Correct Answer: A

QUESTION 190

You are trying to break into a highly classified top-secret mainframe computer with highest security system in place at Merclyn Barley Bank located in Los Angeles. You know that conventional hacking doesn't work in this case, because organizations such as banks are generally tight and secure when it comes to protecting their systems. In other words you are trying to penetrate an otherwise impenetrable system. How would you proceed?

A. Look for "zero-day" exploits at various underground hacker websites in Russia and China and buy the necessary exploits from these hackers and target the bank's network.
B. Try to hang around the local pubs or restaurants near the bank, get talking to a poorly-paid or disgruntled employee, and offer them money if they'll abuse their access privileges by providing you with sensitive information.
C. Launch DDOS attacks against Merclyn Barley Bank's routers and firewall systems using 100,000 or more "zombies" and "bots".
D. Try to conduct Man-in-the-Middle (MITM) attack and divert the network traffic going to the Merclyn Barley Bank's Webserver to that of your machine using DNS Cache Poisoning techniques.

Correct Answer: B

QUESTION 191

This is an attack that takes advantage of a web site vulnerability in which the site displays content that includes un-sanitized user-provided data.

<ahref="http://foobar.com/index.html?id=%3Cscript%20src=%22http://baddomain.com/badscript.js %22%3E%3C/script%3E">See foobar

What is this attack?

A. Cross-site-scripting attack
B. SQL Injection
C. URL Traversal attack
D. Buffer Overflow attack

Correct Answer: A

QUESTION 192

Buffer X in an Accounting application module for Brownies Inc. can contain 200 characters. The programmer makes an assumption that 200 characters are more than enough. Because there were no proper boundary checks being conducted, Bob decided to insert 400 characters into the 200-character buffer. (Overflows the buffer). Below is the code snippet:

```
Void func (void)
{
int I; char buffer [200];
for (I=0; I<400; I++)
buffer [I]= 'A';
return;
}
```

How can you protect/fix the problem of your application as shown above?

A. Because the counter starts with 0, we would stop when the counter is less than 200.
B. Because the counter starts with 0, we would stop when the counter is more than 200.
C. Add a separate statement to signify that if we have written less than 200 characters to the buffer, the stack should stop because it cannot hold any more data.
D. Add a separate statement to signify that if we have written 200 characters to the buffer, the stack should stop because it cannot hold any more data.

Correct Answer: AD

QUESTION 193
Which of the following encryption is NOT based on block cipher?

A. DES
B. Blowfish
C. AES (Rijndael)
D. RC4

Correct Answer: D

QUESTION 194
Michael is a junior security analyst working for the National Security Agency (NSA) working primarily on breaking terrorist encrypted messages. The NSA has a number of methods they use to decipher encrypted messages including Government Access to Keys (GAK) and inside informants. The NSA holds secret backdoor keys too many of the encryption algorithms used on the Internet. The problem for the NSA, and Michael, is that terrorist organizations are starting to use custom-built algorithms or obscure algorithms purchased from corrupt governments. For this reason, Michael and other security analysts like him have been forced to find different methods of deciphering terrorist messages. One method that Michael thought of using was to hide malicious code inside seemingly harmless programs. Michael first monitors sites and bulletin boards used by known terrorists, and then he is able to glean email addresses to some of these suspected terrorists. Michael then inserts a stealth keylogger into a mapping program file readme.txt and then sends that as an attachment to the terrorist. This keylogger takes

screenshots every 2 minutes and also logs all keyboard activity into a hidden file on the terrorist's computer. Then, the keylogger emails those files to Michael twice a day with a built in SMTP server. What technique has Michael used to disguise this keylogging software?

A. Steganography
B. Wrapping
C. ADS
D. Hidden Channels

Correct Answer: C

QUESTION 195
In which step Steganography fits in CEH System Hacking Cycle (SHC)

A. Step 2: Crack the password
B. Step 1: Enumerate users
C. Step 3: Escalate privileges
D. Step 4: Execute applications
E. Step 5: Hide files
F. Step 6: Cover your tracks

Correct Answer: E

QUESTION 196
Which definition below best describes a covert channel?

A. A server program using a port that is not well known.
B. Making use of a protocol in a way it was not intended to be used.
C. It is the multiplexing taking place on a communication link.
D. It is one of the weak channels used by WEP that makes it insecure.

