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.pass2lead.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 documents helps in creating a confidential relationship between the pen tester and client to protect critical and confidential information or trade secrets?

A. Penetration Testing Agreement

B. Rules of Behavior Agreement

C. Liability Insurance

D. Non-Disclosure Agreement

Correct Answer: D

QUESTION 2

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 3

Which of the following statements is true about Multi-Layer Intrusion Detection Systems (mIDSs)?

A. Decreases consumed employee time and increases system uptime

B. Increases detection and reaction time

C. Increases response time

D. Both a and c

Correct Answer: A

QUESTION 4

You are conducting a penetration test against a company and you would like to know a personal email address of John, a crucial employee. What is the fastest, cheapest way to find out John\\'s email address.

A. Call his wife and ask for his personal email account

B. Call a receptionist and ask for John Stevens\\' personal email account

C. Search in Google for his personal email ID

D. Send an email to John stating that you cannot send him an important spreadsheet attachment file to his business email account and ask him if he has any other email accounts

Correct Answer: D

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

Metasploit framework in an open source platform for vulnerability research, development, and penetration testing. Which one of the following metasploit options is used to exploit multiple systems at once?

A. NinjaDontKill

B. NinjaHost

C. RandomNops

D. EnablePython

Correct Answer: A

QUESTION 7

Which one of the following is a useful formatting token that takes an int * as an argument, and writes the number of bytes already written, to that location?

A. "%n"

B. "%s"

C. "%p"

D. "%w"

Correct Answer: A

QUESTION 8

HTTP protocol specifies that arbitrary binary characters can be passed within the URL by using %xx notation, where \\'xx\\' is the

A. ASCII value of the character

B. Binary value of the character

C. Decimal value of the character

D. Hex value of the character

Correct Answer: C

QUESTION 9

Port numbers are used to keep track of different conversations crossing the network at the same time. Both TCP and UDP use port (socket) numbers to pass information to the upper layers. Port numbers have the assigned ranges. The port numbers above 1024 are considered as which one of the following? (Select all that apply)

A. Well-known port numbers

B. Dynamically assigned port numbers

C. Unregistered port numbers

D. Statically assigned port numbers

Correct Answer: B

QUESTION 10

Traffic on which port is unusual for both the TCP and UDP ports?

A. Port 81

B. Port 443

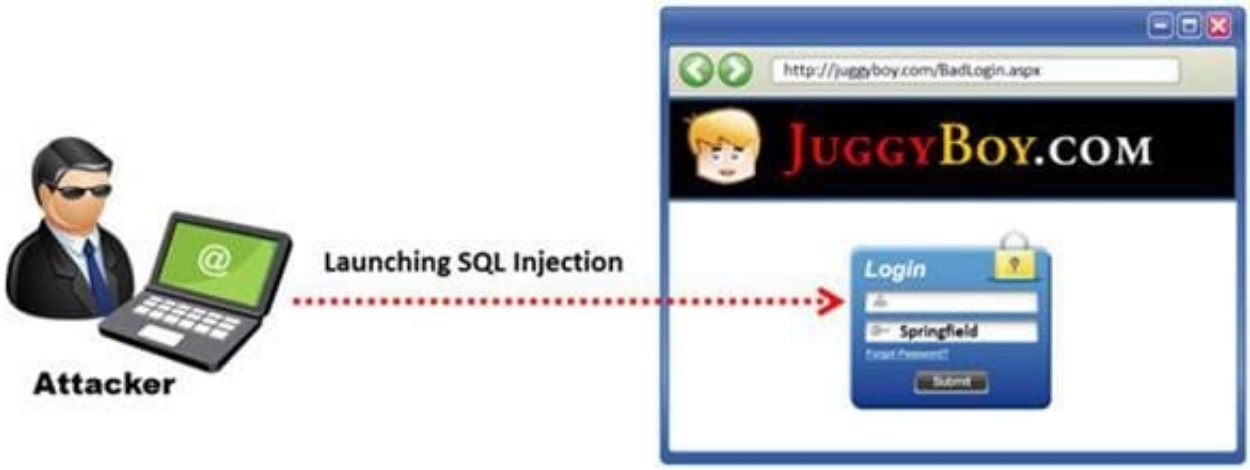
C. Port 0

D. Port21

Correct Answer: C

QUESTION 11

SQL injection attacks are becoming significantly more popular amongst hackers and there has been an estimated 69 percent increase of this attack type. This exploit is used to great effect by the hacking community since it is the primary way to steal sensitive data from web applications. It takes advantage of non-validated input vulnerabilities to pass SQL commands through a web application for execution by a back-end database. The below diagram shows how attackers launched SQL injection attacks on web applications.



Which of the following can the attacker use to launch an SQL injection attack?

