NETWORK

&

CYBER SECURITY FUNDAMENTALS LABS

Prepared by : Mohamed Abosehly

LABS

labs are proving the theoretical concepts that have been taught in lectures and enhance the technical skills for learners

HOW TO PREPARE YOUR PC TO DO THE LABS EFFECTIVELY?

1- It is preferred that you do your labs and Assignments in your Virtual Machine not on your original operating systems.

To setup A Virtual Machine on your pc see this course on mahara tech

- *https://maharatech.gov.eg/course/view.php?id=2116*

2- During Testing Don't forget to

a. **Turn off Firewall Both on Client and Server PCs**
b. **Turn off Firewall of any Antivirus Both Client and Server.**
c. **Test Connectivity between Client and Server.**
d. **Do not use Proxy Server on Both Client and Server PCs**

3- After finished your labs don't forget to:

a. **Uninstall the programs you used**
b. **Disabled the accounts you create**
c. **Disables the rules you setup on firewall**
d. **Enable your firewall and antivirus**

Labs

In these labs, you will learn how to Configure TCP/IP Protocols on your pcs (Clients & Servers) and prove the theoretical concepts that have been taught in lectures which will enhance your technical skills

Prepared by: Mohamed Abosehly

Lab 1

❖ Building the network (Configuring your IP address)

- By default the DHCP (distribute IP address to Client) will give your PC an IP address if they are assigned to obtain an IP address automatically.

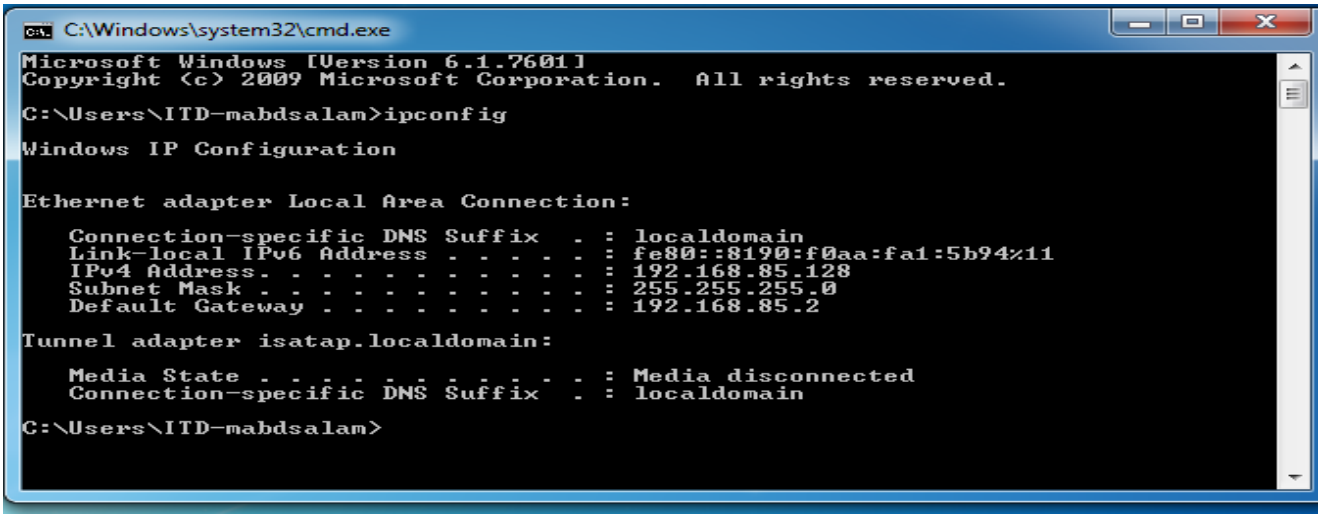
To know your current IP address (logical) use the command:

