| ITCS 461 Computer & Communication Security  | Date : <u>02/04/2023</u>   |
|---|--|
| ID: 6388087 Name: Chanisara Kotrachai   | Section :2   |
| Save this answer sheet as "Lab8-5988xxx-Name.docx" (Resize).  | moving all figures will help reduce the file   |
| Submit this file to the lab folder in mycourse website accordi  | ing to your session.   |
| Lab 8 : Firewa  | all  |
| Follow Lab 8 document (Lab8.pdf) and answer these question  | ns:  |
| Part I: Without Firewall  |  |
| no question in this part  |  |
| Part II: With Firewall  |  |
| Question 1:  1) Observe the traffic flowing from the Internet is network to the Internet. Is your network connected to the Internet. It is your network are several rule cloud and various services, including Web, Von Database, which suggest that the network is controlled of its own local network.  Add some active attacks by clicking on several several rule cloud and various services, including Web, Von Database, which suggest that the network is controlled of its own local network.  Add some active attacks by clicking on several rule cloud and various services, including Web, Von Database, which suggest that the network is controlled of its own local network.  Add some active attacks by clicking on several rule cloud and various services, including Web, Von Database, which suggest that the network is controlled of its own local network.  Add some active attacks by clicking on several rule cloud and various services, including Web, Von Database, which suggest that the network is controlled of its own local network.  Add some active attacks by clicking on several rule cloud and various services, including Web, Von Database, which suggest that the network is controlled of its own local network.  Add some active attacks by clicking on several rule cloud and various services, including Web, Von Database, which suggest that the network is controlled or controlled of its own local network.  Add some active attacks able to get into your network.  What is a several rule cloud and various services, including Web, Von Database, which services is a several rule cloud and various services, including Web, Von Database, which services is a several rule cloud and various services, including Web, Von Database, which services is a several rule cloud and various services | ected to the Internet?Y_ (Y/N)  les indicating traffic between the OIP, DNS, Mail, Chat, and ommunicating with resources  ral different options.  k?N_ (Y/N) |
| <ul> <li>Question 2: What is firewall rule which allows only</li> <li>Source IP: Any Port:</li> <li>Destination IP: Any Port:</li> <li>Protocol: TCP</li> </ul>   | *  |

(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.)

| <ul><li>Source IP :</li><li>Destination IP :</li></ul> | Mail                                  | Port :                   | 25            |                        |
|--|---------------------------------------|--------------------------|---------------|------------------------|
| • Protocol: TCP  | IVIUII                                | 1010                     |               |                        |
| • 110t0cor. <u>1cr</u>                                 |                                       |                          |               |                        |
| (Move "Email out" rule                                 | e to Inactive F                       | Rules box. Then          | create new    | firewall rule named    |
| <b>"Email in"</b> , similar to E                       | · · · · · · · · · · · · · · · · · · · |                          |               |                        |
| Email, try until you get s                             |                                       |                          |               |                        |
| to your answer.)                                       | ,                                     | ,                        |               |                        |
| <i>y</i> ,   |                                       |                          |               |                        |
| <b>Question 4:</b> What is a se                        | et of firewall                        | rules which allow        | ws only Em    | nail traffic to come i |
| and go out?  |                                       |                          | ·             |                        |
| The 1st Rule:  |                                       |                          |               |                        |
| <ul><li>Source IP :</li><li>Destination IP :</li></ul> | Mail                                  | Port :                   | 25            |                        |
| • Destination IP :                                     | Any                                   | Port :                   | *             |                        |
| • Protocol : <u>TCP</u>                                |                                       |                          |               |                        |
|  |                                       |                          |               |                        |
| The 2nd Rule:  |                                       |                          |               |                        |
| <ul><li>Source IP :</li><li>Destination IP :</li></ul> | Mail                                  | Port :                   | 25            |                        |
| • Destination IP :                                     | Any                                   | Port :                   | *             |                        |
| • Protocol : <u>TCP</u>                                |                                       |                          |               |                        |
|  |                                       |                          |               |                        |
| (Combine, "Email in" a                                 | and "Email o                          | ut" rules into <u>Ac</u> | tive Rules    | box, try to play unti  |
| you get success, copy IP                               | , Port and Pro                        | otocol from Firev        | wall1 Rule    | window to your         |
| answer.)   |                                       |                          |               |                        |
|  |                                       |                          |               |                        |
| Question 5:  |                                       |                          |               |                        |
| <ul> <li>Change a sequence</li> </ul>                  | e of Email in                         | and Email out ru         | ıles. After 1 | the change, does the   |
| traffic still flow?                                    | $\underline{Y}$ $(Y/N)$               |                          |               |                        |
| • Why? <u>Emai</u>                                     | l in and Emai                         | 1 out are using sa       | ıme port an   | ıd IP.                 |
|  |                                       |                          |               |                        |
|  |                                       |                          |               |                        |
|  |                                       |                          |               |                        |