A. Blah\\' "2=2 "

B. Blah\\' and 2=2 -

C. Blah\\' and 1=1 -

D. Blah\\' or 1=1 -

Correct Answer: D

QUESTION 12

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

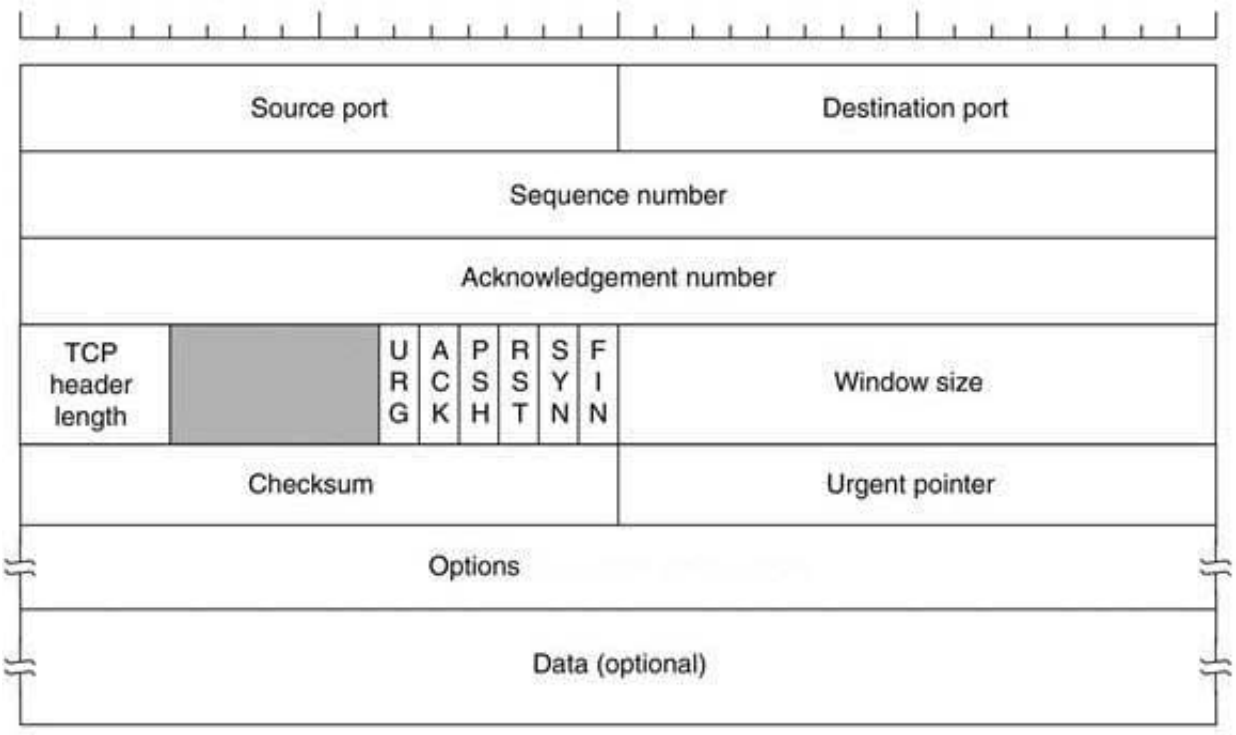
C. Searching for trade association directories

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

Correct Answer: A

QUESTION 13

Transmission control protocol accepts data from a data stream, divides it into chunks, and adds a TCP header creating a TCP segment. The TCP header is the first 24 bytes of a TCP segment that contains the parameters and state of an endto-end TCP socket. It is used to track the state of communication between two TCP endpoints. For a connection to be established or initialized, the two hosts must synchronize. The synchronization requires each side to send its own initial sequence number and to receive a confirmation of exchange in an acknowledgment (ACK) from the other side The below diagram shows the TCP Header format:



How many bits is a acknowledgement number?

A. 16 bits

B. 32 bits

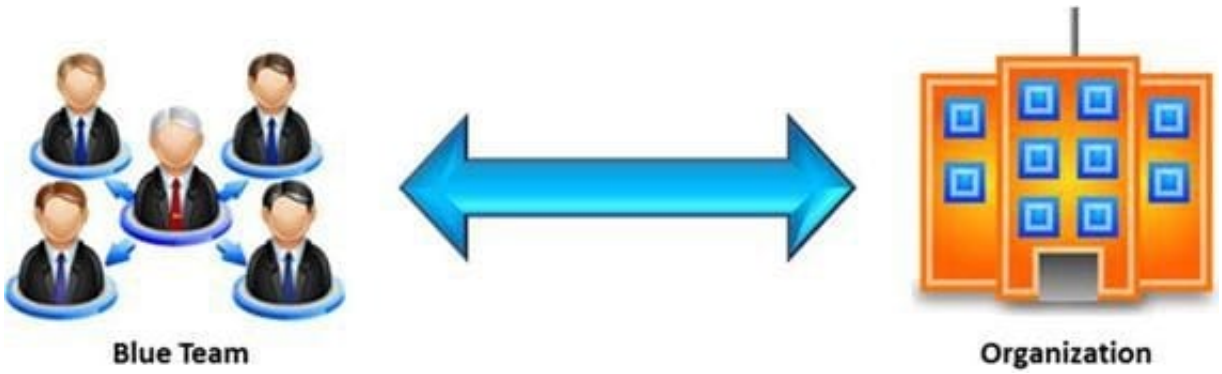
C. 8 bits

D. 24 bits

Correct Answer: B

QUESTION 14

In the context of penetration testing, what does blue teaming mean?



A. A penetration test performed with the knowledge and consent of the organization\\'s IT staff

B. It is the most expensive and most widely used

C. It may be conducted with or without warning

D. A penetration test performed without the knowledge of the organization\\'s IT staff but with permission from upper management

Correct Answer: A

QUESTION 15

Which of the following attacks is an offline attack?

A. Pre-Computed Hashes

B. Hash Injection Attack

C. Password Guessing

D. Dumpster Diving

Correct Answer: A