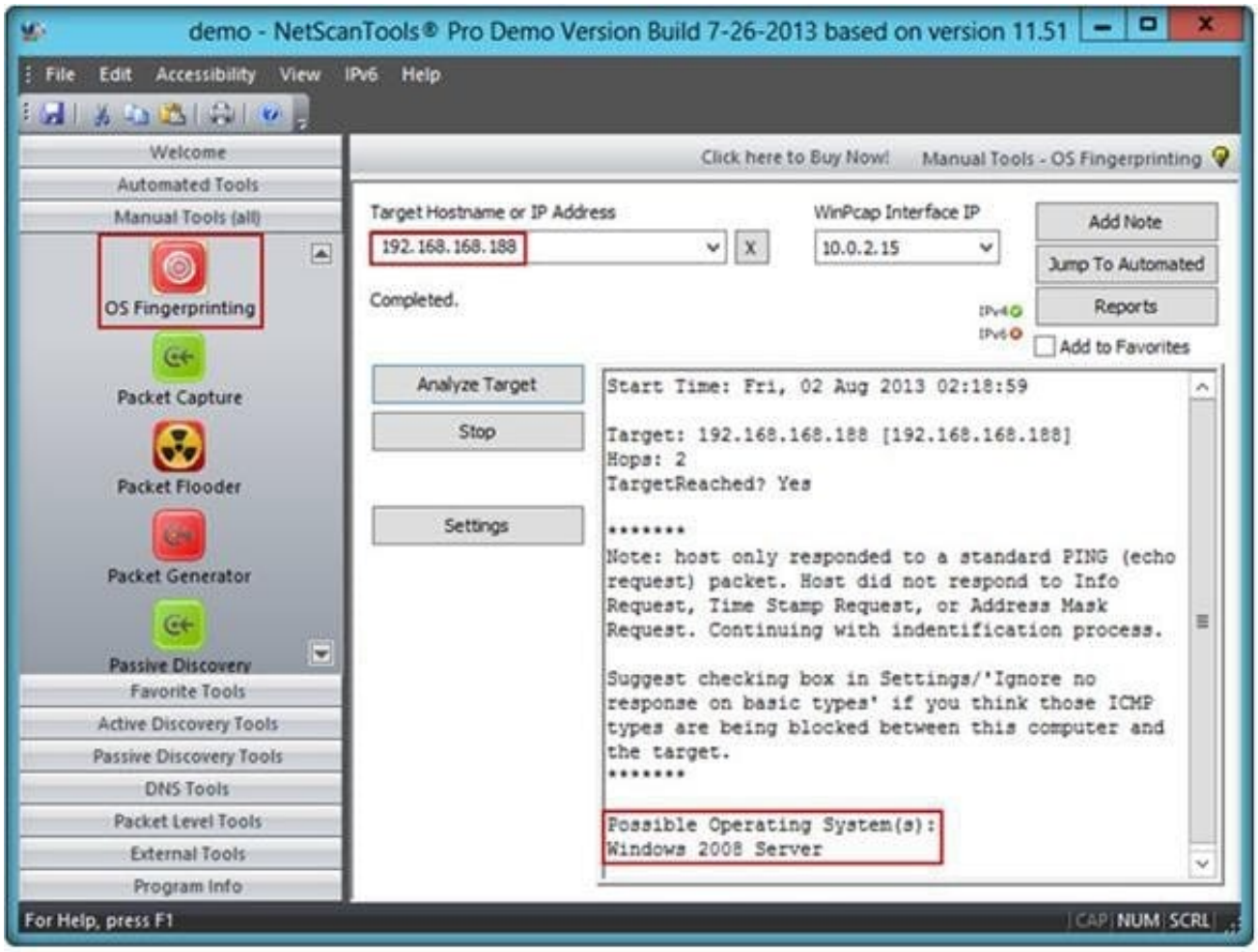
C. Remote Desktop Protocol (RDP)

D. Session Initiation Protocol (SIP)

Correct Answer: C

QUESTION 8

A penetration tester performs OS fingerprinting on the target server to identify the operating system used on the target server with the help of ICMP packets.



While performing ICMP scanning using Nmap tool, message received/type displays "3 Destination

Unreachable[5]" and code 3.

Which of the following is an appropriate description of this response?

