Q1.Entering Password::blah' or 1=1- into a web form in order to get a password is an example of what type of attack?

1. Buffer overflow
2. Heap-based overflow
3. Stack-based overflow
4. SQL injection

Q2. Replacing NOP instructions with other code in a buffer overflow mutation serves what purpose?

1. Bypassing an IDS
2. Overwriting the return pointer
3. Advancing the return pointer
4. Bypassing a firewall

Q3. Which of the following is used to store dynamically allocated variables?

1. Heap overflow
2. Stack overflow
3. Heap
4. Stack

Q4. What is the first step in a SQL injection attack?

1. Enter arbitrary commands at a user prompt.
2. Locate a user input field on a web page.
3. Locate the return pointer.
4. Enter a series of NOP instructions.

Q5. What command is used to retrieve information from a SQL database?

1. INSERT
2. GET
3. SET
4. SELECT

Q6. Which of the following is a countermeasure for buffer overflows?

1. Not using single quotes
2. Securing all login pages with SSL
3. Bounds checking
4. User validation

Q7. Why are many programs vulnerable to SQL injection and buffer overflow attacks?

1. The programs are written quickly and use poor programming techniques.
2. These are inherent flaws in any program.
3. The users have not applied the correct service packs.
4. The programmers are using the wrong programming language.

Q8. What are two types of buffer overflow attacks?

1. Heap and stack
2. Heap and overflow
3. Stack and memory allocation
4. Injection and heap

Q9. Which application will help identify whether a website is vulnerable to SQL injection attacks?

1. BlackWidow
2. Metasploit
3. Scrawlr
4. SQL Block

Q10. An ethical hacker is performing a penetration test on a web application. The hacker finds a user input field on a web form and enters a single quotation mark. The website responds with a server error. What does the error indicate?

1. The web application is susceptible to SQL injection attacks.
2. The web application is not susceptible to SQL injection attacks.
3. The server is experiencing a denial of service.
4. The web application has crashed.

Q11. Which of the following are countermeasures to SQL injection attacks? (Choose two.)

1. Rejecting known bad input
2. Sanitizing and validating input field
3. Performing user validation
4. Ensuring all user input is a variable

Q12.What is the type for object 5.6?

1. Int
2. Float
3. Str

Q13.Suppose s is "Welcome", what is s.upper()?

1. Welcome
2. WELCOME
3. Welcome

Q14.what is the output of the following code?

1. <type 'tuple'>
2. <type 'int'>
3. <type 'set'>
4. <type 'complex'>
5. <type 'list'>

Q15.What gets printed?

def f(): pass

print type(f())

1. <type 'function'>
2. <type 'tuple'>
3. <type 'NoneType'>
4. <type 'str'>
5. <type 'type'>

Q16. what is the output of the below program?

a = [1,2,3,None,(),[],]

print len(a)

1. syntax error
2. 4
3. 5
4. 6
5. 7

Q17.What gets printed?

nums = set([1,1,2,3,3,3,4])

print len(nums)

1. 1
2. 2
3. 4
4. 5
5. 7

Q18. What gets printed?

x = True

y = False

z = False

if x or y and z:

print "yes"

else:

print "no"

1. yes
2. no
3. fails to compile

Q19.If PYTHONPATH is set in the environment, which directories are searched for modules?

A) PYTHONPATH directory

B) current directory

C) home directory

D) installation dependent default path

1. A only
2. A and D
3. A,B and C
4. A, B and D
5. A, B, C and D

 Q20. What gets printed?

class parent:

def \_\_init\_\_(self, param):

self.v1 = param

class child(parent):

def \_\_init\_\_(self, param):

self.v2 = param

obj = child(11)

print "%d %d" % (obj.v1, obj.v2)

1. None None
2. None 11
3. 11 None
4. 11 11
5. Error is generated by the program

Q21. What gets printed?

class Account:

def \_\_init\_\_(self, id):

self.id = id

id = 666

acc = Account(123)

print acc.id

1. None
2. 123
3. 666
4. SyntaxError, this program will not run

Q22.To open a file c:\scores.txt for reading, use \_\_\_\_\_\_\_\_\_\_.

1. infile = open("c:\scores.txt", "r")
2. infile = open("c:\\scores.txt", "r")
3. infile = open(file = "c:\scores.txt", "r")
4. infile = open(file = "c:\\scores.txt", "r")

Q23.What is displayed when the following program is run?  
try:  
    list = 5 \* [0]  
    x = list[5]  
    print("Done")  
except IndexError:   
    print("Index out of bound")

1. "Done" followed by "Index out of bound"
2. "Index out of bound"
3. "Done"
4. Nothing displayed

Q24. What is displayed when the following program is run?

try:  
    list = 10 \* [0]  
    x = list[9]  
    print("Done")  
except IndexError:   
    print("Index out of bound")  
else:   
    print("Nothing is wrong")  
finally:   
    print("Finally we are here")

1. "Done" followed by "Nothing is wrong"
2. "Done" followed by "Nothing is wrong" followed by "Finally we are here"
3. "Index out of bound" followed by "Nothing is wrong" followed by "Finally we are here"
4. "Nothing is wrong" followed by "Finally we are here"

Q25. You are a programmer analyzing the code of an application running on your organization's servers. There are an excessive number of fgets () commands. These are C++ functions that do not perform bounds checking. What kind of attack is this program susceptible to?

1. Buffer overflow
2. Denial of service
3. SQL injection
4. Password cracking

Q26. Which of the following is a session-hijacking tool that runs on Linux operating systems?

1. Juggernaut
2. Hunt
3. TTYWatcher
4. TCP Reset Utility

Q27. What is session hijacking?

1. Monitoring UDP sessions
2. Monitoring TCP sessions
3. Taking over UDP sessions
4. Taking over TCP sessions

Q28. What types of packets are sent to the victim of a session-hijacking attack to cause them to close their end of the connection?

1. FIN and ACK
2. SYN or ACK
3. SYN and ACK
4. FIN or RST

Q29. What is an ISN?

1. Initiation session number
2. Initial sequence number
3. Initial session number
4. Indication sequence number

Q30. Which of the following are types of HTTP web authentication? (Choose all that apply.)

1. Digest
2. Basic
3. Windows
4. Kerberos