➢ 1- Ipconfig Command

➢ Ipconfig

Gives details about your network settings

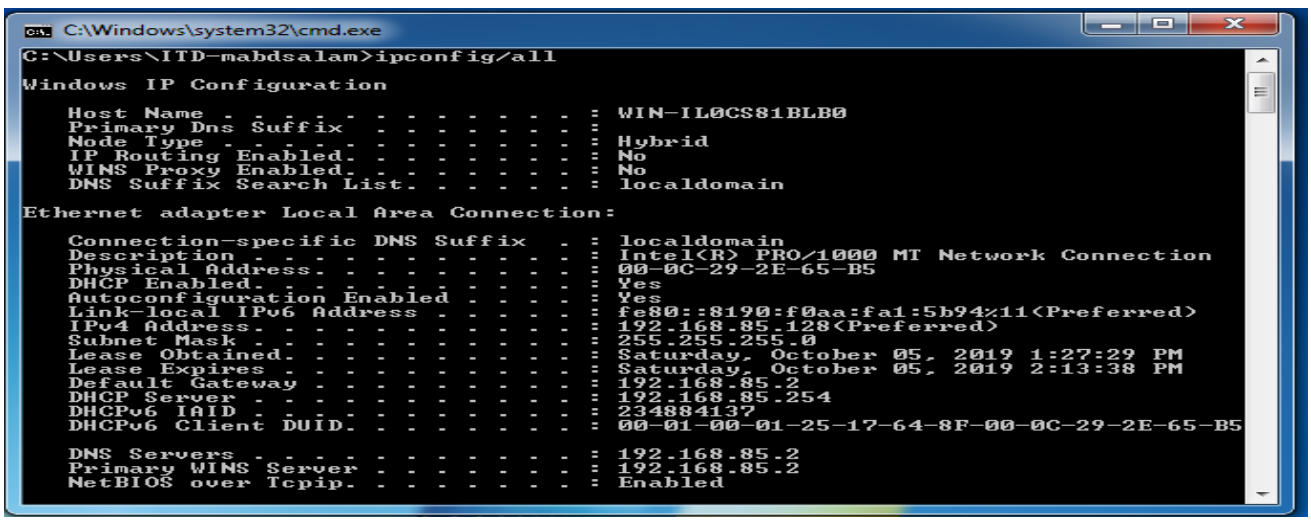
Start →cmd→ipconfig



➢ Ipconfig /all

Gives **more** details about your network settings

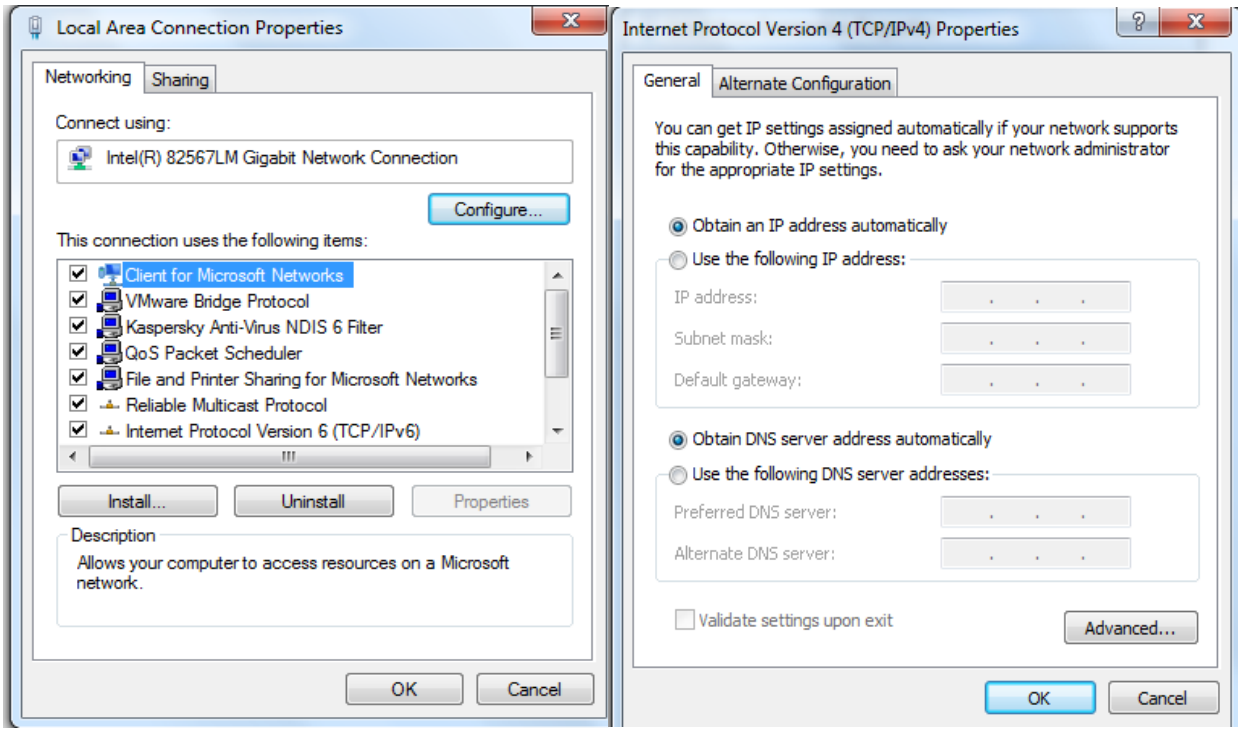
Start →cmd→ipconfig/all

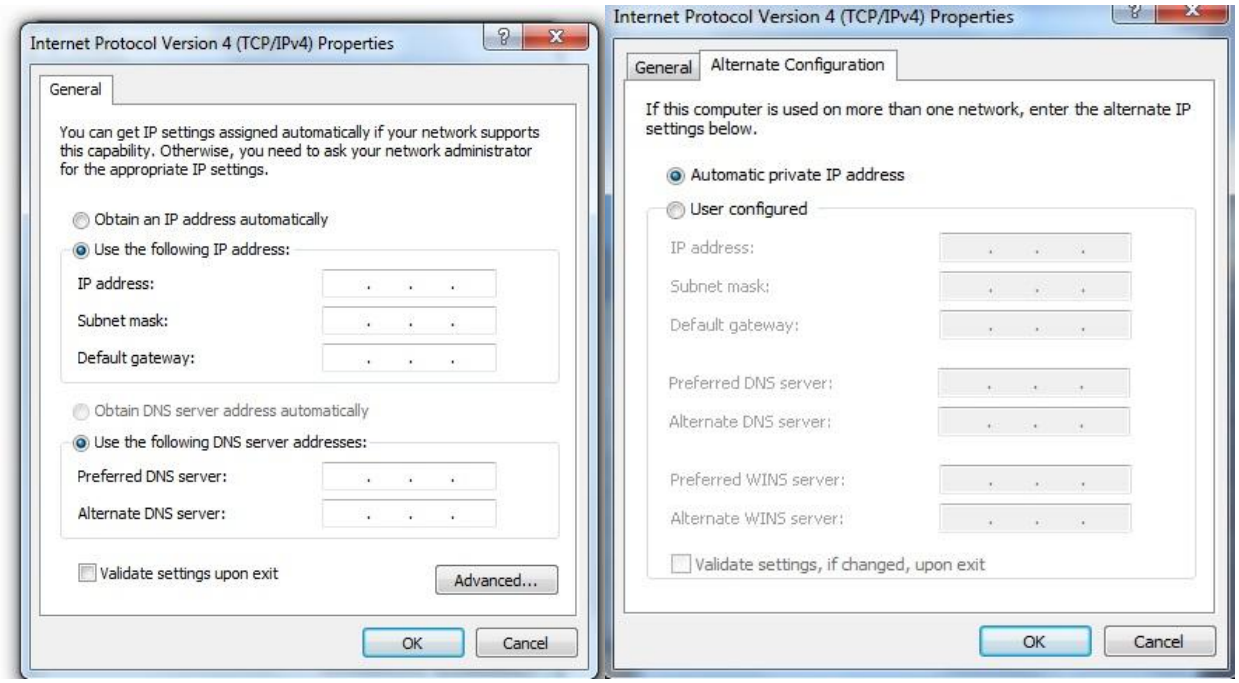


- **ipconfig /release** ---To Release the conflict or faulty IP Address.
- **ipconfig /renew** --- To Request a new IP from a DHCP server
  - IF there is a problem and your pc can't get an IP address you can configure it Manually

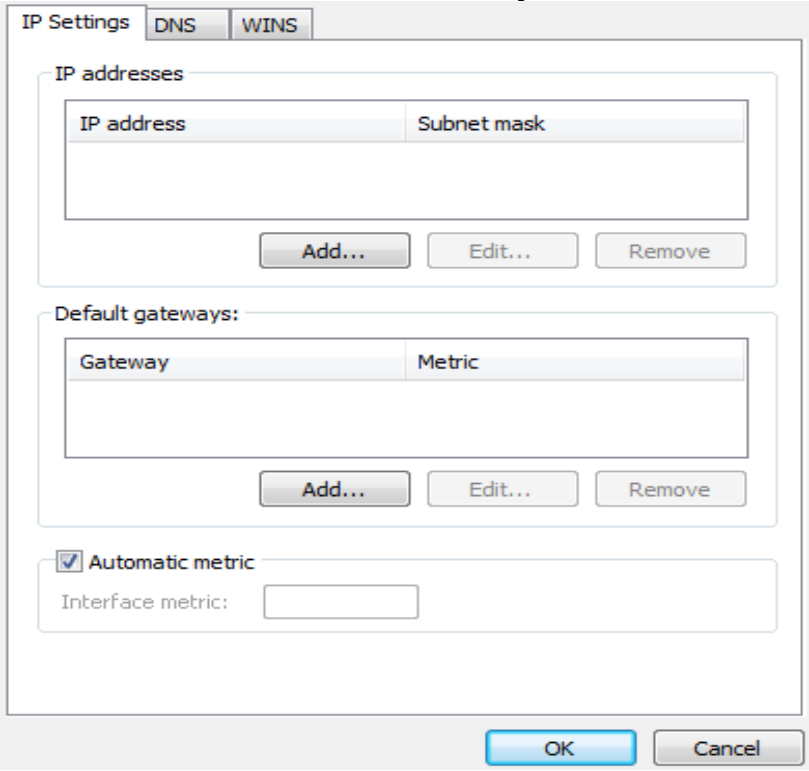
2- Configure IP address manually.

