Date:

Module Name: SC

Q. No. 1

Question:

The default configuration file of MySQL on a linux machine is:

Answer Choices

A: mysql.conf
B: sql.conf
C:my.cnf
D: db.cnf

Q. No. 2

Question:

To delete a database in MySQL, the _____ DATABASE statement is used.

Answer Choices

A: DELETE
B: DEL
C: DROP
D: ERASE

Q. No. 3

Question:

In Python Regular Expression, if the search is successful, the search() method returns a _____object.

Answer Choices
A: find
B: match
C: true
D: string

Q. No. 4

Question:

_____occurs when an application doesn't securely encrypt it's sensitive data when it is stored into a database.

Answer Choices
A: CSRF
B: Insecure Direct Object Reference
C: Insecure cryptographic storage
D: Broken authentication

Q. No. 5

Question:

_____ is systematic examination (often known as peer review) of computer

source code

Answer Choices

A: Obfuscation
B: Code review
C: Fuzzing
D: Tagging

Q. No. 6

Question:

Open Redirects, and Directory Traversals are all examples of _____

Answer Choices
A: File Injection
B: Insecure Direct Object Reference
C: Directory Traversal
D: Broken authentication

Q. No. 7

Question:

_____allows an attacker to instantiate a class without running any of the class constructors

Answer Choices

A: Cloning
B: Copying
C: Declaring
D: Importing

Q. No. 8

Question:

The purpose /object of the _____ attack is to inject and execute commands specified by the attacker in the vulnerable application.

Answer Choices
A: File Injection
B: CSRF
C: Command Injection
D: DOS

Q. No. 9

Question:

_____vulnerabilities occur when developers fail to use authentication methods that have been adequately tested and rely on their own, often flawed, method for authenticating users.

Answer Choices
A: File Injection
B: XSS
C: Directory Traversal
D: Broken authentication

Q. No. 10

Question:

The value of b in the following example:

```
>>> a = [1,2,3,4]
>>> a
[1, 2, 3, 4]
>>> b = a.append(5)
>>> print b
```

Answer Choices
A: [1,2,3]

B: [1,2,3,4]
C: [1,2,3,4,5]
D: None

Q. No. 11

Question:

The methods dict.keys() return _____ of the keys explicitly.

Answer Choices
A: string
B: list
C: tuple
D: sets

Q. No. 12

Question:

The _____ construct is an easy way to test if an element appears in a list, returning True/False.

Answer Choices
A: for
B: while
C: in
D: else

Q. No. 13

Question:

The _____-returns a list of substrings separated by the given delimiter.

Answer Choices
A: str.sub('delim')
B: str.cut('delim')
C: str.split('delim')
D: str.divide('delim')

Q. No. 14

Question:

The sys module is an _____ which has (among other things) an _____ called path.

Answer Choices
A: attribute, object
B: object, attribute
C: attribute, method
D:method, attribute

Q. No. 15

Question:

In Python, to find out the default EOL for your OS, use _____

Answer Choices
A: os.linesep
B: os.eol
C: eol.os
D: linesep.os()

Q. No. 16

Question:

_____ is defined as any potential danger to information or systems.

Answer Choices
A: Threat
B: Vulnerability
C: Exploit
D: Risk

Q. No. 17

Question:

_____is the identification, assessment, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events.

Answer Choices
A: Risk Mitigation
B: Risk Identification
C: Risk Assessment
D: Risk Management

Q. No. 18

Question:

NSLookup is a good tool to use to gain additional information about a target network. What does the following command accomplish?

nslookup
> server <ipaddress>
> set type =any
> ls -d <target.com>

Answer Choices
A: Enables DNS spoofing
B: Loads bogus entries into the DNS table
C: Verifies zone security
D: Performs a zone transfer

Q. No. 19

Question:

What does black box examing mean?

