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

Identify the type of testing that is carried out without giving any information to the employees or administrative head of the organization.

A. Unannounced Testing

B. Double Blind Testing

C. Announced Testing

D. Blind Testing

Correct Answer: A

QUESTION 2

An antenna is a device that is designed to transmit and receive the electromagnetic waves that are generally called radio waves. Which one of the following types of antenna is developed from waveguide technology?

A. Leaky Wave Antennas

B. Aperture Antennas

C. Reflector Antenna

D. Directional Antenna

Correct Answer: B

QUESTION 3

SQL injection attack consists of insertion or "injection" of either a partial or complete SQL query via the

data input or transmitted from the client (browser) to the web application.

A successful SQL injection attack can:

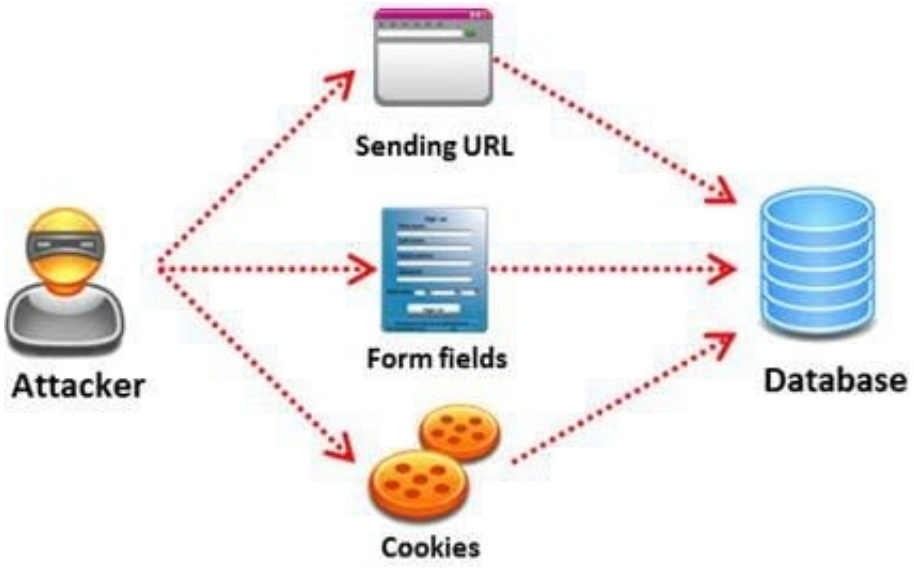
i)Read sensitive data from the database

iii)Modify database data (insert/update/delete)

iii)Execute administration operations on the database (such as shutdown the DBMS)

iV)Recover the content of a given file existing on the DBMS file system or write files into the file system

v)Issue commands to the operating system



Pen tester needs to perform various tests to detect SQL injection vulnerability. He has to make a list of all input fields whose values could be used in crafting a SQL query, including the hidden fields of POST requests and then test them separately, trying to interfere with the query and to generate an error.

In which of the following tests is the source code of the application tested in a non-runtime environment to detect the SQL injection vulnerabilities?

A. Automated Testing

B. Function Testing

C. Dynamic Testing

D. Static Testing

Correct Answer: D

QUESTION 4

Output modules allow Snort to be much more flexible in the formatting and presentation of output to its users. Snort has 9 output plug-ins that push out data in different formats. Which one of the following output plug-ins allows alert data to be written in a format easily importable to a database?

A. unified

B. csv

C. alert_unixsock

D. alert_fast

Correct Answer: B

QUESTION 5

Assessing a network from a hacker\\'s point of view to discover the exploits and vulnerabilities that are accessible to the outside world is which sort of vulnerability assessment?

A. Network Assessments

B. Application Assessments

C. Wireless Network Assessments

D. External Assessment

Correct Answer: D

QUESTION 6

Which of the following reports provides a summary of the complete pen testing process, its outcomes, and recommendations?

A. Vulnerability Report

B. Executive Report

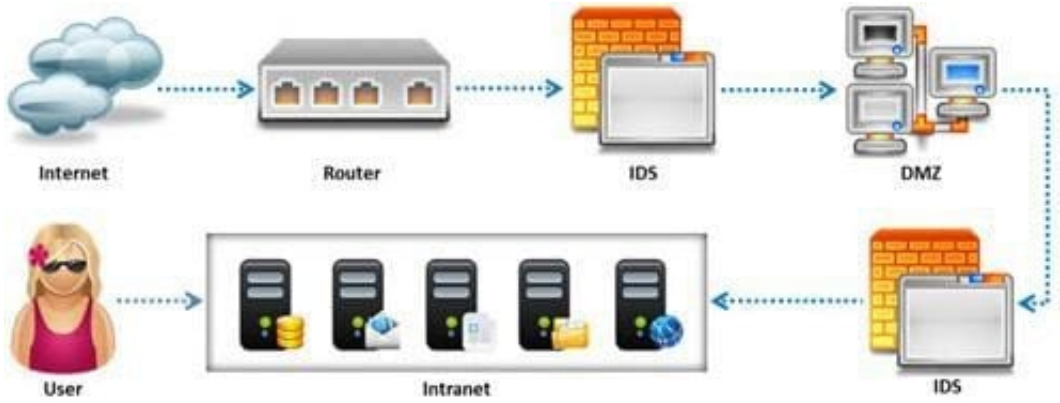
C. Client-side test Report

D. Host Report

Correct Answer: B

QUESTION 7

Due to illegal inputs, various types of TCP stacks respond in a different manner. Some IDSs do not take into account the TCP protocol\\'s urgency feature, which could allow testers to evade the IDS.