## **Question 6:**

| The 1st Rule:          |                  | d traffics?         |      |
|------------------------|------------------|---------------------|------|
| Source IP :            | Anv              | Port:               | *    |
| Destination IP :       |                  |                     |      |
| Protocol:              |                  |                     |      |
| The 2nd Rule:          | <del></del>      |                     |      |
| Source IP :            | Any              | Port :              | *    |
| Destination IP:        |                  |                     | 25   |
| Protocol:              |                  |                     |      |
| The 3rd Rule:          |                  |                     |      |
| Source IP :            | Any              | Port :              | *    |
| Destination IP : _     |                  |                     | 3306 |
| Protocol:              |                  |                     |      |
| The 4th Rule:          |                  |                     |      |
| Source IP :            | Any              | Port : _            | *    |
| Destination IP : _     | VOIP             | Port : <u>382</u>   | 287  |
| Protocol:              |                  |                     |      |
| The 5th Rule:          |                  |                     |      |
| Source IP :            | Any              | Port:               | *    |
| Destination IP : _     |                  | Port :              |      |
| Protocol:              |                  |                     |      |
| The 6th Rule:          |                  |                     |      |
| Source IP :            | Any              | Port :              | *    |
| Destination IP:        |                  | Port :              |      |
|                        |                  |                     |      |
| Protocol:Y             |                  | nd traffics?        |      |
| The 1st Rule:          | anows an outdour | <u>na</u> traffics: |      |
| Source IP:             | DNS              | Port ·              | 53   |
| Destination IP :       |                  |                     |      |
| Protocol:              |                  | 1 010               |      |
| The 2nd Rule:          | <u> </u>         |                     |      |
| Source IP:             | Mail             | Port ·              | 25   |
| Destination IP :       |                  |                     |      |
| Destination in         | -                | 1 01t               |      |
| Protocol ·             | ICP              |                     |      |
| Protocol:              | ICP              |                     |      |
| <u> The 3rd Rule :</u> |                  | Dort ·              | 2206 |
|                        | Database         |                     |      |

