412-79V10^Q&As

EC-Council Certified Security Analyst (ECSA) V10

Pass EC-COUNCIL 412-79V10 Exam with 100% Guarantee

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

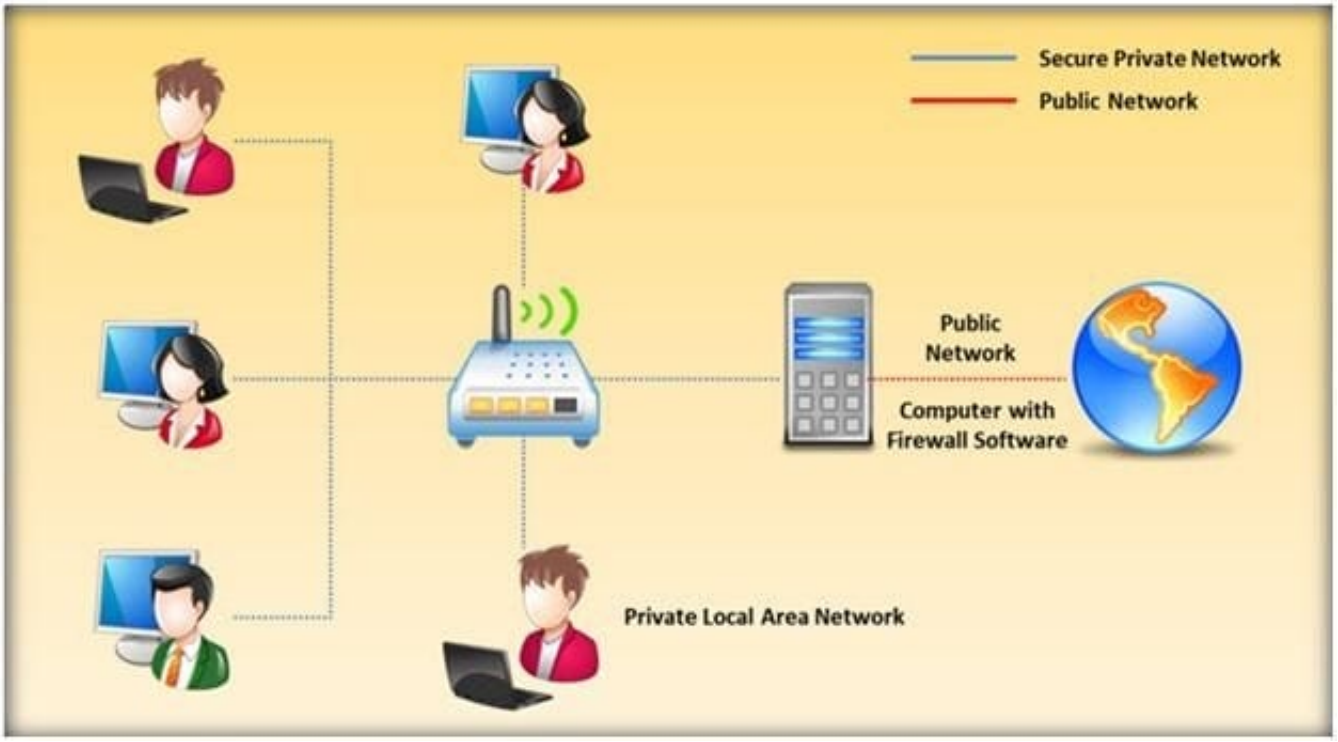
https://www.certbus.com/412-79v10.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Packet filtering firewalls are usually a part of a router. In a packet filtering firewall, each packet is compared to a set of criteria before it is forwarded. Depending on the packet and the criteria, the firewall can: i)Drop the packet ii)Forward it or send a message to the originator



At which level of the OSI model do the packet filtering firewalls work?

A. Application layer

B. Physical layer

C. Transport layer

D. Network layer

Correct Answer: D

Reference:

http://books.google.com.pk/books?id=KPjLAyA7HgoCandpg=PA208andlpg=PA208anddq=At+whi ch+level+of

+the+OSI+model+do+the+packet+filtering+firewalls+workandsource=blandots=zRrb cmY3pjandsig=I3vuS3VA7r3VF8lC 6xq_c_r31Mandhl=enandsa=Xandei=wMcfVMetI8HPaNSRgPgDandved=0CC8Q6AEwAg#v

=onepageandq=At%20which%20level%20of%20the%20OSI%20model%20do%20the%20pa cket%

20filtering%20firewalls%20workandf=false (packet filters)

QUESTION 2

A penetration test consists of three phases: pre-attack phase, attack phase, and post- attack phase.

Active reconnaissance which includes activities such as network mapping, web profiling, and perimeter mapping is a part which phase(s)?