Start →Control panel→Network and Internet→Network and sharing Center → In the Left panel Change Adaptor settings → select Local Area Connection adaptor→ Double click and edit network settings





Click the Advanced button and you can add IP address, Gateway, DNS,..etc

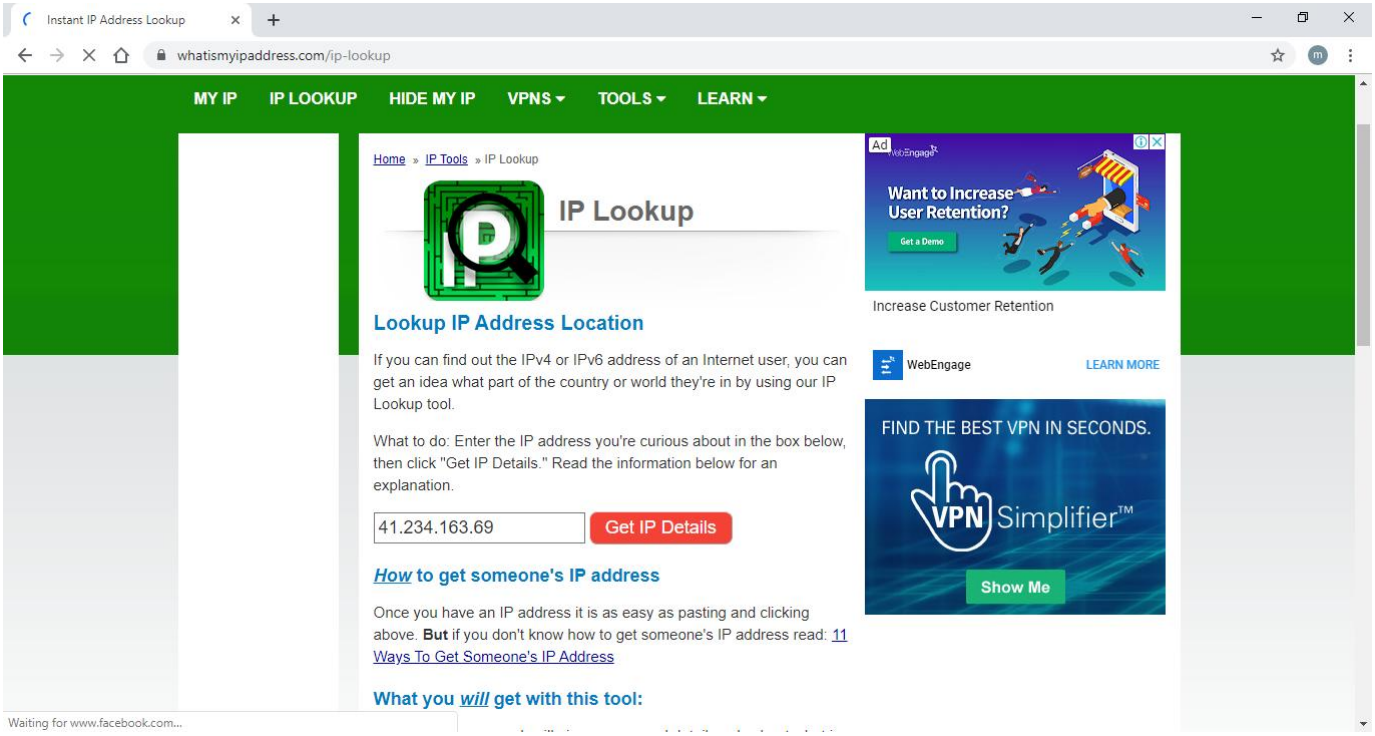


- To check the connectivity between devices use the

To know your Real IP (Static) address

Use website like as :

https://whatismyipaddress.com/



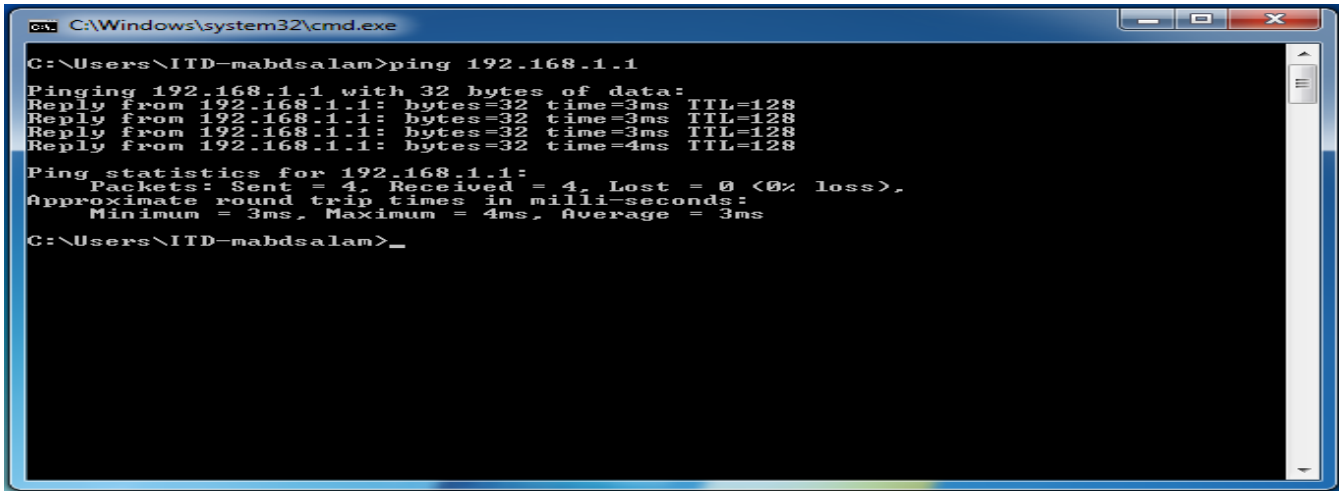
➢ 3- Ping Command

➢ Check the connectivity

Ping *Destination IP Of_Remote_Host*

- **Suppose that the remote host has the ip 192.168.1.1**

C:\>ping 192.168.1.1



➢ Check the Availability of website

C:\>ping Yahoo.com

➢ Continue ping operation unlimited **(just add the switch "-t")**

C:\>ping 192.168.1.1 -t

to exit write: ctrl+c

- **To control the number of pinging packets,**
  (just add the switch "-n" followed by the required packet number (space))

C:\>ping 192.168.1.1 –n 7

- **To control the size of pinging packets,**
  (just add the switch "-l" followed by the required packet size)

C:\>ping 163.121.25.40 -l 2000

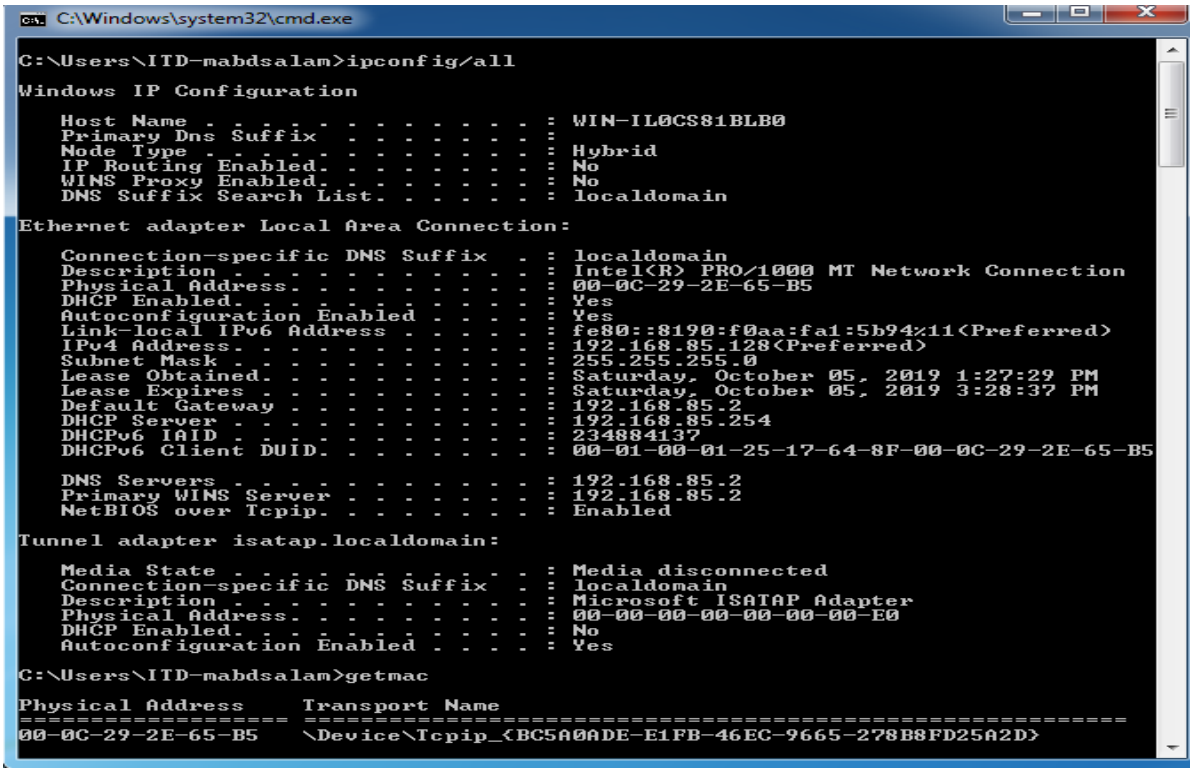
C:\> Ping 163.121.12.40 -l 2000 –n 6

```
Reply from 163.121.12.40: bytes=2000 time=1ms TTL=128
Reply from 163.121.12.40: bytes=2000 time=1ms TTL=128
Reply from 163.121.12.40: bytes=2000 time=1ms TTL=128
Reply from 163.121.12.40: bytes=2000 time=1ms TTL=128
Reply from 163.121.12.40: bytes=2000 time=1ms TTL=128
Reply from 163.121.12.40: bytes=2000 time=1ms TTL=128
```