| •           | The 4th Rule:  |   |   |  |
|-------------|--|---|---|--|
|             |  | VOIP  | Port :                                    | 38287                                      |
|             | <ul><li>Destination IP :</li></ul>   |   |   |  |
|             | • Protocol: T  |   |   |  |
| •           | The 5th Rule:  |   |   |  |
|             | <ul><li>Source IP :</li></ul>  | Web   | Port :                                    | 80   |
|             | • Destination IP :   | Any   | Port :                                    | *  |
|             | • Protocol:T   |   |   |  |
| •           | The 6th Rule:  |   |   |  |
|             | • Source IP :  | Chat  | Port :                                    | 5222                                       |
|             | • Destination IP :   | Any   | Port :                                    | *  |
|             |  | -   |   |  |
|             |  |   |   |  |
| •           | What is a rule which <u>l</u>  |   |   |  |
|             |  | Deny All  |   |  |
| <b>O</b>    | diam 7.  |   |   |  |
| 1 /1165     | stion 7:   | 10 W.:4- 111 -£                                       | thom                                      |  |
| _           | many rules do we need  |   | ипсии.                                    |  |
| _           | many rules do we need  | i? write down all of                                  |   |  |
| How         | ce IP Port   |   |   | t Protocol                                 |
| How<br>Sour | ce IP Port   |   |   | rt Protocol                                |
| How<br>Sour | ce IP Port  The 1st Rule:  | <b>Destination IP</b>                                 | Por                                       |  |
| How<br>Sour | ce IP Port  The 1st Rule: Source IP:   | <b>Destination IP</b> Any                             | <b>Por</b><br>Port :                      | 80   |
| How<br>Sour | ce IP Port  The 1st Rule: Source IP: Destination IP:   | Destination IP  Any Web                               | <b>Por</b><br>Port :                      | 80   |
| How<br>Sour | ce IP Port  The 1st Rule:  Source IP:  Destination IP:  Protocol:  T   | Destination IP  Any Web                               | <b>Por</b><br>Port :                      | 80   |
| How<br>Sour | The 1st Rule: Source IP: Destination IP: Protocol: The 2nd Rule:   | Destination IP  Any Web                               | Port:<br>Port:                            | <u>80</u><br><u>80</u>                     |
| How<br>Sour | The 1st Rule: Source IP: Destination IP: Protocol: The 2nd Rule: Source IP:  | Any Web CCP Database                                  | Port : Port : Port :                      | 80<br>80<br>3306                           |
| How<br>Sour | The 1st Rule: Source IP: Destination IP: Protocol: The 2nd Rule: Destination IP: Destination IP:   | Any Web CCP Database Any                              | Port : Port : Port :                      | 80<br>80<br>3306                           |
| How<br>Sour | The 1st Rule: Source IP: Destination IP: Protocol: Source IP: Destination IP: Protocol: The 2nd Rule: Destination IP: Protocol:  | Any Web CCP Database Any                              | Port : Port : Port :                      | 80<br>80<br>3306                           |
| How<br>Sour | The 1st Rule: Source IP: Destination IP: Protocol: Source IP: Destination IP: The 2nd Rule: Destination IP: Protocol: The 3rd Rule:  | Any Web CCP Database Any CCP                          | Port: Port: Port: Port:                   | 80<br>80<br>3306<br>3306                   |
| How<br>Sour | The 1st Rule: Source IP: Destination IP: Protocol: Source IP: Destination IP: The 2nd Rule: Destination IP: The 3rd Rule: Source IP: Source IP: Source IP:   | Any Web CCP  Database Any CCP  Any                    | Port : Port : Port : Port : Port :        | 80<br>80<br>3306<br>3306<br>38287          |
| How<br>Sour | The 1st Rule: Source IP: Destination IP: Protocol: The 2nd Rule: Destination IP: Protocol: The 3nd Rule: Protocol: The 3rd Rule: Destination IP: Destination IP:   | Any Web CCP  Database Any CCP  Any VOIP               | Port : Port : Port : Port : Port :        | 80<br>80<br>3306<br>3306                   |
| How<br>Sour | The 1st Rule: Source IP: Destination IP: Protocol: Source IP: Destination IP: Destination IP: Source IP: Protocol: The 3rd Rule: Source IP: Protocol: The 3rd Rule: Protocol:  | Any Web CCP  Database Any CCP  Any VOIP               | Port : Port : Port : Port : Port :        | 80<br>80<br>3306<br>3306<br>38287          |
| How<br>Sour | The 1st Rule: Source IP: Destination IP: Protocol: The 2nd Rule: Destination IP: Protocol: The 3rd Rule: Source IP: Protocol: The 3rd Rule: Protocol: The 3rd Rule: Protocol: The 4th Rule:                                | Any Web CCP  Database Any CCP  Any VOIP               | Port: Port: Port: Port: Port: Port:       | 3306<br>3306<br>3306<br>38287<br>38287     |
| How<br>Sour | The 1st Rule: Source IP: Destination IP: Protocol: Source IP: Destination IP: Destination IP: Protocol: The 3rd Rule: Source IP: Protocol: The 3rd Rule: Source IP: Source IP: Source IP: Source IP: Source IP: Source IP: | Any Web CCP  Database Any CCP  Any VOIP CCP  VOIP     | Port: Port: Port: Port: Port: Port: Port: | 80<br>80<br>3306<br>3306<br>38287<br>38287 |
| How<br>Sour | The 1st Rule: Source IP: Destination IP: Protocol: Source IP: Destination IP: Destination IP: Protocol: The 3rd Rule: Source IP: Protocol: The 3rd Rule: Source IP: Source IP: Source IP: Source IP: Source IP: Source IP: | Any Web CCP  Database Any CCP  Any VOIP CCP  VOIP Any | Port: Port: Port: Port: Port: Port: Port: | 80<br>80<br>3306<br>3306<br>38287<br>38287 |

