QUESTION 119

Bob was frustrated with his competitor, Brownies Inc., and decided to launch an attack that would result in serious financial losses. He planned the attack carefully and carried out the attack at the appropriate moment. Meanwhile, Trent, an administrator at Brownies Inc., realized that their main financial transaction server had been attacked. As a result of the attack, the server crashed and Trent needed to reboot the system, as no one was able to access the resources of the company. This process involves human interaction to fix it. What kind of Denial of Service attack was best illustrated in the scenario above?

A. Simple DDoS attack.
B. DoS attacks which involves flooding a network or system.
C. DoS attacks which involves crashing a network or system.
D. DoS attacks which is done accidentally or deliberately.

Correct Answer: C

QUESTION 120

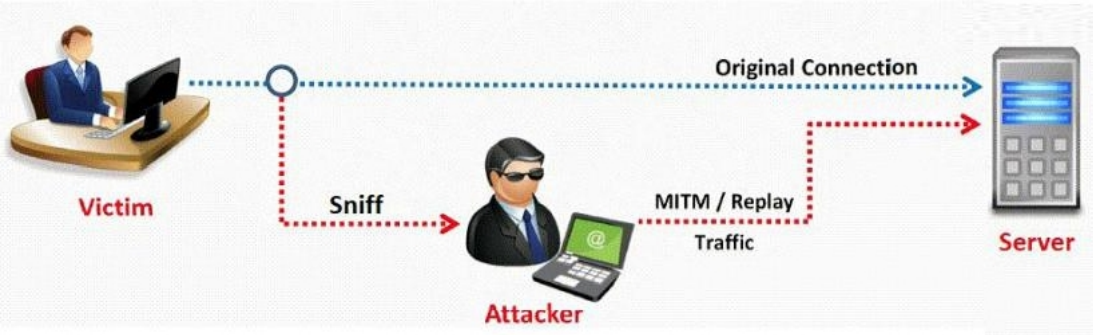
Johnny is a member of the hacking group Orpheus1. He is currently working on breaking into the Department of Defense's front end Exchange Server. He was able to get into the server, located in a DMZ, by using an unused service account that had a very weak password that he was able to guess. Johnny wants to crack the administrator password, but does not have a lot of time to crack it. He wants to use a tool that already has the LM hashes computed for all possible permutations of the administrator password. What tool would be best used to accomplish this?

A. SMBCrack
B. SmurfCrack
C. PSCrack
D. RainbowTables

Correct Answer: D

QUESTION 121

In this type of Man-in-the-Middle attack, packets and authentication tokens are captured using a sniffer. Once the relevant information is extracted, the tokens are placed back on the network to gain access.



A. Token Injection Replay attacks
B. Shoulder surfing attack
C. Rainbow and Hash generation attack
D. Dumpster diving attack

Correct Answer: A

QUESTION 122
The FIN flag is set and sent from host A to host B when host A has no more data to transmit (Closing a TCP connection). This flag releases the connection resources. However, host A can continue to receive data as long as the SYN sequence numbers of transmitted packets from host B are lower than the packet segment containing the set FIN flag.

A. false
B. true

Correct Answer: B

QUESTION 123
Jason is the network administrator of Spears Technology. He has enabled SNORT IDS to detect attacks going through his network. He receives Snort SMS alerts on his iPhone whenever there is an attempted intrusion to his network.

He receives the following SMS message during the weekend.

```
[**] [111:6:1] spp_stream4: STEALTH ACTIVITY (Full XMAS scan) detection [**]
05/12-11:05:08.858815 192.168.12.88:1211 -> 192.168.12.56:22
TCP TTL:118 TOS:0x10 ID:50387 IpLen:20 DgmLen:40 DF
**UAPRSF Seq: 0x130331C9 Ack: 0x6C694D7D Win: 0x200 TcpLen: 20 UrgPtr: 0x0
```

An attacker Chew Siew sitting in Beijing, China had just launched a remote scan on Jason's

network with the hping command. Which of the following hping2 command is responsible for the above snort alert?

A. chenrocks:/home/siew # hping -S -R -P -A -F -U 192.168.2.56 -p 22 -c 5 -t 118
B. chenrocks:/home/siew # hping -F -Q -J -A -C -W 192.168.2.56 -p 22 -c 5 -t 118
C. chenrocks:/home/siew # hping -D -V -R -S -Z -Y 192.168.2.56 -p 22 -c 5 -t 118
D. chenrocks:/home/siew # hping -G -T -H -S -L -W 192.168.2.56 -p 22 -c 5 -t 118

Correct Answer: A

QUESTION 124

Leesa is the senior security analyst for a publicly traded company. The IT department recently rolled out an intranet for company use only with information ranging from training, to holiday schedules, to human resources data. Leesa wants to make sure the site is not accessible from outside and she also wants to ensure the site is Sarbanes-Oxley (SOX) compliant. Leesa goes to a public library as she wants to do some Google searching to verify whether the company's intranet is accessible from outside and has been indexed by Google. Leesa wants to search for a website title of "intranet" with part of the URL containing the word "intranet" and the words "human resources" somewhere in the webpage. What Google search will accomplish this?