4- MAC address

to know **your** current MAC (physical) address use the command:

- **Ipconfig /all**
- **Get mac**



- To know **other devices** MAC (physical) address use the **ARP** command:

5- ARP Command

Definition: ARP (Address Resolution Protocol) mapping an Internet Protocol (IP) address to its corresponding physical network address (Mac)

ARP **request** is broadcast; an ARP **reply** is unicast

Run the following command to view the contents of the ARP cache (Run as Admin)

C:\>arp -a

C. To delete the arp cache write the command

C:\>arp –d

6- Opened ports and sessions

netstat (network statistics) is a command-line tool that displays network connections (both incoming and outgoing), routing tables, and a number of network interface statistics. It is available on Unix, Unix-like, and Windows NT-based operating systems.

To know about the concurrent TCP connections on my PC, write the following command

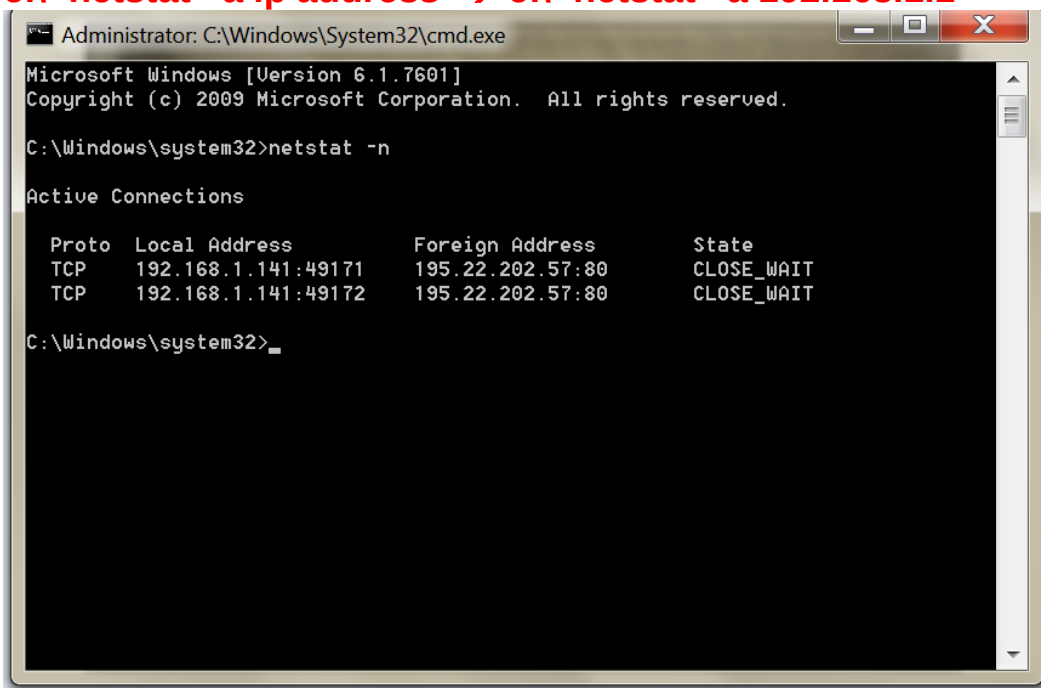
C:\>netstat –n

Displays addresses and port numbers in numerical form.

To know about the concurrent TCP connections on my PC, write the following command

c:\>netstat –n

c:\>netstat –a ip address → c:\>netstat –a 192.168.1.1



7- Domain name System:

Translating human-friendly computer hostnames (URL) into IP addresses.
For example, the domain name
www.example.com
translates to the addresses: *93.184.216.34* (IPv4) and
: *2606:2800:220:1:248:1893:25c8:1946* (IPv6).

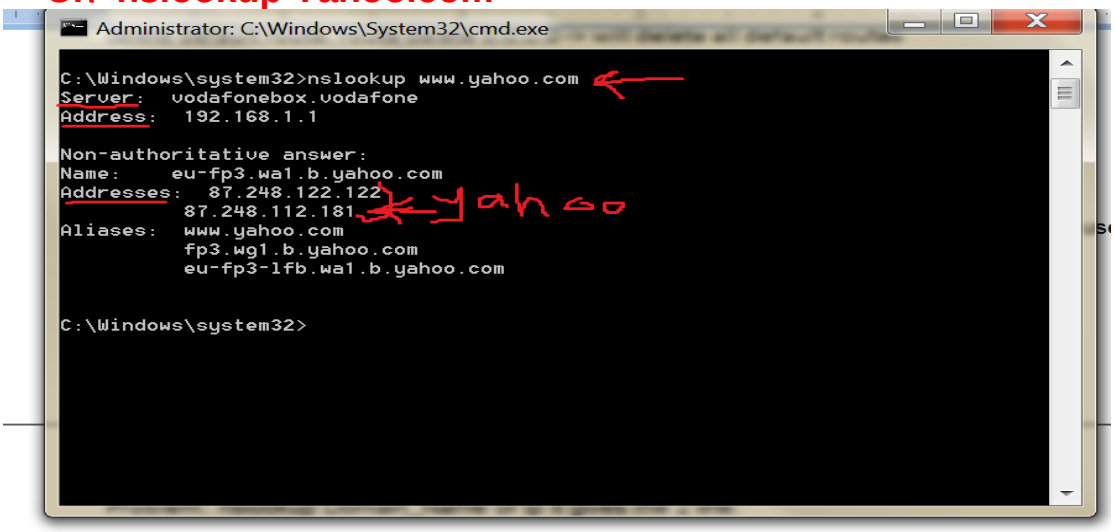
LOCAL DNS ON PC

1) Hosts file C:\Windows\System32\drivers\etc\hosts
2) Hosts file in Linux /etc/hosts

-To know which IP address related to a certain domain name, type the following command;

C:\>nslookup Domain_Name

C:\>nslookup Yahoo.com



server unknown -> it should be DNS Server name but it unknown

address 62.240.110.198 -> DNS Server which used to resolve IP address

-To know which domain name mapped to a certain IP address, type the following command;

