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.certbus.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 of the following contents of a pen testing project plan addresses the strengths, weaknesses, opportunities, and threats involved in the project?

A. Project Goal

B. Success Factors

C. Objectives

D. Assumptions

Correct Answer: B

QUESTION 2

Before performing the penetration testing, there will be a pre-contract discussion with different pen-testers (the team of penetration testers) to gather a quotation to perform pen testing.

Which of the following factors is NOT considered while preparing a price quote to perform pen testing?

A. Total number of employees in the client organization

B. Type of testers involved

C. The budget required

D. Expected time required to finish the project

Correct Answer: A

QUESTION 3

In which of the following IDS evasion techniques does IDS reject the packets that an end system accepts?

A. IPS evasion technique

B. IDS evasion technique

C. UDP evasion technique

D. TTL evasion technique

Correct Answer: D

QUESTION 4

Which one of the following Snort logger mode commands is associated to run a binary log file through Snort in sniffer mode to dump the packets to the screen?

A. ./snort -dvr packet.log icmp

B. ./snort -dev -l ./log

C. ./snort -dv -r packet.log

D. ./snort -l ./log b

Correct Answer: C

QUESTION 5

Logs are the record of the system and network activities. Syslog protocol is used for delivering log information across an IP network. Syslog messages can be sent via which one of the following?

A. UDP and TCP

B. TCP and SMTP

C. SMTP

D. UDP and SMTP

Correct Answer: A

QUESTION 6

DNS information records provide important data about:

A. Phone and Fax Numbers

B. Location and Type of Servers

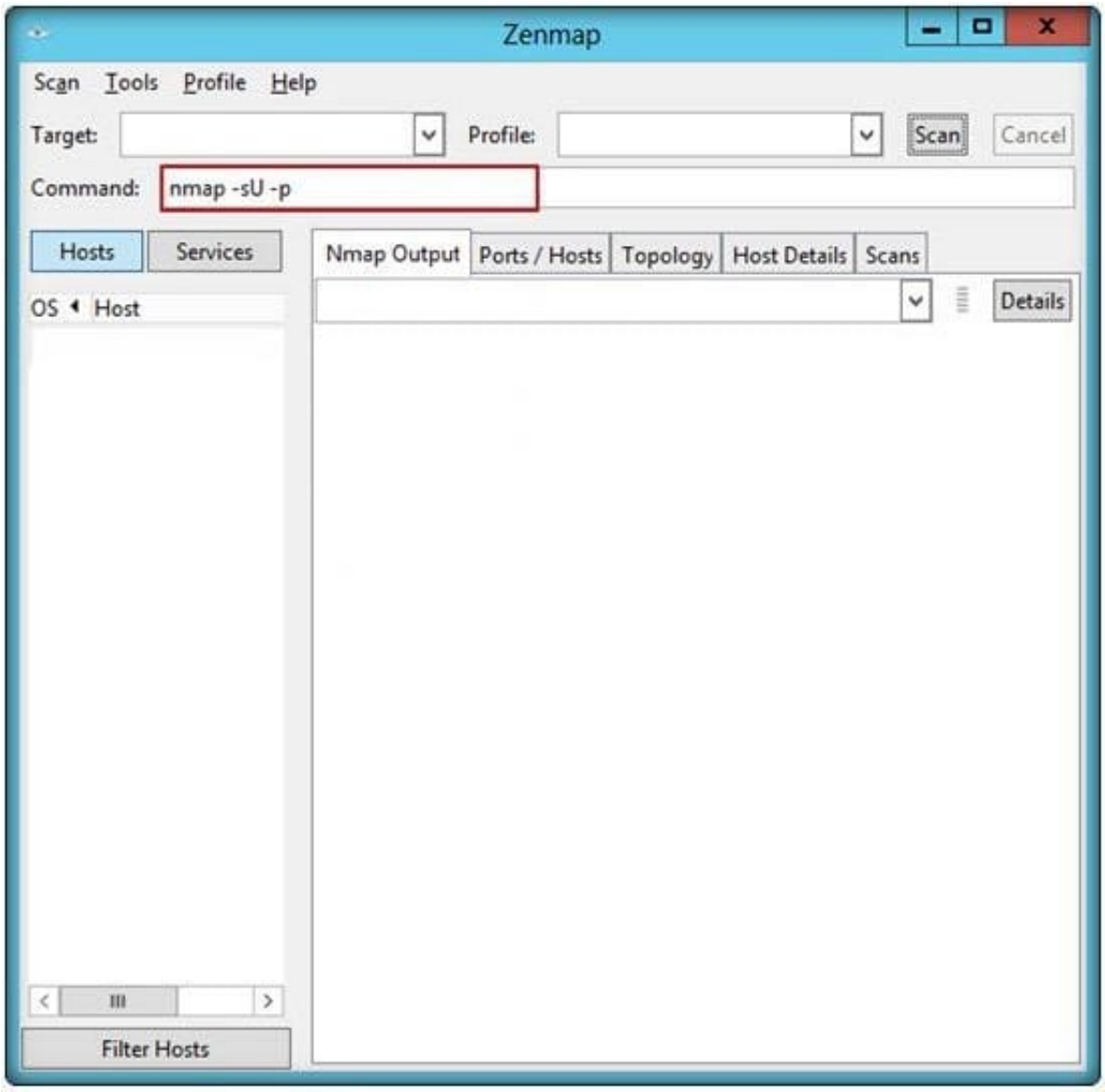
C. Agents Providing Service to Company Staff