A. related:intranet allinurl:intranet:"human resources"
B. cache:"human resources" inurl:intranet(SharePoint)
C. intitle:intranet inurl:intranet+intext:"human resources"
D. site:"human resources"+intext:intranet intitle:intranet

Correct Answer: C

QUESTION 125

Bob has been hired to do a web application security test. Bob notices that the site is dynamic and must make use of a back end database. Bob wants to see if SQL Injection would be possible. What is the first character that Bob should use to attempt breaking valid SQL request?

A. Semi Column
B. Double Quote
C. Single Quote
D. Exclamation Mark

Correct Answer: C

QUESTION 126

Hampton is the senior security analyst for the city of Columbus in Ohio. His primary responsibility is to ensure that all physical and logical aspects of the city's computer network are secure from all angles. Bill is an IT technician that works with Hampton in the same IT department. Bill's primary responsibility is to keep PC's and servers up to date and to keep track of all the agency laptops that the company owns and lends out to its employees. After Bill setup a wireless network for the agency, Hampton made sure that everything was secure. He instituted encryption, rotating keys, turned off SSID broadcasting, and enabled MAC filtering. According to agency policy, only company laptops are allowed to use the wireless network, so Hampton entered all the MAC addresses for those laptops into the wireless security utility so that only those laptops should be able to access the wireless network. Hampton does not keep track of all the laptops, but he is pretty certain that the agency only purchases Dell laptops. Hampton is curious about this because he notices Bill working on a Toshiba laptop one day and saw that he was on the Internet. Instead of jumping to conclusions, Hampton decides to talk to Bill's boss and see if they had purchased a Toshiba laptop instead of the usual Dell. Bill's boss said no, so now Hampton is very curious to see how Bill is accessing the Internet. Hampton does site surveys every couple of days, and has yet to see any outside wireless network signals inside the company's building. How was Bill able to get Internet access without using an agency laptop?

A. Bill spoofed the MAC address of Dell laptop.
B. Bill connected to a Rogue access point.
C. Toshiba and Dell laptops share the same hardware address.
D. Bill brute forced the Mac address ACLs.

Correct Answer: A

QUESTION 127

LAN Manager Passwords are concatenated to 14 bytes, and split in half. The two halves are hashed individually. If the password is 7 characters or less, than the second half of the hash is always:

A. 0xAAD3B435B51404EE
B. 0xAAD3B435B51404AA
C. 0xAAD3B435B51404BB
D. 0xAAD3B435B51404CC

Correct Answer: A

QUESTION 128

When writing shellcodes, you must avoid _____ because these will end the string.

```
char shellcode[] =
"\xeb\x1f\x5e\x89\x76\x08\x31\xc0\x88\x46\x07\x89\x46\x0c\xb0\x0b"
"\x89\xf3\x8d\x4e\x08\x8d\x56\x0c\xcd\x80\x31\xdb\x89\xd8\x40\xcd"
"\x80\xe8\xdc\xff\xff\xff/bin/sh";

void main() {
int *ret;
ret = (int *)&ret + 2;
(*ret) = (int)shellcode;
}
```

A. Root bytes
B. Null bytes
C. Char bytes
D. Unicode bytes

Correct Answer: B

QUESTION 129

Jess the hacker runs L0phtCrack's built-in sniffer utility that grabs SMB password hashes and stores them for offline cracking. Once cracked, these passwords can provide easy access to whatever network resources the user account has access to. But Jess is not picking up hashes from the network. Why?

A. The network protocol is configured to use SMB Signing.
B. The physical network wire is on fibre optic cable.
C. The network protocol is configured to use IPSEC.
D. L0phtCrack SMB sniffing only works through Switches and not Hubs.

Correct Answer: A

QUESTION 130

Harold works for Jacobson Unlimited in the IT department as the security manager. Harold has created a security policy requiring all employees to use complex 14 character passwords. Unfortunately, the members of management do not want to have to use such long complicated passwords so they tell Harold's boss this new password policy should not apply to them. To comply with the management's wishes, the IT department creates another Windows domain and moves all the management users to that domain. This new domain has a password policy only requiring 8 characters. Harold is concerned about having to accommodate the managers, but cannot do anything about it. Harold is also concerned about using LanManager security on his network instead of NTLM or NTLMv2, but the many legacy applications on the network prevent