Fast2Test
FIRST TEST, FIRST PASS!

Fast2Test

We're not the only ones **happy** about Fast2test Practice Materials ...

62316+ customers in 100+ countries use Fast2test Self Test Engine. Meet our customers.

https://www.fast2test.com

Everything you need to prepare, learn & pass your certification exam easily.

Exam : **ECSAv10**

Title : EC-Council Certified Security Analyst (ECSA) v10 : Penetration Testing

Vendor : ECCouncil

Version : DEMO

NO.1 Which of the following is NOT related to the Internal Security Assessment penetration testing strategy?

A. Testing performed from a number of network access points representing each logical and physical segment

B. Testing to provide a more complete view of site security

C. Testing focused on the servers, infrastructure, and the underlying software, including the target

D. Testing including tiers and DMZs within the environment, the corporate network, or partner company connections

Answer: C

NO.2 Simon is a former employee of Trinitron XML Inc. He feels he was wrongly terminated and wants to hack into his former company's network. Since Simon remembers some of the server names, he attempts to run the AXFR and IXFR commands using DIG.

What is Simon trying to accomplish here?

A. Send DOS commands to crash the DNS servers

B. Perform DNS poisoning

C. Enumerate all the users in the domain

D. Perform a zone transfer

Answer: D

NO.3 Which vulnerability assessment phase describes the scope of the assessment, identifies and ranks the critical assets, and creates proper information protection procedures such as effective planning, scheduling, coordination, and logistics?

A. Threat-Assessment Phase

B. Assessment Phase

C. Pre-Assessment Phase

D. Post-Assessment Phase

Answer: C

NO.4 Which of the following scan option is able to identify the SSL services?

A. -sS

B. -sV

C. -sU

D. -sT

Answer: B

NO.5 : 11

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

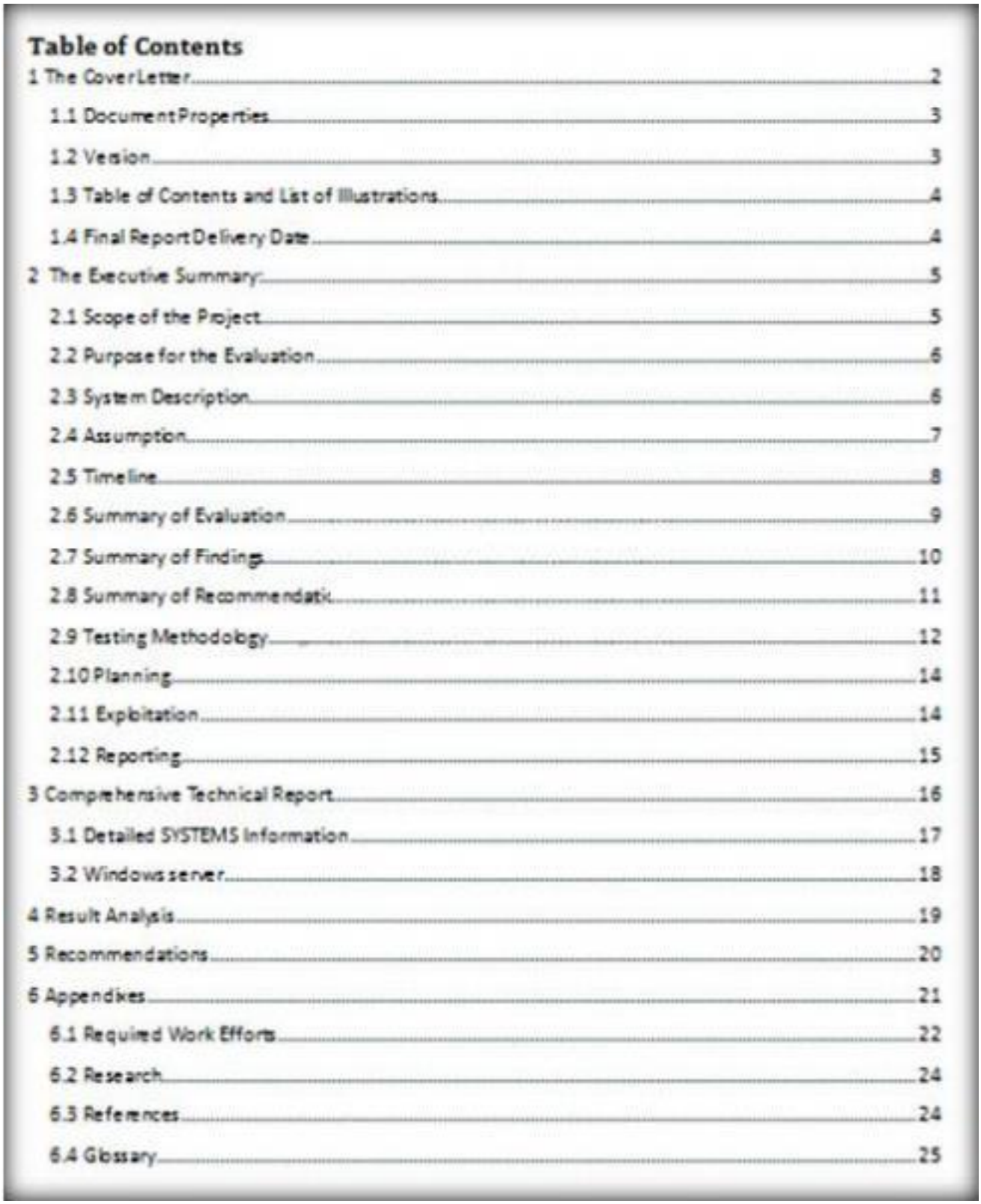


Table of Contents

A. Host Report
B. Activity Report
C. Vulnerability Report
D. Client-Side Test Report
Answer: D

NO.6 Which one of the following tools of trade is a commercial shellcode and payload generator written in Python by Dave Aitel?

