ITCS 461 Computer & Communication Security Date : ___02/04/2023____

ID:_6388087_ Name:___Chanisara Kotrachai___________ Section : ____2______ ______

Save this answer sheet as “ **Lab8-5988xxx-Name.docx**” (Removing all figures will help reduce the file size).

Submit this file to the lab folder in mycourse website according to your session.

Lab 8 : Firewall

Follow Lab 8 document (Lab8.pdf) and answer these questions:

Part I: Without Firewall

no question in this part

Part II: With Firewall

Question 1:

1) Observe the traffic flowing from the Internet into your system or from your network to the Internet. Is your network connected to the Internet? __Y_ (Y/N)
2) Explain why or why not: There are several rules indicating traffic between the cloud and various services, including Web, VOIP, DNS, Mail, Chat, and Database, which suggest that the network is communicating with resources outside of its own local network.

   Add some **active attacks** by clicking on several different options.
3) Are these attacks able to get into your network? __N__ (Y/N)
4) Do you feel your system is secure? __Y____ (Y/N)
5) What’s wrong with this scenario? ___None__________________________________

   ____

Question 2: What is firewall rule which allows only Email traffic to go out ?

- Source IP : ______Any______________ Port : _____*_____
- Destination IP : ________Any________ Port : _____25____
- Protocol : __TCP_______

(Create firewall rule named, **“Email out”**, similar to **DNS out**, try until you get success, copy IP, Port and Protocol from Firewall1 Rule window to your answer.)

Question 3: What is firewall rule which allows only Email traffic to come in ?

- Source IP : ______Any_____________ Port : _____*_____
- Destination IP : __Mail_____________ Port : _____25____
- Protocol : __TCP_______

(Move **"Email out"** rule to Inactive Rules box. Then create new firewall rule named, **"Email in"**, similar to Email out, but define source IP as any and destination IP as Email, try until you get success, copy IP, Port and Protocol from Firewall1 Rule window to your answer.)

Question 4: What is a set of firewall rules which allows only Email traffic to come in and go out ?

The 1st Rule :

- Source IP : ______Mail_____________ Port : _____25____
- Destination IP : __Any_____________ Port : _____*_____
- Protocol : __TCP_______

The 2nd Rule :

- Source IP : ______Mail_____________ Port : _____25____
- Destination IP : __Any_____________ Port : _____*_____
- Protocol : __TCP_______

(Combine, **"Email in"** and **"Email out"** rules into Active Rules box, try to play until you get success, copy IP, Port and Protocol from Firewall1 Rule window to your answer.)

Question 5:

- Change a sequence of Email in and Email out rules. After the change, does the traffic still flow? __Y__ (Y/N)
- Why? _____Email in and Email out are using same port and IP._______________
  ____

Question 6:

What is a rule which allows all inbound traffics?

- The 1st Rule :
  - Source IP : Any Port : *
  - Destination IP : DNS Port : 53
  - Protocol : UDP
- The 2nd Rule :
  - Source IP : Any Port : *
  - Destination IP : Mail Port : 25
  - Protocol : TCP
- The 3rd Rule :
  - Source IP : Any Port : *
  - Destination IP : Database Port : 3306
  - Protocol : TCP
- The 4th Rule :
  - Source IP : Any Port : *
  - Destination IP : VOIP Port : 38287
  - Protocol : TCP
- The 5th Rule :
  - Source IP : Any Port : *
  - Destination IP : Web Port : 80
  - Protocol : TCP
- The 6th Rule :
  - Source IP : Any Port : *
  - Destination IP : Chat Port : 5222
  - Protocol : TCP

What is a rule which allows all outbound traffics?

- The 1st Rule :
  - Source IP : DNS Port : 53
  - Destination IP : Any Port : *
  - Protocol : UDP
- The 2nd Rule :
  - Source IP : Mail Port : 25
  - Destination IP : Any Port : *
  - Protocol : TCP
- The 3rd Rule :
  - Source IP : Database Port : 3306
  - Destination IP : Any Port : *
  - Protocol : TCP

- The 4th Rule :
  - Source IP : VOIP Port : 38287
  - Destination IP : Any Port : *
  - Protocol : TCP
- The 5th Rule :
  - Source IP : Web Port : 80
  - Destination IP : Any Port : *
  - Protocol : TCP
- The 6th Rule :
  - Source IP : Chat Port : 5222
  - Destination IP : Any Port : *

- What is a rule which blocks all traffics?
  Deny All

Question 7:
How many rules do we need? Write down all of them.

Source IP Port Destination IP Port Protocol

- The 1st Rule :
  - Source IP : Any Port : 80
  - Destination IP : Web Port : 80
  - Protocol : TCP
- The 2nd Rule :
  - Source IP : Database Port : 3306
  - Destination IP : Any Port : 3306
  - Protocol : TCP
- The 3rd Rule :
  - Source IP : Any Port : 38287
  - Destination IP : VOIP Port : 38287
  - Protocol : TCP
- The 4th Rule :
  - Source IP : VOIP Port : 38287
  - Destination IP : Any Port : 38287
  - Protocol : TCP

Part III: With 2 Firewalls

Question 8:
What is a set of firewall rules such that **Firewall 1** allows only **DNS**, **Chat** and **Email** to come in and out, **Firewall 2** allows only **Chat** and **Email** to come in and out.

Source IP Port Destination IP Port Protocol

Firewall 1

- The 1st Rule :
    - Source IP : Any Port : *
    - Destination IP : DNS Port : 53
    - Protocol : UDP
- The 2nd Rule :
    - Source IP : DNS Port : 53
    - Destination IP : Any Port : *
    - Protocol : UDP
- The 3rd Rule :
    - Source IP : Any Port : *
    - Destination IP : Chat Port : 5222
    - Protocol : TCP
- The 4th Rule :
    - Source IP : Chat Port : 5222
    - Destination IP : Any Port : *
    - Protocol : TCP
- The 5th Rule :
    - Source IP : Any Port : *
    - Destination IP : Mail Port : 25
    - Protocol : TCP
- The 6th Rule :
    - Source IP : Mail Port : 25
    - Destination IP : Any Port : *
    - Protocol : TCP

Firewall 2

- The 1st Rule :
  - Source IP : Any Port : *
  - Destination IP : Chat Port : 5222
  - Protocol : TCP
- The 2nd Rule :
  - Source IP : Chat Port : 5222
  - Destination IP : Any Port : *
  - Protocol : TCP
- The 3rd Rule :
  - Source IP : Any Port : *
  - Destination IP : Mail Port : 25
  - Protocol : TCP
- The 4th Rule :
  - Source IP : Mail Port : 25
  - Destination IP : Any Port : *
  - Protocol : TCP