D. New Customer

Correct Answer: B

QUESTION 7

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

QUESTION 8

A chipset is a group of integrated circuits that are designed to work together and are usually marketed as a single product." It is generally the motherboard chips or the chips used on the expansion card. Which one of the following is well supported in most wireless applications?

A. Orinoco chipsets

B. Prism II chipsets

C. Atheros Chipset

D. Cisco chipset

Correct Answer: B

QUESTION 9

John, a penetration tester, was asked for a document that defines the project, specifies goals, objectives, deadlines, the resources required, and the approach of the project. Which of the following includes all of these requirements?

A. Penetration testing project plan

B. Penetration testing software project management plan

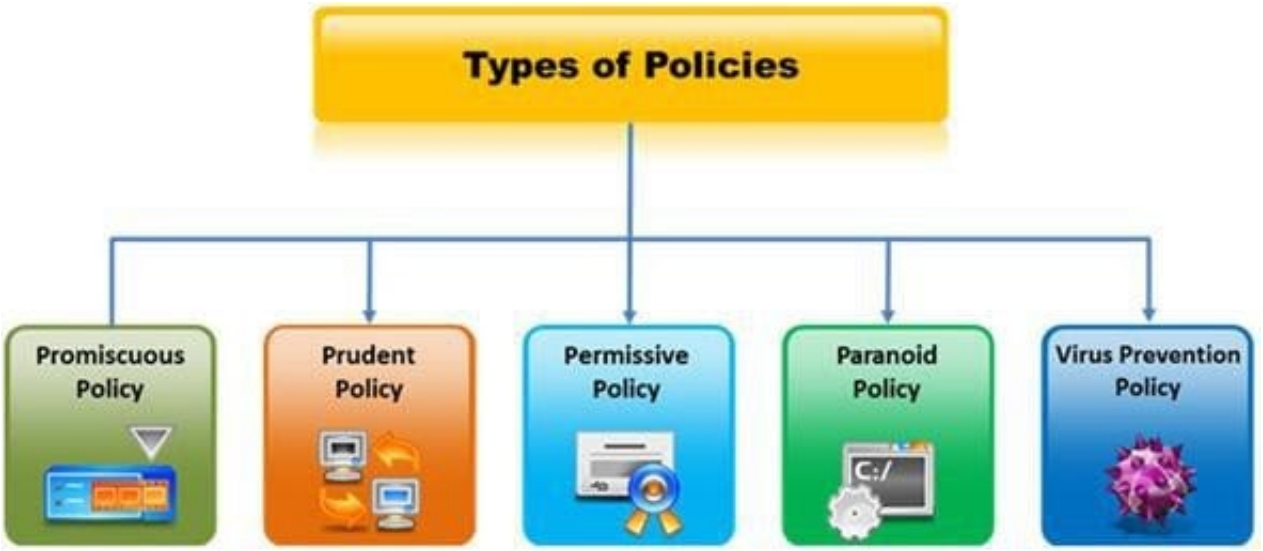
C. Penetration testing project scope report

D. Penetration testing schedule plan

Correct Answer: A

QUESTION 10

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 11

Which of the following defines the details of services to be provided for the client\\'s organization and the list of services required for performing the test in the organization?

A. Draft

B. Report

C. Requirement list

D. Quotation

Correct Answer: D

QUESTION 12

Which of the following is an ARP cache poisoning technique aimed at network switches?

A. Replay Attack

B. Mac Flooding

C. Man-in-the Middle Attack

D. DNS Poisoning

Correct Answer: B

QUESTION 13

Identify the injection attack represented in the diagram below:

A. XPath Injection Attack

B. XML Request Attack

C. XML Injection Attack

D. Frame Injection Attack

Correct Answer: C

QUESTION 14

Which of the following external pen testing tests reveals information on price, usernames and passwords, sessions, URL characters, special instructors, encryption used, and web page behaviors?

A. Check for Directory Consistency and Page Naming Syntax of the Web Pages

B. Examine Server Side Includes (SSI)

C. Examine Hidden Fields

D. Examine E-commerce and Payment Gateways Handled by the Web Server

Correct Answer: C

QUESTION 15

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