A. Destination port unreachable

B. Destination host unavailable

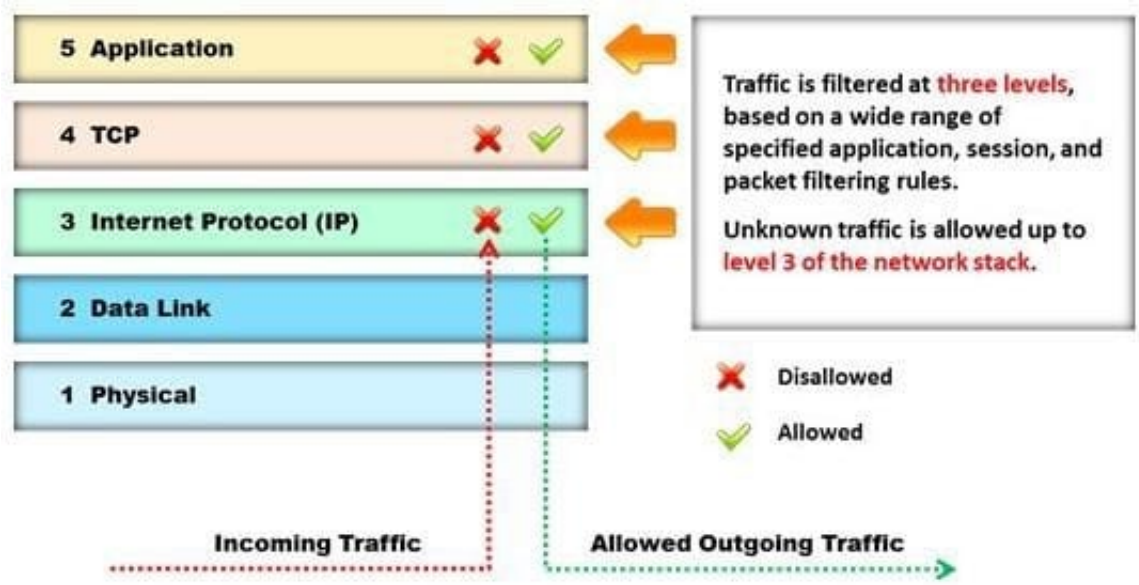
C. Destination host unreachable

D. Destination protocol unreachable

Correct Answer: A

QUESTION 9

Identify the type of firewall represented in the diagram below: A. Stateful multilayer inspection firewall



B. Application level gateway

C. Packet filter

D. Circuit level gateway

Correct Answer: B

QUESTION 10

What threat categories should you use to prioritize vulnerabilities detected in the pen testing report?

A. 1, 2, 3, 4, 5

B. Low, medium, high, serious, critical

C. Urgent, dispute, action, zero, low

D. A, b, c, d, e

Correct Answer: B

QUESTION 11

Amazon, an IT based company, conducts a survey on the usage of the Internet. They found that company employees spend most of the time at work surfing the web for their personal use and for inappropriate web site viewing. Management decide to block all such web sites using URL filtering software.

How can employees continue to see the blocked websites?

A. Using session hijacking

B. Using proxy servers

C. Using authentication

D. Using encryption

Correct Answer: B

QUESTION 12

Transmission Control Protocol (TCP) is a connection-oriented four layer protocol. It is responsible for breaking messages into segments, re-assembling them at the destination station, and re-sending. Which one of the following protocols does not use the TCP?

A. Reverse Address Resolution Protocol (RARP)

B. HTTP (Hypertext Transfer Protocol)

C. SMTP (Simple Mail Transfer Protocol)

D. Telnet

Correct Answer: A

QUESTION 13

Which of the following policy forbids everything with strict restrictions on all usage of the company systems and network?

