Kafrelsheikh University - Faculty of Engineering			
Course	**Network Security**	**Date**	**31/5/2018**
Time	**2 Hours**	**Mark**	**40**
Students	**4th year Electronics and Electrical Communications**		

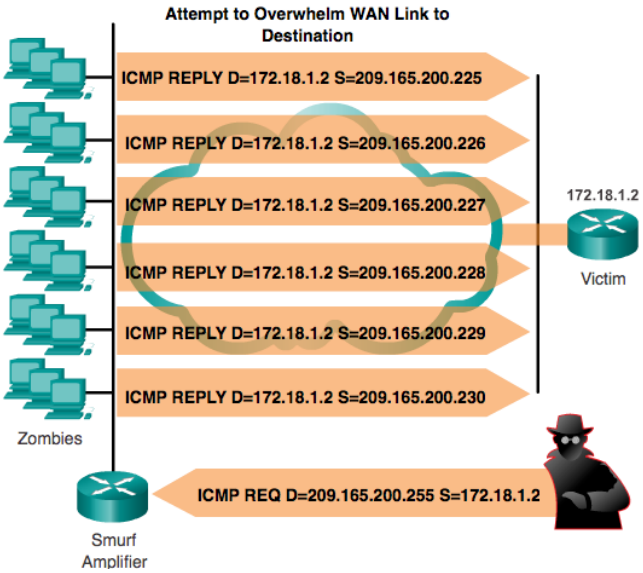
This exam measures ILOs no.: a. 8. a.12, b.1, b.3.

Answer all the following questions:

Q1. Explain in detail the flowing terms: (10 Marks)

a. Smurf attacks. b. SYN Flood Attack

- **ANS: Smurf attack: A Smurf Attack is a DDoS attack in which large numbers of ICMP packets with the intended victim's spoofed source IP are broadcast to a computer network.**
- **This attack sends a large number of ICMP requests to directed broadcast addresses, all with spoofed source addresses on the same network as the respective directed broadcast.**
  - **If the routing device delivering traffic to those broadcast addresses forwards the directed broadcasts, all hosts on the destination networks send ICMP replies, multiplying the traffic by the number of hosts on the networks.**
  - **On a multi-access broadcast network, hundreds of machines might reply to each packet.**



SYN Flood Attack: A flood of TCP SYN packets is sent, often with a forged sender address. Each packet is handled like a connection request, causing the server to spawn a half-open (embryonic) connection by sending back a TCP SYN-ACK packet and waiting for a packet in response from the sender address. However, because the sender address is forged, the response never comes. These half-open connections saturate the number of available connections the server is able to make, keeping it from responding to legitimate requests until after the attack ends.

Q2. In the following configuration: **(10 Marks)**

```
R1(config)# time-range EMPLOYEE-TIME
R1(config-time-range)# periodic weekdays 12:00 to 13:00
R1(config-time-range)# periodic weekdays 17:00 to 19:00
R1(config-time-range)# exit
R1(config)# access-list 100 permit ip 192.168.1.0 0.0.0.255 any time-range EMPLOYEE-TIME
R1(config)# access-list 100 deny ip any any
R1(config)# interface FastEthernet 0/1
R1(config-if)# ip access-group 100 in
R1(config-if)# exit
```

a- Explain the configuration code. **(5 Marks)**

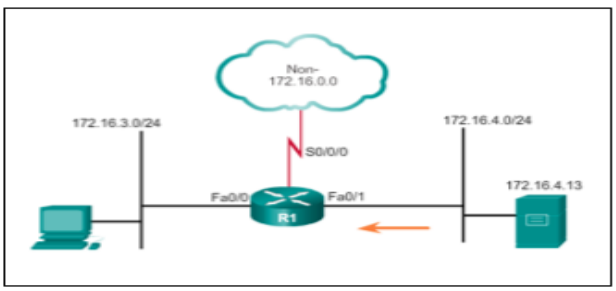
ANS: 1- Set a time range with the name "EMPLOYEE-TIME".
2- Set time interval between 12:00 to 13:00 every day during weekdays.
3- Set a time interval between 17:00 to 19:00 every day during weekdays.
4- exit "EMPLOYEE-TIME".
5- Set an access list that allows ip connection from devices in network 192.168.1.0/ 255.255.255.0 to any other network during "EMPLOYEE-TIME".
6-Deny any other connection other than "EMPLOYEE-TIME".
7- Configure the interface FastEthernet 0/1
8-apply the access list to packets entering the interface.
9- exit the interface configuration.

b- Write a configuration code so that it denies access to the internet only during Sundays from 14:00 to 16:00. **(5 Marks)**

ANS: R1(config)# time-range Employee-TIME
Periodic Sunday 14:00 to 16:00.
Exit
Access-list 100 deny ip 192.168.1.0 0.0.0.255 any time-range Employee-TIME
Access-list 100 permit any any

Q3. In the following configuration, we need the hosts in the 172.16.4.0 network to access the 172.16.3.0 using FTP protocol and not access the internet, but the access list does not work as intended.
(10 Marks)

a. **R1(config)# access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 21**
b. **R1(config)# access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 20**
c. **R1(config)# access-list 101 permit ip any any**
d. **R1(config)# interface FastEthernet 0/1**
e. **R1(config-if)# ip access-group 101 in**



a. **Explain why this configuration code not working.** **(5 Marks)**
   ANS: because the first two lines blocks the FTP connection from 172.16.4.0 to 172.16.3.0.
b. **Write the correct code.** **(5 Marks)**
   ANS: Change every deny to permit and permit to deny.

Q4. In the following configuration: l (10 Marks)

```
R1# show login failures
Total failed logins: 22
Detailed information about last 50 failures

Username     SourceIPAddr     lPort Count TimeStamp
admin        1.1.2.1          23    5     15:38:54 UTC Wed Dec 10 2008
Admin        10.10.10.10      23    13    15:58:43 UTC Wed Dec 10 2008
admin        10.10.10.10      23    3     15:57:14 UTC Wed Dec 10 2008
cisco        10.10.10.10      23    1     15:57:21 UTC Wed Dec 10 2008

R1#
```

a. **Explain the configuration code.** **(5 Marks)**
   ANS: The show login failures shows 22 failed logins and these logins are explained in detail in a table.
b. **What is the difference between the *show* and *debug* commands?** **(5 Marks)**

The debug command shows the real time interaction with the command while the show command shows the current state of the configuration.

Good Luck and Best Wishes **Dr. Ibrahim Elashry**