C:\>nslookup IP_address

C:\>nslookup 87.248.113.14

C:\>nslookup www.yahoo.com

Server: host-213-131-65-20.static.link.com.eg
Address: 213.131.65.20 >>>> DNS Server which used to resolve IP address

Non-authoritative answer:
Name: www.yahoo-ht3.akadns.net
Address: 87.248.113.14 >>>> yahoo IP Address
Aliases: www.yahoo.com

➢ 8- Dealing with FTP protocol:

We need to have: * **ftp server** *

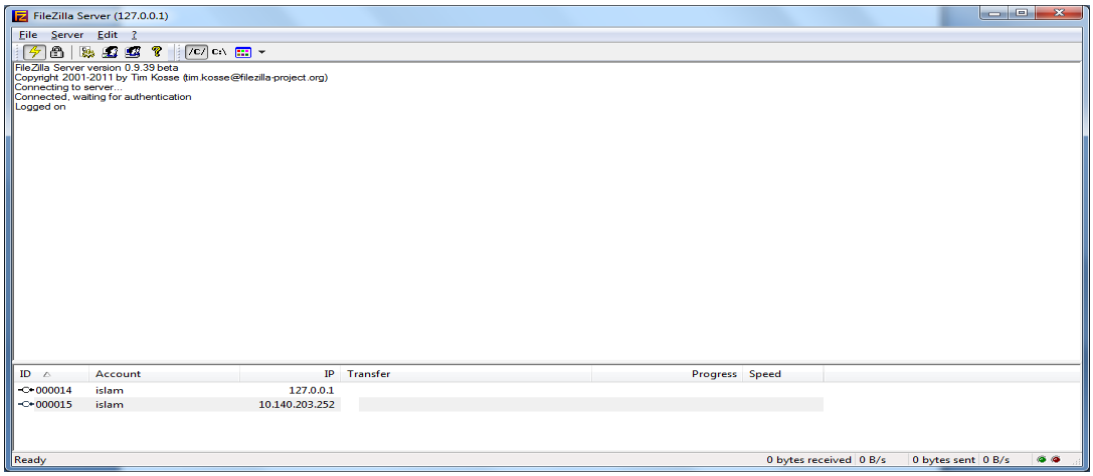
- user account (Authentication)
- home directory
- permission (Authorization)

Steps:

Step 1 : Configure FTP server

1. Install FileZilla ftp server on one machine.

A. Concerning FileZilla ftp server,

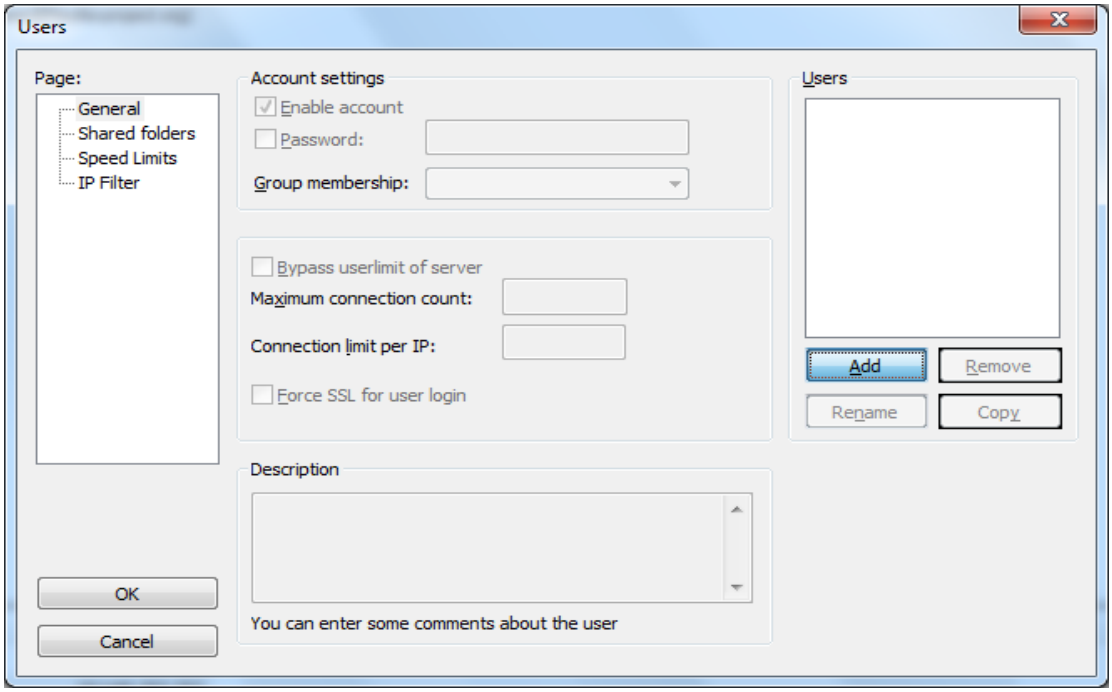


B. We need to add users, who can log on the ftp server remotely, by going to

Edit menu → Users, then click the Add button.

C. Add the user and set the shared folders and permissions.

Then click Ok



Step 2 : Configure FTP Clients

❖ Method 1 (Using URL)

1) Internet explorer (**N.B.: YOU MAY DISABLE THE PROXY)**

ftp:\\IP → ftp:\\192.168.1.1.
ftp:\\IP:port no → ftp:\\192.168.1.1:553

❖ Method 2 (FTP Commands)

Using windows built-in Cmd

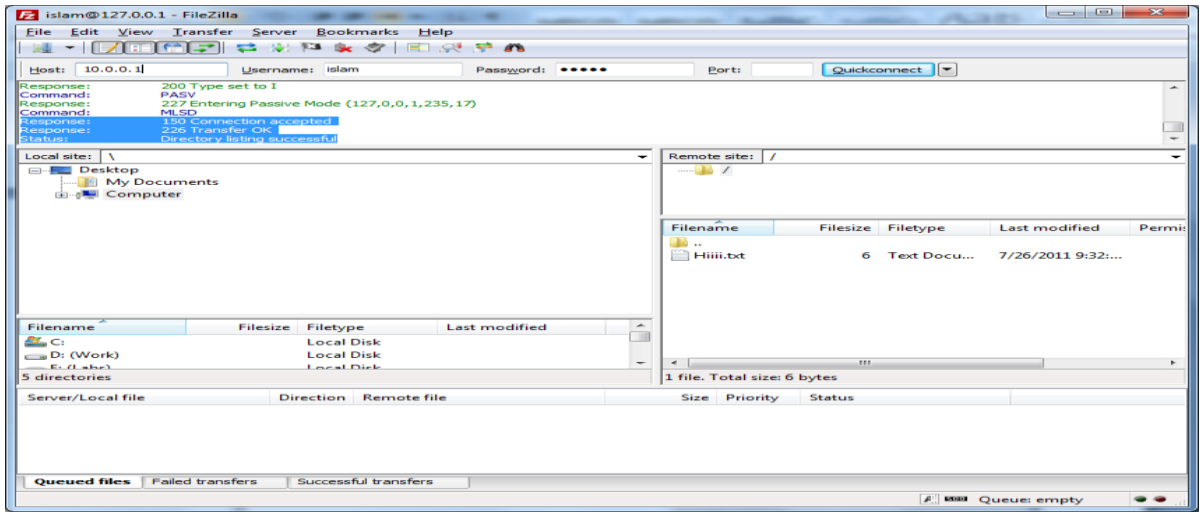
- **ftp >?** /// to see all commands
- **ftp >open ip**

Enter username and password

- **get filename** /// download file& save in the current directory
- **put file name**
- **hash** // to see progress bar during process of download
- **disconnect** //close session
- **bye** // close ftp service

❖ Method 3 (FTP FileZilla Client)

A. First check connectivity between your machine and your colleague's one (using ping)
B. Start the FileZilla ftp server, then go to the Client and run the Filezilla ftp client.
C. Type the IP address of the ftp server host and the username and password allowed to access this ftp server, and then click connect.