A. Network Security Analysis Tool (NSAT)

B. Canvas

C. Microsoft Baseline Security Analyzer (MBSA)

D. CORE Impact

Answer: B

NO.7 Which of the following has an offset field that specifies the length of the header and data?

A. TCP Header

B. IP Header

C. UDP Header

D. ICMP Header

Answer: A

NO.8 Which of the following is the objective of Gramm-Leach-Bliley Act?

A. To certify the accuracy of the reported financial statement

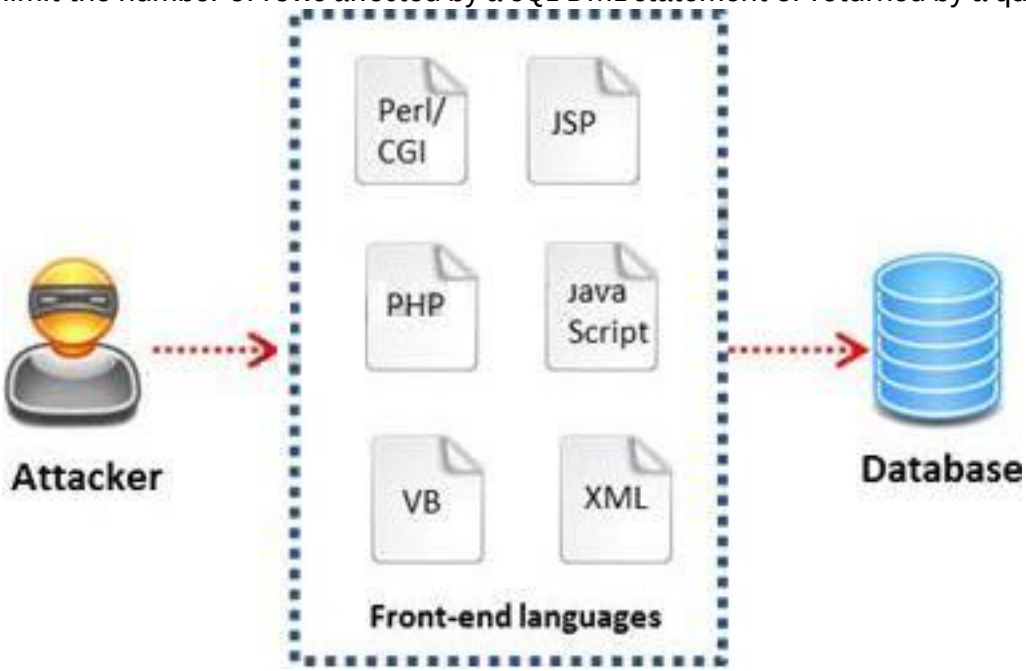
B. To set a new or enhanced standards for all U.S. public company boards, management and public accounting firms

C. To ease the transfer of financial information between institutions and banks

D. To protect the confidentiality, integrity, and availability of data

Answer: C

NO.9 A WHERE clause in SQL specifies that a SQL Data Manipulation Language (DML) statement should only affect rows that meet specified criteria. The criteria are expressed in the form of predicates. WHERE clauses are not mandatory clauses of SQL DML statements, but can be used to limit the number of rows affected by a SQL DML statement or returned by a query.



A pen tester is trying to gain access to a database by inserting exploited query statements with a

WHERE clause. The pen tester wants to retrieve all the entries from the database using the WHERE clause from a particular table (e.g. StudentTable).
What query does he need to write to retrieve the information?
A. SELECT * FROM StudentTable WHERE roll_number = '' or '1' = '1'
B. EXTRACT* FROM StudentTable WHERE roll_number = 1 order by 1000
C. RETRIVE * FROM StudentTable WHERE roll_number = 1'#
D. DUMP * FROM StudentTable WHERE roll_number = 1 AND 1=1-
Answer: A

NO.10 You are the security analyst working for a private company out of France. Your current assignment is to obtain credit card information from a Swiss bank owned by that company. After initial reconnaissance, you discover that the bank security defenses are very strong and would take too long to penetrate. You decide to get the information by monitoring the traffic between the bank and one of its subsidiaries in London.
After monitoring some of the traffic, you see a lot of FTP packets traveling back and forth. You want to sniff the traffic and extract usernames and passwords. What tool could you use to get this information?
A. Snort
B. Airsnort
C. Ettercap
D. RaidSniff
Answer: C

NO.11 You are a security analyst performing a penetration tests for a company in the Midwest. After some initial reconnaissance, you discover the IP addresses of some Cisco routers used by the company.
You type in the following URL that includes the IP address of one of the routers:
http://172.168.4.131/level/99/exec/show/config
After typing in this URL, you are presented with the entire configuration file for that router.
What have you discovered?
A. Cisco IOS Arbitrary Administrative Access Online Vulnerability
B. HTML Configuration Arbitrary Administrative Access Vulnerability
C. HTTP Configuration Arbitrary Administrative Access Vulnerability
D. URL Obfuscation Arbitrary Administrative Access Vulnerability
Answer: C

NO.12 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. ABC

C. QRT

D. EMP

Answer: D