A. Information-Protection Policy

B. Paranoid Policy

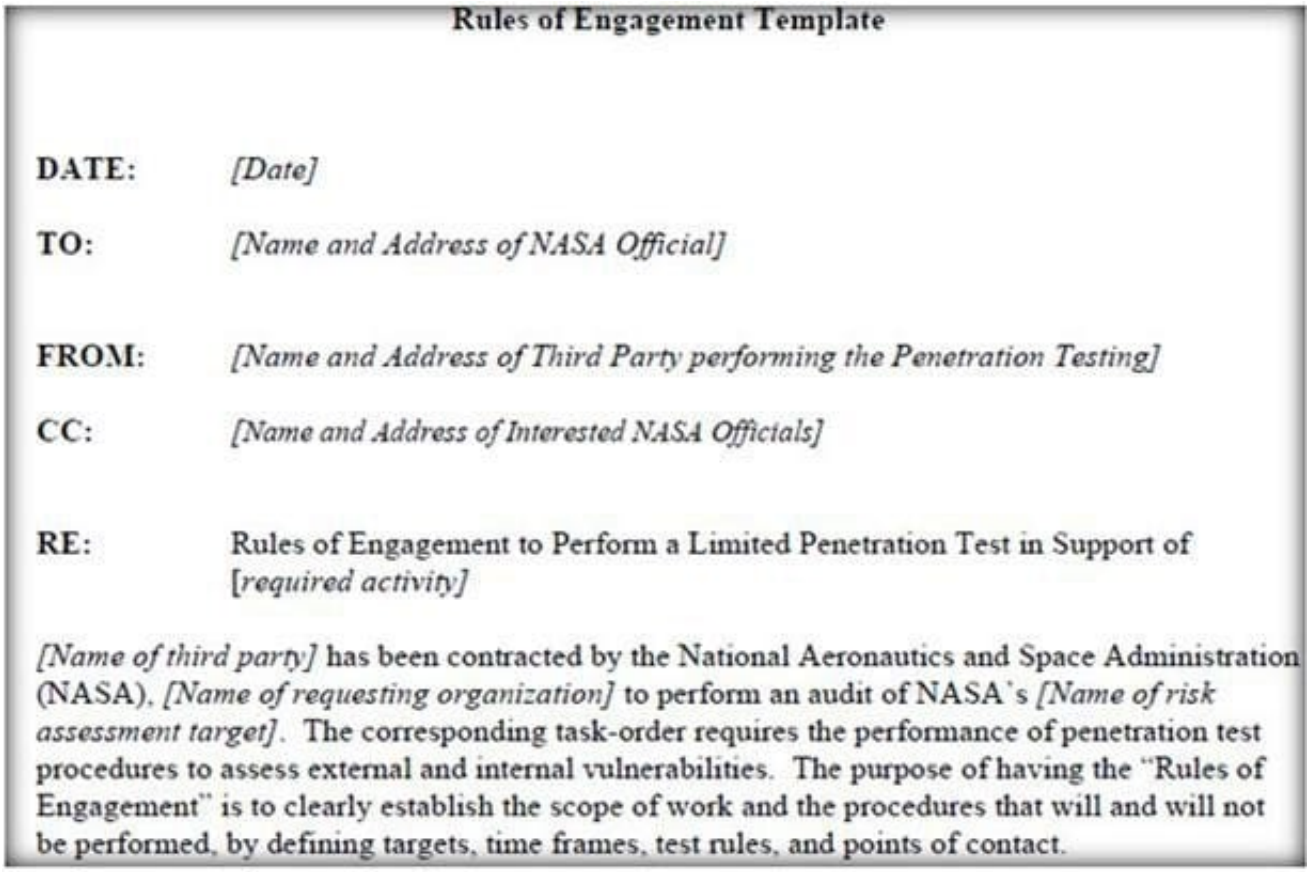
C. Promiscuous Policy

D. Prudent Policy

Correct Answer: B

QUESTION 14

Rules of Engagement (ROE) document provides certain rights and restriction to the test team for performing the test and helps testers to overcome legal, federal, and policy-related restrictions to use different penetration testing tools and techniques.



Rules of Engagement Template

DATE: *[Date]*

TO: *[Name and Address of NASA Official]*

FROM: *[Name and Address of Third Party performing the Penetration Testing]*

CC: *[Name and Address of Interested NASA Officials]*

RE: Rules of Engagement to Perform a Limited Penetration Test in Support of *[required activity]*

[Name of third party] has been contracted by the National Aeronautics and Space Administration (NASA). *[Name of requesting organization]* to perform an audit of NASA's *[Name of risk assessment target]*. The corresponding task-order requires the performance of penetration test procedures to assess external and internal vulnerabilities. The purpose of having the "Rules of Engagement" is to clearly establish the scope of work and the procedures that will and will not be performed, by defining targets, time frames, test rules, and points of contact.

What is the last step in preparing a Rules of Engagement (ROE) document?

A. Conduct a brainstorming session with top management and technical teams

B. Decide the desired depth for penetration testing

C. Conduct a brainstorming session with top management and technical teams

D. Have pre-contract discussions with different pen-testers

Correct Answer: B

QUESTION 15

Phishing is typically carried out by email spoofing or instant messaging and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Phishing is an example of social engineering techniques used to deceive users, and exploits the poor usability of current web security technologies. Attempts to deal with the growing number of reported phishing incidents include legislation, user training, public awareness, and

technical security measures.

What characteristics do phishing messages often have that may make them identifiable?

A. Invalid email signatures or contact information B. Suspiciously good grammar and capitalization

C. They trigger warning pop-ups

D. Suspicious attachments

Correct Answer: D