C. Depending on the switch manufacturer, the device will either delete every entry in its ARP cache or reroute packets to the nearest switch.
D. The switches will route all traffic to the broadcast address created collisions.

Correct Answer: A

QUESTION 172
You are programming a buffer overflow exploit and you want to create a NOP sled of 200 bytes in the program exploit.c.

```
char shellcode[] =
"\x31\xc0\xb0\x46\x31\xdb\x31\xc9\xcd\x80\xeb\x16\x5b\x31\xc0"
"\x88\x43\x07\x89\x5b\x08\x89\x43\x0c\xb0\x0b\x8d\x4b\x08\x8d"
"\x53\x0c\xcd\x80\xe8\xe5\xff\xff\xff\x2f\x62\x69\x6e\x2f\x73"
"\x68";
```

What is the hexadecimal value of NOP instruction?

A. 0x60
B. 0x80
C. 0x70
D. 0x90

Correct Answer: D

QUESTION 173
This TCP flag instructs the sending system to transmit all buffered data immediately.

A. SYN
B. RST
C. PSH
D. URG
E. FIN

Correct Answer: C

QUESTION 174

The network administrator at Spears Technology, Inc has configured the default gateway Cisco router's access-list as below:

```
Current configuration : 1206 bytes
!
version 12.3
!
hostname Victim
!
enable secret 5 $1$h2iz$DHYpcqURFOAPD2aDuA.YX0
!
interface Ethernet0/0
ip address dhcp
ip nat outside
half-duplex
!
interface Ethernet0/1
ip address 192.168.1.1 255.255.255.0
ip nat inside
half-duplex
!
router rip
network 192.168.1.0
!
ip nat inside source list 102 interface Ethernet0/0 overload
no ip http server
ip classless
!
access-list 1 permit 192.168.1.0 0.0.0.255
access-list 102 permit ip any any
!
snmp-server community public RO

snmp-server community private RW 1
snmp-server enable traps tty
!
line con 0
logging synchronous
login
line aux 0
line vty 0 4
password secret
login
!!
end
```

You are hired to conduct security testing on their network. You successfully brute-force the SNMP community string using a SNMP crack tool. The access-list configured at the router prevents you from establishing a successful connection. You want to retrieve the Cisco configuration from the router. How would you proceed?

A. Use the Cisco's TFTP default password to connect and download the configuration file.
B. Run a network sniffer and capture the returned traffic with the configuration file from the router.

C. Run Generic Routing Encapsulation (GRE) tunneling protocol from your computer to the router masking your IP address.
D. Send a customized SNMP set request with a spoofed source IP address in the range 192.168.1.0.

Correct Answer: BD

QUESTION 175
You work for Acme Corporation as Sales Manager. The company has tight network security restrictions. You are trying to steal data from the company's Sales database (Sales.xls) and transfer them to your home computer. Your company filters and monitors traffic that leaves from the internal network to the Internet. How will you achieve this without raising suspicion?

A. Encrypt the Sales.xls using PGP and e-mail it to your personal gmail account.
B. Package the Sales.xls using Trojan wrappers and telnet them back your home computer.
C. You can conceal the Sales.xls database in another file like photo.jpg or other files and send it out in an innocent looking email or file transfer using Steganography techniques.
D. Change the extension of Sales.xls to sales.txt and upload them as attachment to your hotmail account.

Correct Answer: C

QUESTION 176
Study the snort rule given below and interpret the rule.

alert tcp any any --> 192.168.1.0/24 111 (content:"|00 01 86 a5|"; msg. "mountd access";)

A. An alert is generated when a TCP packet is generated from any IP on the 192.168.1.0 subnet and destined to any IP on port 111.
B. An alert is generated when any packet other than a TCP packet is seen on the network and destined for the 192.168.1.0 subnet.
C. An alert is generated when a TCP packet is originated from port 111 of any IP address to the 192.168.1.0 subnet.
D. An alert is generated when a TCP packet originating from any IP address is seen on the network and destined for any IP address on the 192.168.1.0 subnet on port 111.

Correct Answer: D

QUESTION 177
What port number is used by LDAP protocol?

A. 110
B. 389
C. 464
D. 445

Correct Answer: B

QUESTION 178
Fred is the network administrator for his company. Fred is testing an internal switch. From an external IP address, Fred wants to try and trick this switch into thinking it already has established a session with his computer. How can Fred accomplish this?

A. Fred can accomplish this by sending an IP packet with the RST/SIN bit and the source address of his computer.
B. He can send an IP packet with the SYN bit and the source address of his computer.
C. Fred can send an IP packet with the ACK bit set to zero and the source address of the switch.
D. Fred can send an IP packet to the switch with the ACK bit and the source address of his machine.

Correct Answer: D

QUESTION 179
Within the context of Computer Security, which of the following statements describes Social Engineering best?

A. Social Engineering is the act of publicly disclosing information.
B. Social Engineering is the means put in place by human resource to perform time accounting.
C. Social Engineering is the act of getting needed information from a person rather than breaking into a system.
D. Social Engineering is a training program within sociology studies.

Correct Answer: C

QUESTION 180

In Trojan terminology, what is a covert channel?

A. A channel that transfers information within a computer system or network in a way that violates the security policy.
B. A legitimate communication path within a computer system or network for transfer of data.
C. It is a kernel operation that hides boot processes and services to mask detection.
D. It is Reverse tunneling technique that uses HTTPS protocol instead of HTTP protocol to establish connections.

Correct Answer: A

QUESTION 181

When a normal TCP connection starts, a destination host receives a SYN (synchronize/start) packet from a source host and sends back a SYN/ACK (synchronize acknowledge). The destination host must then hear an ACK (acknowledge) of the SYN/ACK before the connection is established. This is referred to as the "TCP three-way handshake." While waiting for the ACK to the SYN ACK, a connection queue of finite size on the destination host keeps track of connections waiting to be completed. This queue typically empties quickly since the ACK is expected to arrive a few milliseconds after the SYN ACK. How would an attacker exploit this design by launching TCP SYN attack?

A. Attacker generates TCP SYN packets with random destination addresses towards a victim host.
B. Attacker floods TCP SYN packets with random source addresses towards a victim host.
C. Attacker generates TCP ACK packets with random source addresses towards a victim host.
D. Attacker generates TCP RST packets with random source addresses towards a victim host.

Correct Answer: B