9-Using Remote Administration

1) Using Windows Built-in Remote Desktop:

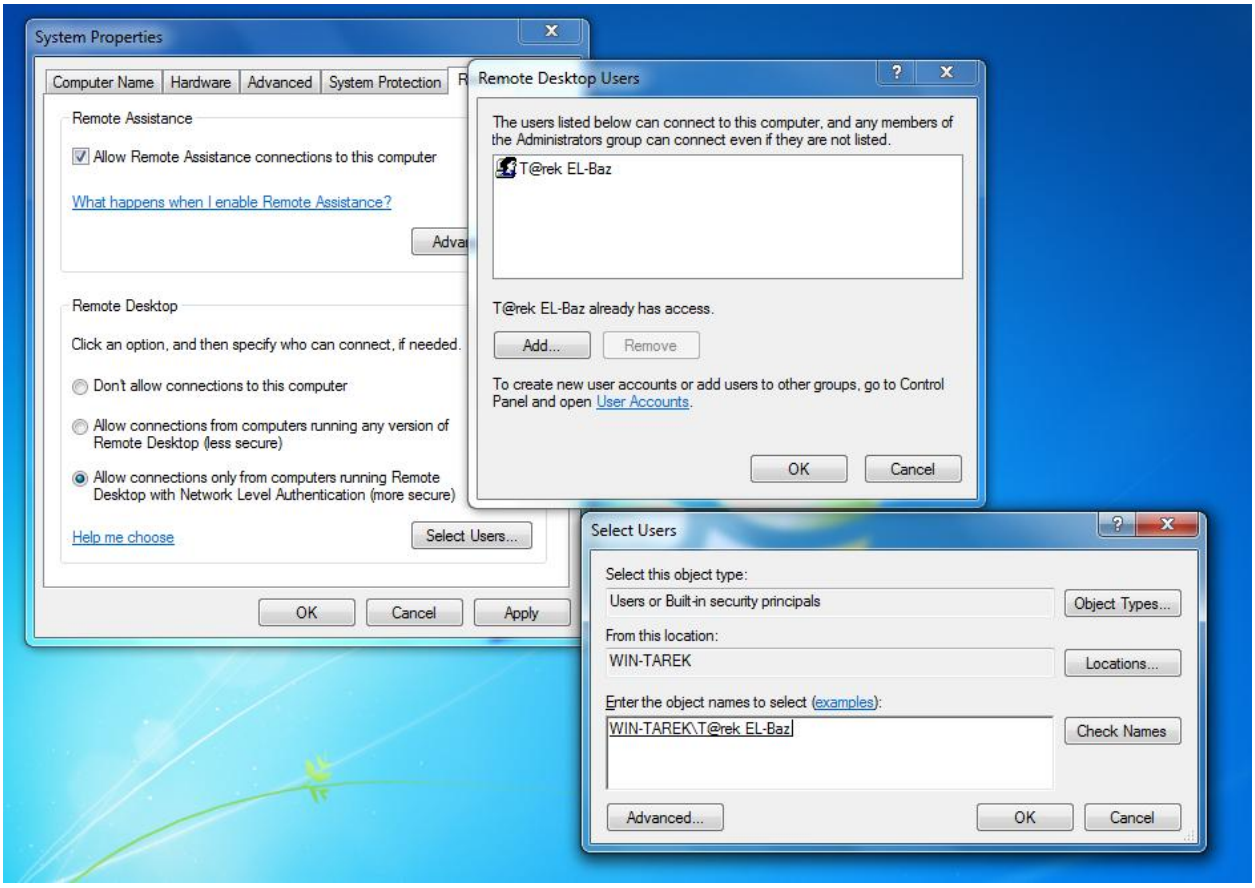
Start → R_Click on my computer → Remote Settings → Remote Desktop

You have 3 optins:

1. Do not allow connections to this computer
2. Allow connections from computers Running any version of remote desktop
3. Allow connections from computers running any version of remote desktop with Network level of authentication.

   You can add any user you want

   N.B: YOU MAY NEED TO ADD THE USER TO THE REMOTE DESKTOP USERS GROUP



➢ 10- Dealing with Electronic Mail Service
○ (mahara tech)

https://maharatech.gov.eg/course/view.php?id=2116

Email can be :

Web based: like yahoo, Hotmail
Access by http ///IE

Mail Client: like r@iti.net.eg
Access by outlook, Thunderbird, incredimail_install

IMAP: Mail stays on server, accessed remotely, normally needs to be deleted manually.

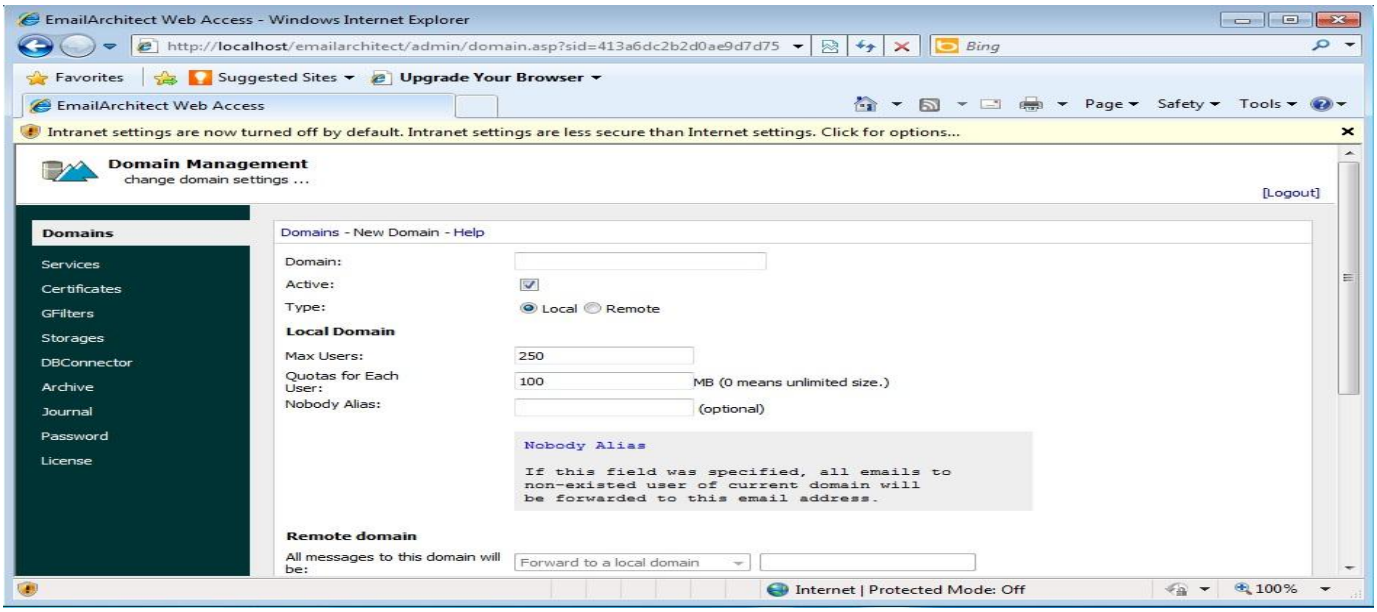
POP3: "Store and Forward" technology, stays on POP3 server until downloaded to client program, then normally auto-deleted from server