Correct Answer: B

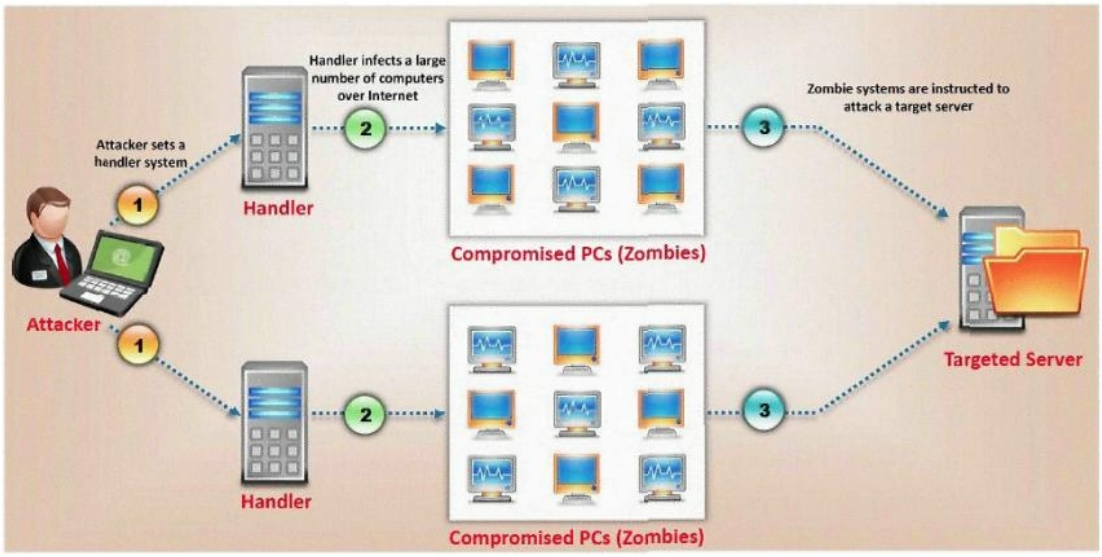
QUESTION 197
Joseph has just been hired on to a contractor company of the Department of Defense as their Senior Security Analyst. Joseph has been instructed on the company's strict security policies that have been implemented, and the policies that have yet to be put in place. Per the Department of Defense, all DoD users and the users of their contractors must use two-factor authentication to access their networks. Joseph has been delegated the task of researching and implementing the best two-factor authentication method for his company. Joseph's supervisor has told him that they would like to use some type of hardware device in tandem with a security or identifying pin

number. Joseph's company has already researched using smart cards and all the resources needed to implement them, but found the smart cards to not be cost effective. What type of device should Joseph use for two-factor authentication?

A. Biometric device
B. OTP
C. Proximity cards
D. Security token

Correct Answer: D

QUESTION 198
What type of attack is shown here?



A. Bandwidth exhaust Attack
B. Denial of Service Attack
C. Cluster Service Attack
D. Distributed Denial of Service Attack

Correct Answer: D

QUESTION 199

What is the correct order of steps in CEH System Hacking Cycle?

A.

Step 1. Gaining Access
Step 2. Escalating Privileges
Step 3. Executing Applications
Step 4. Hiding Files
Step 5. Covering Tracks

B.

Step 1. Covering Tracks
Step 2. Hiding Files
Step 3. Escalating Privileges
Step 4. Executing Applications
Step 5. Gaining Access

C.

Step 1. Executing Applications
Step 2. Gaining Access
Step 3. Covering Tracks
Step 4. Escalating Privileges
Step 5. Hiding Files

D.

Step 1. Escalating Privileges
Step 2. Gaining Access
Step 3. Executing Applications
Step 4. Covering Tracks
Step 5. Hiding Files

Correct Answer: A

QUESTION 200

Identify SQL injection attack from the HTTP requests shown below:

A. http://www.myserver.c0m/search.asp?lname=smith%27%3bupdate%20usertable%20set%20passwd%3d%27hAx0r%27%3b--%00
B. http://www.myserver.c0m/script.php?mydata=%3cscript%20src=%22
C. http%3a%2f%2fwww.yourserver.c0m%2fbadscript.js%22%3e%3c%2fscript%3e
D. http://www.victim.com/example accountnumber=67891&creditamount=999999999

Correct Answer: A