Answer Choices
A: You have full knowledge of the environment
B: You have no knowledge of the environment
C: You have partial knowledge of the environment
D: None of the above

Q. No. 20

Question:
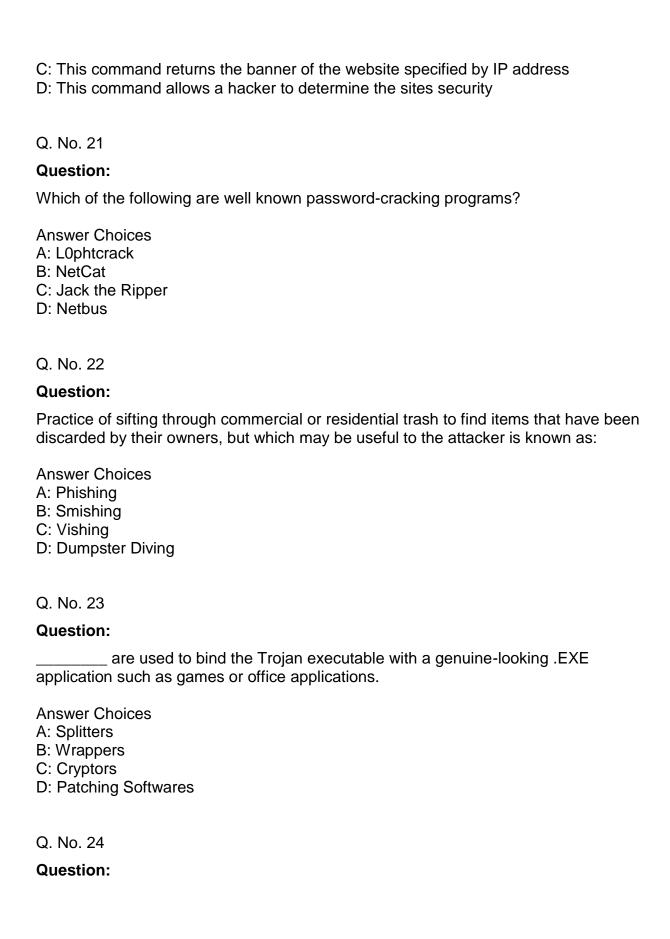
What does the following command achieve?

Telnet <IP Address> <Port 80>
HEAD /HTTP/1.0
<Return>
<Return>

Answer Choices
A: This command returns the home page for the IP address specified
B: This command opens a backdoor Telnet session to the IP address specified

C: This command returns the banner of the website specified by IP address
D: This command allows a hacker to determine the sites security

Q. No. 21

Question:

Which of the following are well known password-cracking programs?

Answer Choices
A: L0phtcrack
B: NetCat
C: Jack the Ripper
D: Netbus

Q. No. 22

Question:

Practice of sifting through commercial or residential trash to find items that have been discarded by their owners, but which may be useful to the attacker is known as:

Answer Choices
A: Phishing
B: Smishing
C: Vishing
D: Dumpster Diving

Q. No. 23

Question:

_____ are used to bind the Trojan executable with a genuine-looking .EXE application such as games or office applications.

Answer Choices
A: Splitters
B: Wrappers
C: Cryptors
D: Patching Softwares

Q. No. 24

Question:

What type of attack changes its signature and/or payload to thwart detection by antivirus programs?

Answer Choices

A: Polymorphic
B: Rootkit
C: Boot sector
D: File infecting

Q. No. 25

Question:

The best security defense against a sniffer on the network is_____.

Answer Choices
A: to use a firewall
B: to use an IDS
C: encryption
D: Hashing

Q. No. 26

Question:

What do Trinoo, TFN2k, WinTrinoo, T-Sight, and Stracheldraht have in common?