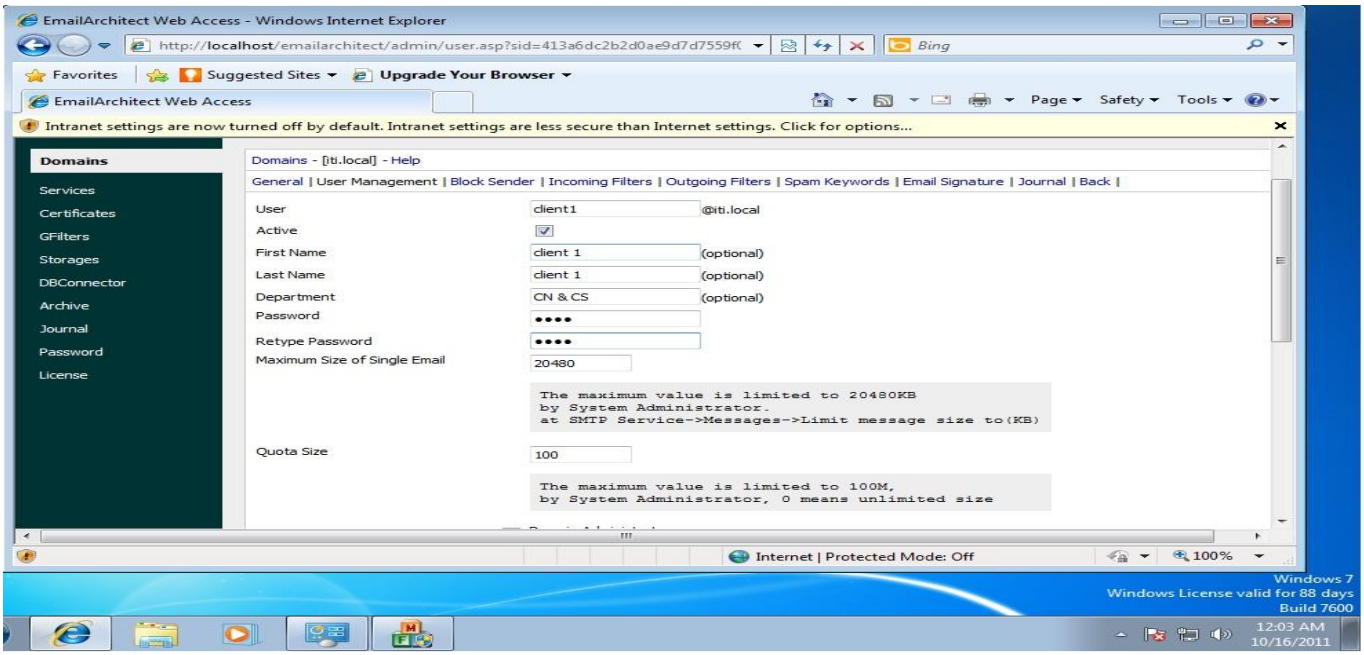
SMTP: used for communication between mail servers,
Client normally sends direct to SMTP server

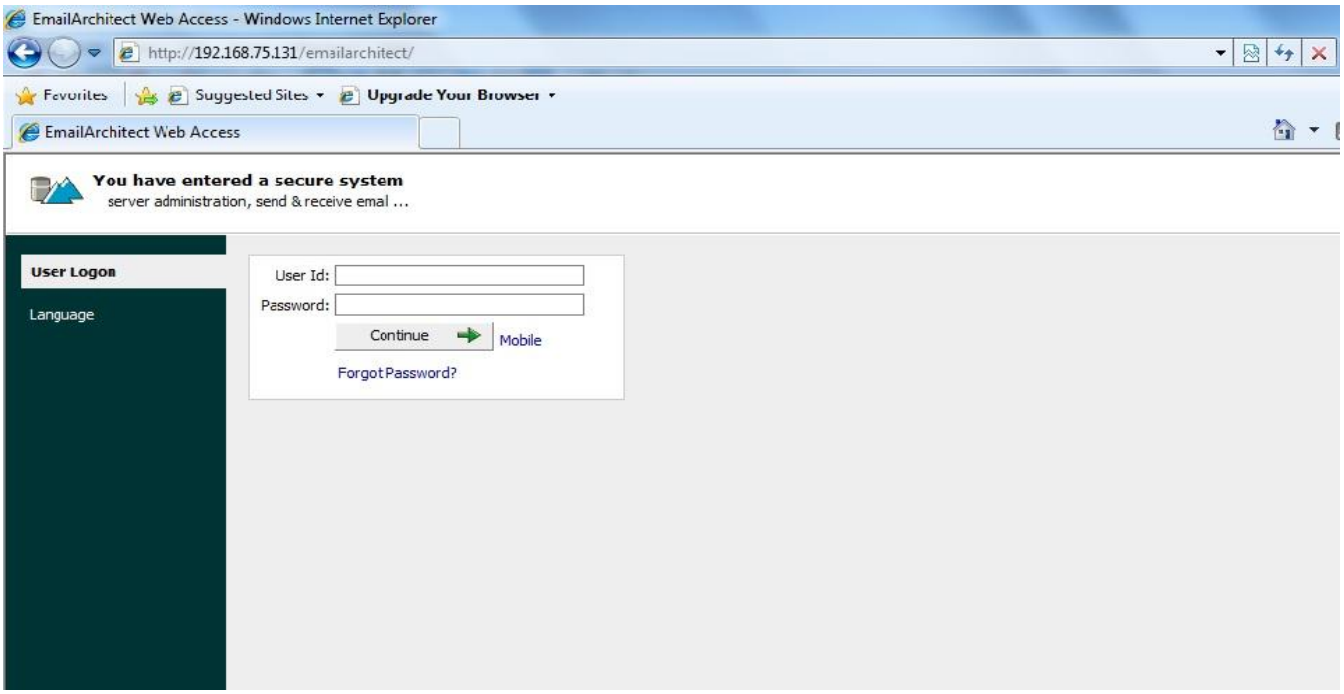
Email Architect Server Software:


EmailArchitect Enterprise Manager
Welcome to Enterprise Manager
Easy to install, light, fast and secure ...
Overview
System Password
Web Access
Server Filters
Documentation
Appendix
EmailArchitect Email Server is a light, fast and secure email server which supports SMTP/ POP3/ SSL/ HTTP/ Webmail protocol. It also supports remote administration and mail access via EmailArchitect Web Access Interface.
Before you start to set up server, we strongly recommend that you read this quick toturial. http://www.emailarchitect.net/emailserver/doc/
EmailArchitect Server Homepage
http://www.emailarchitect.net/emailserver
Copyright © 2004-2010 AdminSystem Software Limited. All rights reserved


EmailArchitect Enterprise Manager
System Password
set the password for built-in account "system" ...
Overview
System Password
Web Access
Server Filters
Documentation
Appendix
"system" is the built-in
full permission to man
account and etc... This
can't send/ receive em
password of "system"
Set the password of "system" account.
After the password is set, you can logon Web Access of EmailArchitect Server to manage services, domains and user accounts.
Set the password of "system" account
New password
Retype password
OK
Cancel


EmailArchitect Web Access - Windows Internet Explorer
http://localhost/emailarchitect/admin/domain.asp?sid=413a6dc2b2d0ae9d7d75
Favorites
Suggested Sites
Upgrade Your Browser
EmailArchitect Web Access
Intranet settings are now turned off by default. Intranet settings are less secure than Internet settings. Click for options...
Domain Management
change domain settings ...
[Logout]
Domains
Services
Certificates
GFilters
Storages
DBConnector
Archive
Journal
Password
License
Domains - New Domain - Help
Domain:
Active:
Type:
Local
Remote
Local Domain
Max Users:
250
Quotas for Each User:
100
MB (0 means unlimited size.)
Nobody Alias:
(optional)
Nobody Alias
If this field was specified, all emails to non-existed user of current domain will be forwarded to this email address.
Remote domain
All messages to this domain will be:
Forward to a local domain
Internet | Protected Mode: Off
100%