A. Post-attack phase

B. Pre-attack phase and attack phase

C. Attack phase

D. Pre-attack phase

Correct Answer: D

Reference: https://www.duo.uio.no/bitstream/handle/10852/34904/Shrestha- masterthesis.pdf? sequence=1 (page 28, first para)

QUESTION 3

Which of the following will not handle routing protocols properly?

A. "Internet-router-firewall-net architecture"

B. "Internet-firewall-router-net architecture"

C. "Internet-firewall -net architecture"

D. "Internet-firewall/router(edge device)-net architecture"

Correct Answer: B

QUESTION 4

Which of the following shields Internet users from artificial DNS data, such as a deceptive or mischievous address instead of the genuine address that was requested?

A. DNSSEC

B. Firewall

C. Packet filtering

D. IPSec

Correct Answer: A

Reference: http://tools.ietf.org/html/draft-osterweil-dane-ipsec-01 (abstract, first para)

QUESTION 5

Which of the following policies helps secure data and protects the privacy of organizational information?

A. Special-Access Policy

B. Document retention Policy

C. Cryptography Policy

D. Personal Security Policy

Correct Answer: C

QUESTION 6

Identify the policy that defines the standards for the organizational network connectivity and security standards for computers that are connected in the organizational network.

A. Information-Protection Policy

B. Special-Access Policy

C. Remote-Access Policy

D. Acceptable-Use Policy

Correct Answer: C

QUESTION 7

Which one of the following architectures has the drawback of internally considering the hosted services individually?

A. Weak Screened Subnet Architecture

B. "Inside Versus Outside" Architecture

C. "Three-Homed Firewall" DMZ Architecture

D. Strong Screened-Subnet Architecture

Correct Answer: C

QUESTION 8

Which of the following pen testing reports provides detailed information about all the tasks performed during penetration testing?

