ITCS 461 Computer & Communication Security		02/04/2023
ID: 6388014 Name: Waris Damkham	Section:_	
Save this answer sheet as "Lab8-5988xxx-Name.docx" (lasize).	Removing all fi	gures will help reduce the file
Submit this file to the lab folder in mycourse website according	rding to your se	ession.
Lab 8 : Firev	<u>vall</u>	
Follow Lab 8 document (Lab8.pdf) and answer these quest	tions:	
Part I: Without Firewall		
no question in this part		
Part II: With Firewall		
Question 1:		
1) Observe the traffic flowing from the Interne	• •	•
network to the Internet. Is your network cor		, , ,
2) Explain why or why not: There are several in the		_
cloud and various services, including Web,		
Database, which suggest that the network is	communicat	ing with resources
outside of its own local network.  Add some active attacks by clicking on several seve	varal diffaran	t ontions
3) Are these attacks able to get into your netwo		•
4) Do you feel your system is secure? Y		1/11)
5) What's wrong with this scenario? None	_(1/1/)	
Question 2: What is firewall rule which allows on	nly Email trat	ffic to go out ?
• Source IP : Any Port :	•	2110 10 80 000 1
• Destination IP: Any Port:		•
• Protocol : <u>TCP</u>		

(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></ul>	Mail	Port ·	25	
• Protocol : TCP	iviaii	1 OIt .		
• Flotocol. TCI				
(Move "Email out" rul	e to Inactive 1	Rules box. Then	create new firev	vall rule named
"Email in", similar to I				
Email, try until you get			•	
to your answer.)	,	,		
j a a a a a a a a				
<b>Question 4:</b> What is a s	et of firewall	rules which allow	ws only Email t	raffic to come i
and go out?			J	
The 1st Rule:				
• Source IP:	Mail	Port:	25	
<ul><li>Source IP :</li></ul>	Any	Port :	*	
• Protocol: TCP	<u> </u>			
The 2nd Rule:				
• Source IP :	Mail	Port:	25	
<ul><li> Source IP :</li></ul>	Any	Port :	*	
• Protocol : <u>TCP</u>	<b>y</b>			
(Combine, "Email in"	and <b>"Email o</b>	ut" rules into Ac	tive Rules box,	try to play unt
you get success, copy II				
answer.)				Ĭ
,				
<b>Question 5:</b>				
Change a sequence	ce of Email in	and Email out ru	ales. After the c	hange, does the
traffic still flow?	Y = (Y/N)	)		
• Why? Email			ame port and IP	
<u> </u>		<u> </u>	<u>*</u>	

## **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 Sour	ce IP Port			rt Protocol
How Sour	ce IP Port  The 1st Rule:	<b>Destination IP</b>	Por	
How Sour	ce IP Port  The 1st Rule: Source IP:	<b>Destination IP</b> Any	<b>Por</b> Port :	80
How Sour	ce IP Port  The 1st Rule: Source IP: Destination IP:	Destination IP  Any Web	<b>Por</b> Port :	80
How Sour	ce IP Port  The 1st Rule:  Source IP:  Destination IP:  Protocol:  T	Destination IP  Any Web	<b>Por</b> Port :	80
How Sour	The 1st Rule: Source IP: Destination IP: Protocol: The 2nd Rule:	Destination IP  Any Web	Port : Port :	<u>80</u> <u>80</u>
How Sour	The 1st Rule: Source IP: Destination IP: Protocol: The 2nd Rule: Source IP:	Any Web CCP Database	Port : Port : Port :	80 80 3306
How 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 80 3306
How 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 80 3306
How 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 80 3306 3306
How 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 80 3306 3306 38287
How 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 80 3306 3306
How 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 80 3306 3306 38287
How 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 3306 3306 38287 38287
How 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 80 3306 3306 38287 38287
How 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 80 3306 3306 38287 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:					
	<ul><li>Source IP :</li></ul>	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>	_ ~-	-			