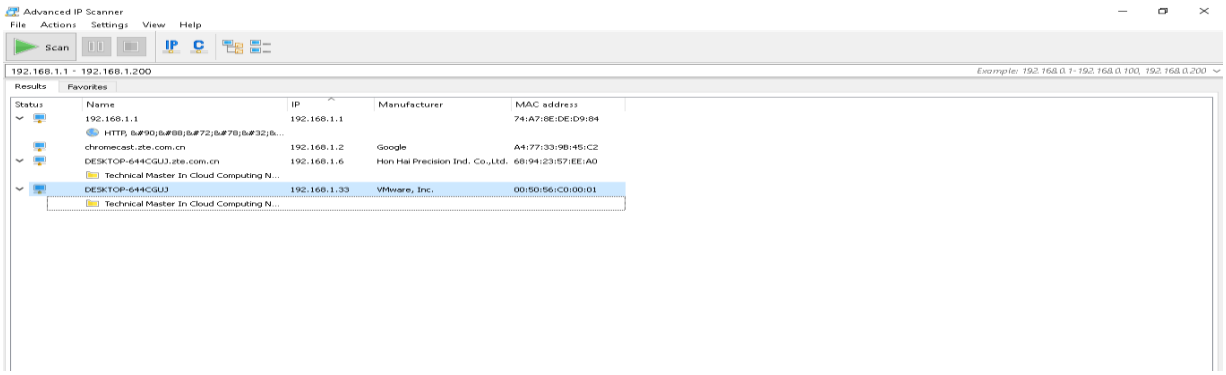

EmailArchitect Web Access - Windows Internet Explorer
http://localhost/emailarchitect/admin/user.asp?sid=413a6dc2b2d0ae9d7d7559f(
Favorites
Suggested Sites
Upgrade Your Browser
EmailArchitect Web Access
Intranet settings are now turned off by default. Intranet settings are less secure than Internet settings. Click for options...
Domains
Services
Certificates
GFilters
Storages
DBConnector
Archive
Journal
Password
License
Domains - [iti.local] - Help
General | User Management | Block Sender | Incoming Filters | Outgoing Filters | Spam Keywords | Email Signature | Journal | Back |
User
client1
@iti.local
Active
First Name
client 1
(optional)
Last Name
client 1
(optional)
Department
CN & CS
(optional)
Password
Retype Password
Maximum Size of Single Email
20480
The maximum value is limited to 20480KB
by System Administrator.
at SMTP Service->Messages->Limit message size to(KB)
Quota Size
100
The maximum value is limited to 100M,
by System Administrator, 0 means unlimited size
Internet | Protected Mode: Off
100%
Windows 7
Windows License valid for 88 days
Build 7600
12:03 AM
10/16/2011


EmailArchitect Web Access - Windows Internet Explorer
http://192.168.75.131/emailarchitect/
Favorites
Suggested Sites
Upgrade Your Browser
EmailArchitect Web Access
You have entered a secure system
server administration, send & receive emal ...
User Logon
Language
User Id:
Password:
Continue
Mobile
Forgot Password?

Lab 2

➢ 8- Port Scanning

You can use any port scanner to scan ports locally or on a remote PC, try using the IP Scanner.

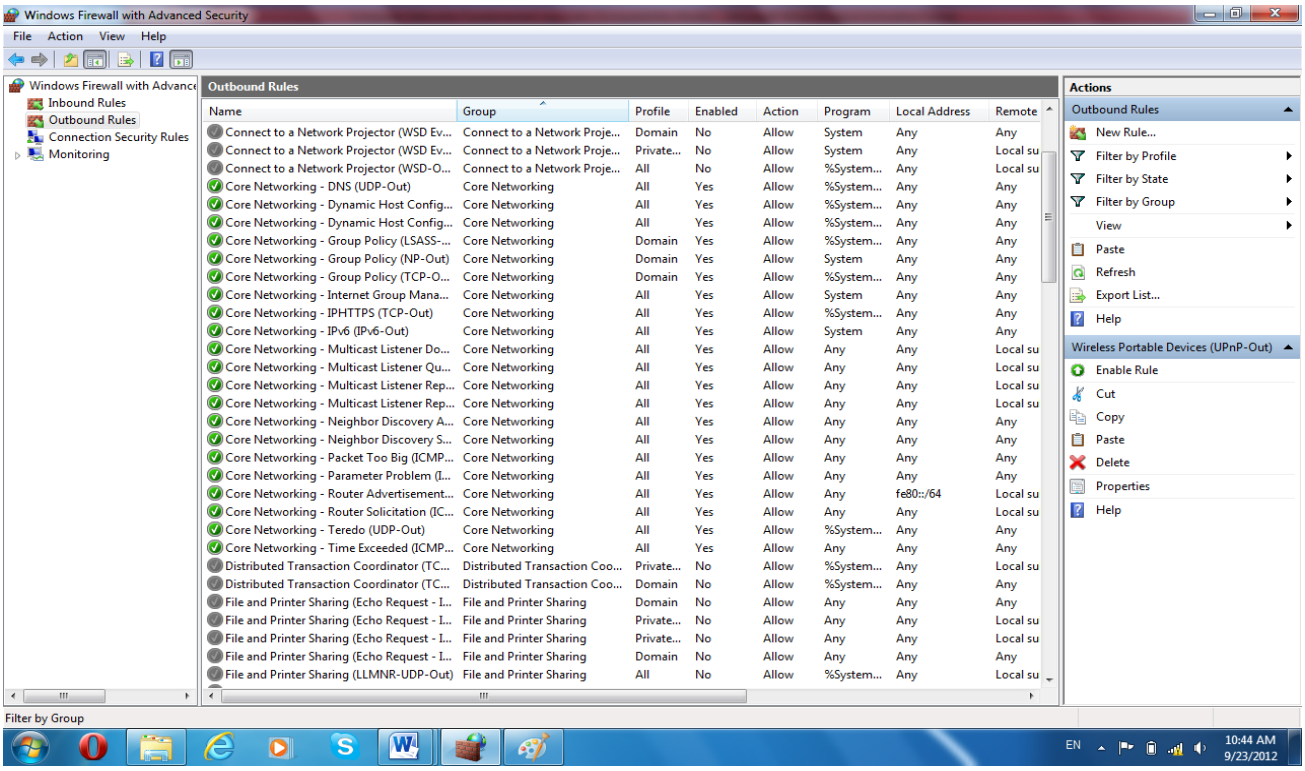


https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

➢ 12- Advanced Firewall Options:

Start → Control Panel →System & Security → Windows Fire →Advanced Settings →on the right panel click on New Rule →Rule Type: Custom → Protocol & Ports →protocol type: ICMPv4 →Custom: Apply to All ICMPV4 →Action: Block This Connection → Name: Block ICMP

From the Remote Machine Try to initiate a ping Request and see the output



- **12- check malicious software**
  - https://www.virustotal.com/gui/home/upload
- **13- check malicious website and links**
  - https://www.virustotal.com/gui/home/url
- **14- check compromised password and data leakages**
  - https://haveibeenpwned.com/

- **15- How to setup a virtual Machine (VM)**
  - **(mahara tech)**
    - https://maharatech.gov.eg/course/view.php?id=2116

Thanks, and best luck

Prepared by: Mohamed Abosehly