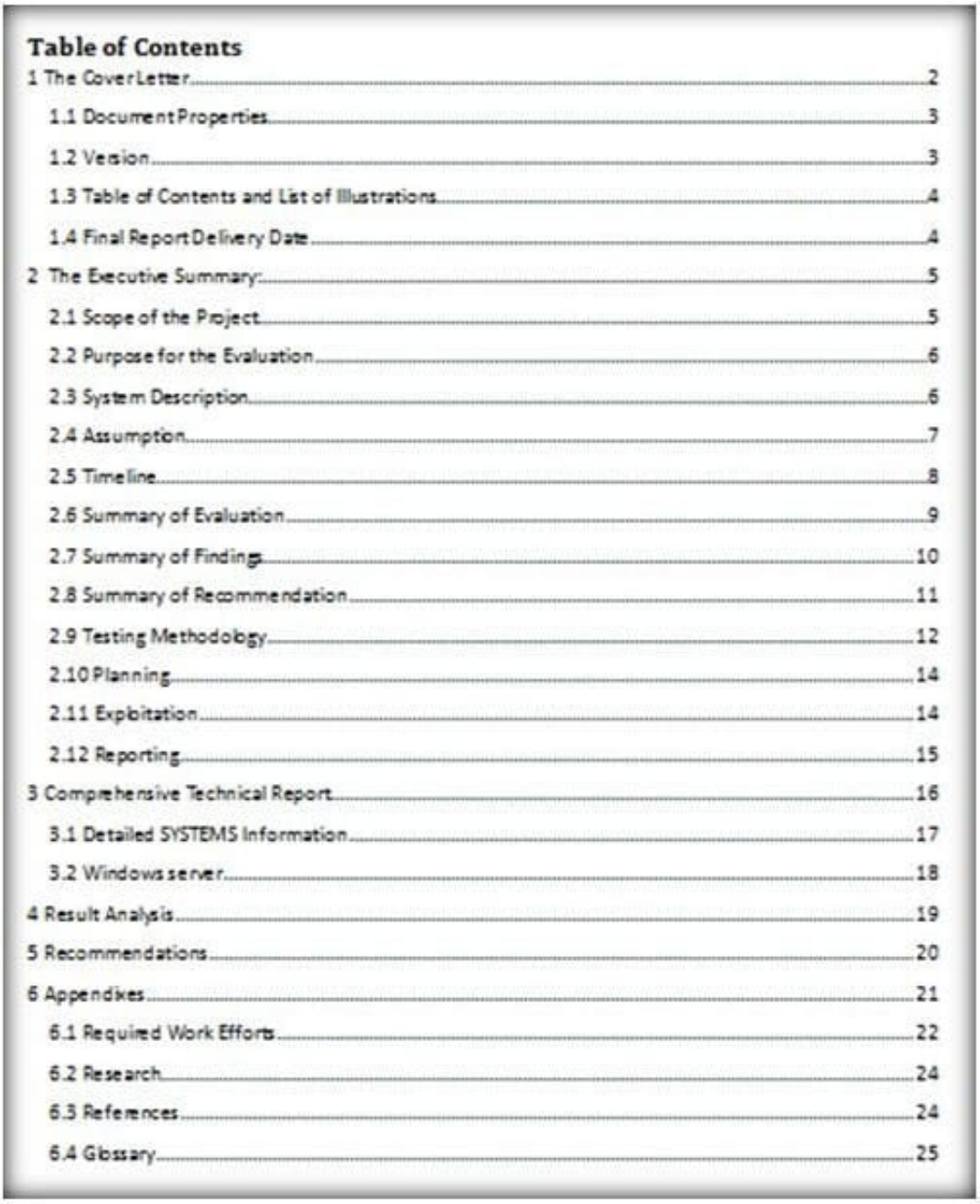


Table of Contents

A. Client-Side Test Report

B. Activity Report

C. Host Report

D. Vulnerability Report

Correct Answer: A

QUESTION 9

A pen tester has extracted a database name by using a blind SQL injection. Now he begins to test the table inside the

database using the below query and finds the table:

http://juggyboy.com/page.aspx?id=1; IF (LEN(SELECT TOP 1 NAME from sysobjects where xtype=\\'U\\')=3) WAITFOR DELAY \\'00:00:10\\'-

http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 NAME from sysobjects where xtype=char(85)),1,1)))=101) WAITFOR DELAY \\'00:00:10\\'-

http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 NAME from sysobjects where xtype=char(85)),2,1)))=109) WAITFOR DELAY \\'00:00:10\\'-

http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 NAME from sysobjects where xtype=char(85)),3,1)))=112) WAITFOR DELAY \\'00:00:10\\'-

What is the table name?

A. CTS

B. QRT

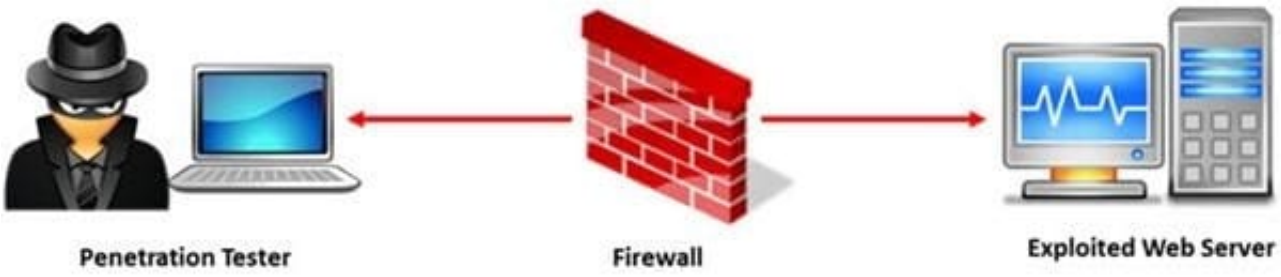
C. EMP

D. ABC

Correct Answer: C

QUESTION 10

A penetration test will show you the vulnerabilities in the target system and the risks associated with it. An educated valuation of the risk will be performed so that the vulnerabilities can be reported as High/ Medium/Low risk issues.



What are the two types of `white-box\\' penetration testing?

A. Announced testing and blind testing

B. Blind testing and double blind testing

C. Blind testing and unannounced testing

D. Announced testing and unannounced testing

Correct Answer: D

QUESTION 11

Snort, an open source network-based intrusion detection sensor, is the most widely installed NIDS in the world. It can be configured to run in the four modes. Which one of the following modes reads the packets off the network and displays them in a continuous stream on the console (screen)?

A. Packet Sniffer Mode

B. Packet Logger Mode

C. Network Intrusion Detection System Mode

D. Inline Mode

Correct Answer: A

QUESTION 12

In the process of hacking a web application, attackers manipulate the HTTP requests to subvert the application authorization schemes by modifying input fields that relate to the user ID, username, access group, cost, file names, file identifiers, etc. They first access the web application using a low privileged account and then escalate privileges to access protected resources. What attack has been carried out?

A. XPath Injection Attack

B. Authorization Attack

C. Authentication Attack

D. Frame Injection Attack

Correct Answer: B

Reference: http://luizfirmino.blogspot.com/2011_09_01_archive.html (see authorization attack)

QUESTION 13

Wireshark is a network analyzer. It reads packets from the network, decodes them, and presents them in an easy-to-understand format. Which one of the following is the command-line version of Wireshark, which can be used to capture the live packets from the wire or to read the saved capture files?

A. Tcpdump

B. Capinfos

C. Tshark

D. Idl2wrs

Correct Answer: B

QUESTION 14

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: D

QUESTION 15

Identify the attack represented in the diagram below:

A. Input Validation

B. Session Hijacking

C. SQL Injection

D. Denial-of-Service

Correct Answer: B

Reference: http://en.wikipedia.org/wiki/Session_hijacking