Penetration tester needs to try different combinations of TCP flags (e.g. none, SYN/FIN, SYN/RST, SYN/ FIN/ACK, SYN/RST/ACK, and All Flags) to test the IDS. Which of the following TCP flag combinations combines the problem of initiation, midstream, and termination flags with the PSH and URG?

A. SYN/RST/ACK

B. SYN/FIN/ACK

C. SYN/FIN

D. All Flags

Correct Answer: D

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

Internet Control Message Protocol (ICMP) messages occur in many situations, such as whenever a datagram cannot reach the destination or the gateway does not have the buffering capacity to forward a datagram. Each ICMP message contains three fields: type, code, and checksum. Different types of Internet Control Message Protocols (ICMPs) are identified by a TYPE field. If the destination is not reachable, which one of the following are generated?

A. Type 8 ICMP codes

B. Type 12 ICMP codes

C. Type 3 ICMP codes

D. Type 7 ICMP codes

Correct Answer: C

QUESTION 10

Besides the policy implications of chat rooms, Internet Relay Chat (IRC) is frequented by attackers and used as a command and control mechanism. IRC normally uses which one of the following TCP ports?

A. 6566 TCP port

B. 6771 TCP port

C. 6667 TCP port

D. 6257 TCP port

Correct Answer: C

QUESTION 11

By default, the TFTP server listens on UDP port 69. Which of the following utility reports the port status of target TCP and UDP ports on a local or a remote computer and is used to troubleshoot TCP/IP connectivity issues?

A. PortQry

B. Netstat

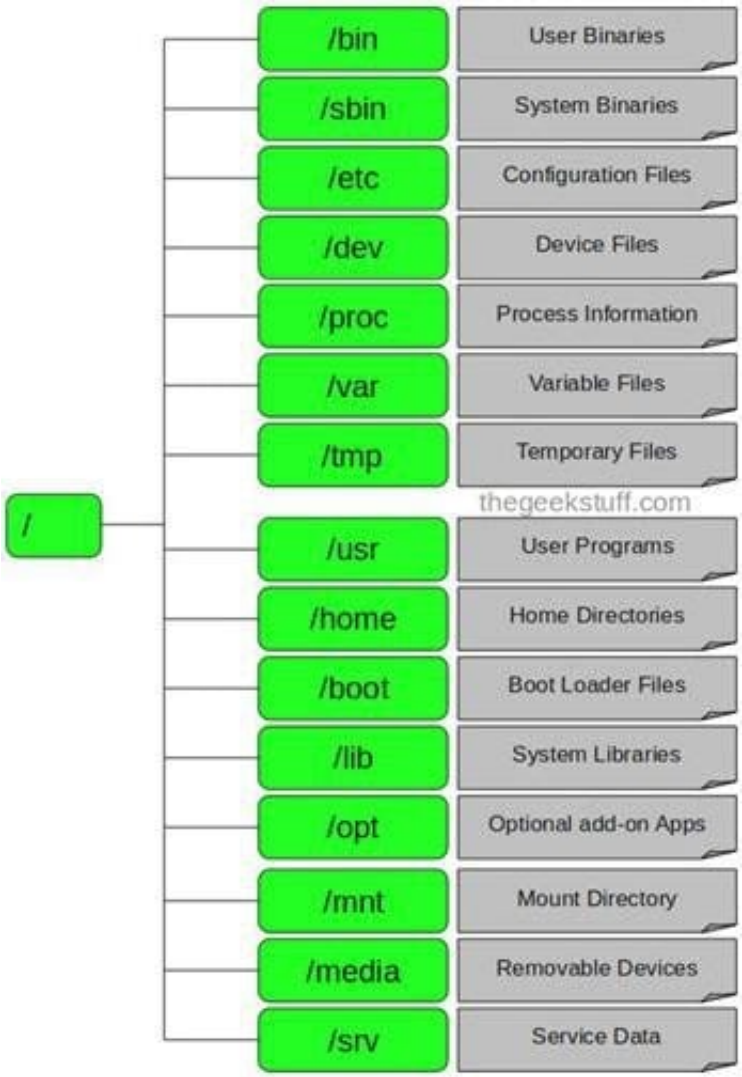
C. Telnet

D. Tracert

Correct Answer: A

QUESTION 12

In Linux, /etc/shadow file stores the real password in encrypted format for user\\'s account with added properties associated with the user\\'s password.



In the example of a /etc/shadow file below, what does the bold letter string indicate? Vivek: 1fnffc$GteyHdicpGOfffXX40w#5:13064:0:99999:7

A. Number of days the user is warned before the expiration date

B. Minimum number of days required between password changes

C. Maximum number of days the password is valid

D. Last password changed

Correct Answer: B

QUESTION 13

Information gathering is performed to:

i) Collect basic information about the target company and its network ii) Determine the operating system

used, platforms running, web server versions, etc.

iii) Find vulnerabilities and exploits

Which of the following pen testing tests yields information about a company\\'s technology infrastructure?

A. Searching for web page posting patterns

B. Analyzing the link popularity of the company\\'s website

C. Searching for trade association directories

D. Searching for a company\\'s job postings

Correct Answer: A

QUESTION 14

Which one of the following acts makes reputational risk of poor security a reality because it requires public disclosure of any security breach that involves personal information if it is unencrypted or if it is reasonably believed that the information has been acquired by an unauthorized person?

A. California SB 1386

B. Sarbanes-Oxley 2002

C. Gramm-Leach-Bliley Act (GLBA)

D. USA Patriot Act 2001

Correct Answer: A

QUESTION 15

The SnortMain () function begins by associating a set of handlers for the signals, Snort receives. It does this using the

signal () function. Which one of the following functions is used as a programspecific signal and the handler for this calls the DropStats() function to output the current Snort statistics?

A. SIGUSR1

B. SIGTERM

C. SIGINT

D. SIGHUP

Correct Answer: A