## 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 <u>in and out</u>, **Firewall 2** allows only **Chat** and **Email** to come <u>in and out</u>.

| Source IP  | Port | Destination | IP Port | Protocol |
|--|------|-------------|---------|----------|
| Firewall 1   |      |             |         |          |
| • The 1st Rule:  |      |             |         |          |
| • Source IP :  | Any  |             | Port :  | *        |
| <ul><li>Source IP :</li><li>Destination IP :</li></ul> |      | DNS         | Port :  | 53       |
| <ul><li>Protocol :</li></ul>                           | UDP  | _           |         |          |
| • The 2nd Rule:  |      |             |         |          |
| <ul><li>Source IP :</li></ul>                          | DNS  |             | Port :  | 53       |
| <ul> <li>Destination IP :</li> </ul>                   | ·    | Any         | Port :  | *        |
| <ul><li>Protocol :</li></ul>                           | UDP  | _           |         |          |
| • The 3rd Rule:  |      |             |         |          |
| <ul><li>Source IP :</li></ul>                          | Any  |             | Port :  | *        |
| <ul> <li>Destination IP :</li> </ul>                   | :    | Chat        | Port :  | 5222     |
| <ul><li>Protocol :</li></ul>                           | TCP  | _           |         |          |
| • The 4th Rule:  |      |             |         |          |
| <ul><li>Source IP :</li></ul>                          | Chat |             |         |          |
| <ul><li>Destination IP :</li></ul>                     | :    | Any         | Port :  | *        |
| <ul><li>Protocol :</li></ul>                           | TCP  | _           |         |          |
| • The 5th Rule:  |      |             |         |          |
| <ul><li>Source IP :</li></ul>                          | Any  |             | Port :  |          |
| <ul><li>Destination IP :</li></ul>                     |      | Mail        | Port :  | 25       |
| <ul><li>Protocol :</li></ul>                           | TCP  | _           |         |          |
| • The 6th Rule:  |      |             |         |          |
| <ul><li>Source IP :</li></ul>                          | Mail |             | Port :  | 25       |
| <ul><li>Destination IP :</li></ul>                     |      |             | Port :  | *        |
| <ul><li>Protocol :</li></ul>                           | TCP  |             |         |          |

## Firewall 2

| • | The 1st Rule:                 |      |      |        |      |  |
|---|-------------------------------|------|------|--------|------|--|
|   | <ul><li>Source IP :</li></ul> | Any  |      | Port : | *    |  |
|   | • Destination IP:             |      | Chat | Port : | 5222 |  |
|   | • Protocol:                   | TCP  | _    |        |      |  |
| • | The 2nd Rule:                 |      |      |        |      |  |
|   | • Source IP :                 | Chat |      | Port : | 5222 |  |
|   | • Destination IP:             |      | Any  |        |      |  |
|   | <ul><li>Protocol :</li></ul>  | TCP  |      |        |      |  |
| • | The 3rd Rule:                 |      |      |        |      |  |
|   | • Source IP :                 | Any  |      | Port:  | *    |  |
|   | • Destination IP:             |      | Mail | Port : | 25   |  |
|   | <ul><li>Protocol :</li></ul>  | TCP  | _    |        |      |  |
| • | The 4th Rule:                 |      |      |        |      |  |
|   | <ul><li>Source IP :</li></ul> | Mail |      | Port : | 25   |  |
|   | • Destination IP:             |      | Any  | Port : | *    |  |
|   | <ul><li>Protocol :</li></ul>  | _ ~- | -    |        |      |  |