Answer Choices
A: All are hack tools developed by the legion of doom
B: All are tools that can be used not only by hackers, but also security personnel
C: All are DDOS tools
D: All are tools that are only effective against Windows

Q. No. 27

Question:

Central Industrial Bank was a medium-sized, regional financial institution in New York. The bank recently deployed a new Internet-accessible Web application. Using this application, Central Frost's customers could access their account balances, transfer money between accounts, pay bills and conduct online financial business through a Web browser. John Stevens was in charge of information security at Central Frost Bank. After one month in production, the Internet banking application was the subject of several customer complaints. Mysteriously, the account balances of many of Central

Frost's customers had been changed! However, money hadn't been removed from the bank. Instead, money was transferred between accounts. Given this attack profile, John Stevens reviewed the Web application's logs and found the following entries:

Attempted login of unknown user: johnm
Attempted login of unknown user: susaR
Attempted login of unknown user: sencat
Attempted login of unknown user: pete";
Attempted login of unknown user: ' or 1=1--
Attempted login of unknown user: '; drop table logins--
Login of user jason, sessionID= 0x75627578626F6F6B
Login of user daniel, sessionID= 0x98627579539E13BE
Login of user rebecca, sessionID= 0x9062757944CCB811
Login of user mike, sessionID= 0x9062757935FB5C64
Transfer Funds user jason
Pay Bill user mike
Logout of user mike

What type of attack did the Hacker attempt?

Answer Choices
A: Brute force attack in which the Hacker attempted guessing login ID and password from password cracking tools.
B: The Hacker used a random generator module to pass results to the Web server and exploited Web application CGI vulnerability.
C: The Hacker attempted SQL Injection technique to gain access to a valid bank login ID.
D: The Hacker attempted Session hijacsheets, in which the Hacker opened an account

with the bank, then logged in to receive a session ID, guessed the next ID and took over

Jason's

Q. No. 28

Question:

You may be able to identify the IP addresses and machine names for the firewall, and the names of internal mail servers by:

Answer Choices

A: Sending a mail message to a valid address on the target network, and examining the header information generated by the IMAP servers
B: Examining the SMTP header information generated by using the –mx command parameter of DIG

C: Examining the SMTP header information generated in response to an e-mail message sent to an invalid address
D: Sending a mail message to an invalid address on the target network, and examining the header information generated by the POP servers

Q. No. 29

Question:

What is a critical part of physical security?

Answer Choices
A. Guard dogs
B. Layered access control
C. Fences
D. CCTV

Q. No. 30

Question:

_____ is a malicious program used to launch other malicious programs.

Answer Choices
A: Launcher
B: Rootkit
C: Spamware
D: Trojan

Q. No. 31

Question:

MySQL, by default, runs on port # _____

Answer Choices
A: 3304
B: 2802
C: 3306
D: 2801

Q. No. 32

Question:

To create a database in MySQL, the _____ DATABASE statement is used.

Answer Choices
A: MAKE
B: CREATE
C: BUILD
D: NEW

Q. No. 33

Question:

In Python, the _____ module provides regular expression support.

Answer Choices
A: regex
B: re
C: rexp
D: regmatch

Q. No. 34

Question:

_____typically happens when a page doesn't have the correct access control policy in place.

Answer Choices
A: Failing to restrict URL access
B: Insecure Direct Object Reference
C: Insecure cryptographic storage
D: Broken authentication

Q. No. 35

Question:

_____involves sending malformed strings into application input and watching for unexpected crashes.

Answer Choices
A: Obfuscating
B: Encyrpting
C: Fuzzing
D: Hashing

Q. No. 36

Question:

_____ is an attack which forces an end user to execute unwanted actions on a web application in which he/she is currently authenticated.

Answer Choices
A: CSRF
B: Insecure Direct Object Reference
C: Directory Traversal
D: Broken authentication

Q. No. 37

Question:

_____ attacks are a type of injection problem, in which malicious scripts are injected into the trusted web sites.

Answer Choices
A: File Injection
B: XSS
C: Directory Traversal
D: DOS

Q. No. 38

Question:

_____is when a web application exposes an internal implementation object to the user.

Answer Choices
A: File Injection
B: Insecure Direct Object Reference
C: Directory Traversal
D: Broken authentication

Q. No. 39

Question:

Python was Designed by

Answer Choices
A: Daniel Mark Lewin

B: Peter L Duetch
C: Guido van Rossum
D: Paul McArthur

Q. No. 40

Question:

Python's efficient key/value hash table structure is called a _____.

Answer Choices
A: datastructure
B: dict
C: string
D: tuble