

Name: Nooreldeen Ayman Mohammed Elmobashar
Track: Open Source
Branch: ITI Mansoura

1- Ipconfig Command

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.19045.2965]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::8f13:9f7c:6388:b43a%3
IPv4 Address. . . . . : 192.168.122.76
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.122.1

C:\Windows\system32>
```

Ipconfig /all

```
Administrator: Command Prompt
C:\Windows\system32>ipconfig/all

Windows IP Configuration

Host Name . . . . . : DESKTOP-I5OED54
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) 82574L Gigabit Network Connection
Physical Address. . . . . : 52-54-00-25-2D-1A
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::8f13:9f7c:6388:b43a%3(Preferred)
IPv4 Address. . . . . : 192.168.122.76(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Friday, November 15, 1889 10:50:11 PM
Lease Expires . . . . . : Monday, December 22, 2025 8:18:27 PM
Default Gateway . . . . . : 192.168.122.1
DHCP Server . . . . . : 192.168.122.1
DHCPv6 IAID . . . . . : 106058752
DHCPv6 Client DUID. . . . . : 00-01-00-01-30-DB-C2-15-52-54-00-25-2D-1A
DNS Servers . . . . . : 192.168.122.1
NetBIOS over Tcpip. . . . . : Enabled

C:\Windows\system32>
```

➤ ipconfig/release
➤ ipconfig /renew

```
C:\Windows\system32>ipconfig/release

Windows IP Configuration

Ethernet adapter Ethernet:

  Connection-specific DNS Suffix . :
  Link-local IPv6 Address . . . . . : fe80::8f13:9f7c:6388:b43a%3
  Default Gateway . . . . . :

C:\Windows\system32>ipconfig/renew

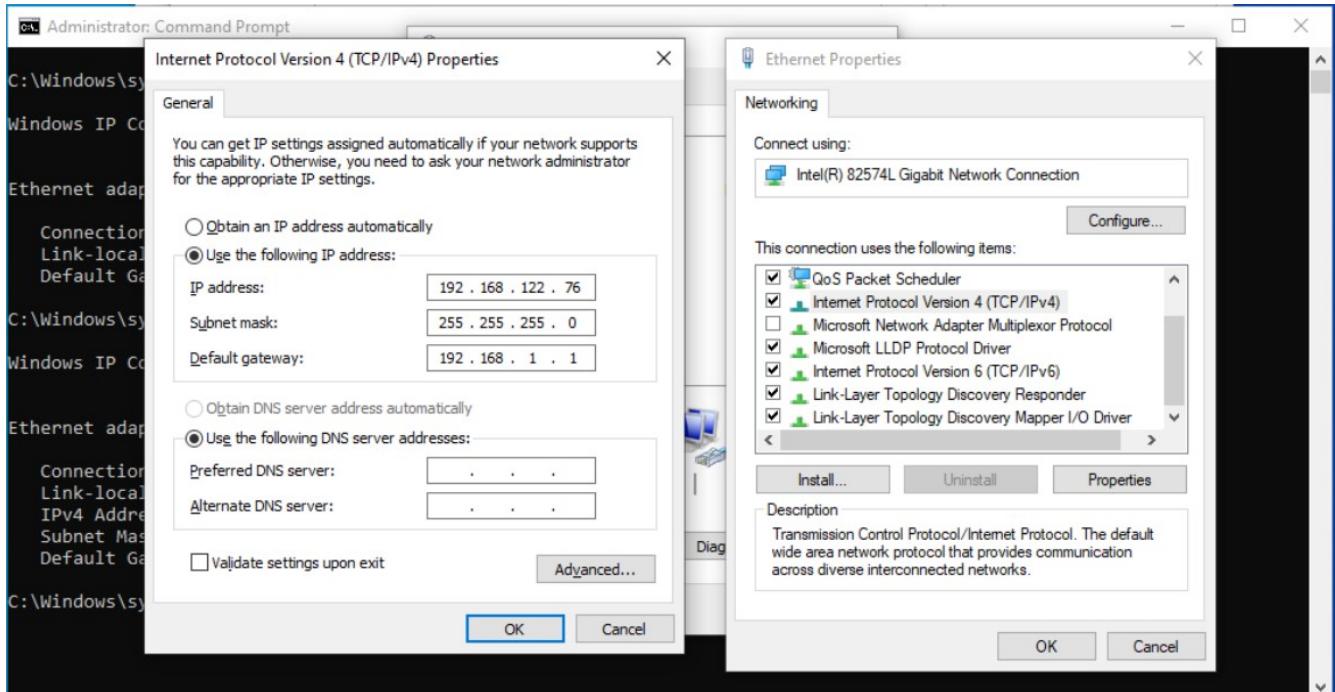
Windows IP Configuration

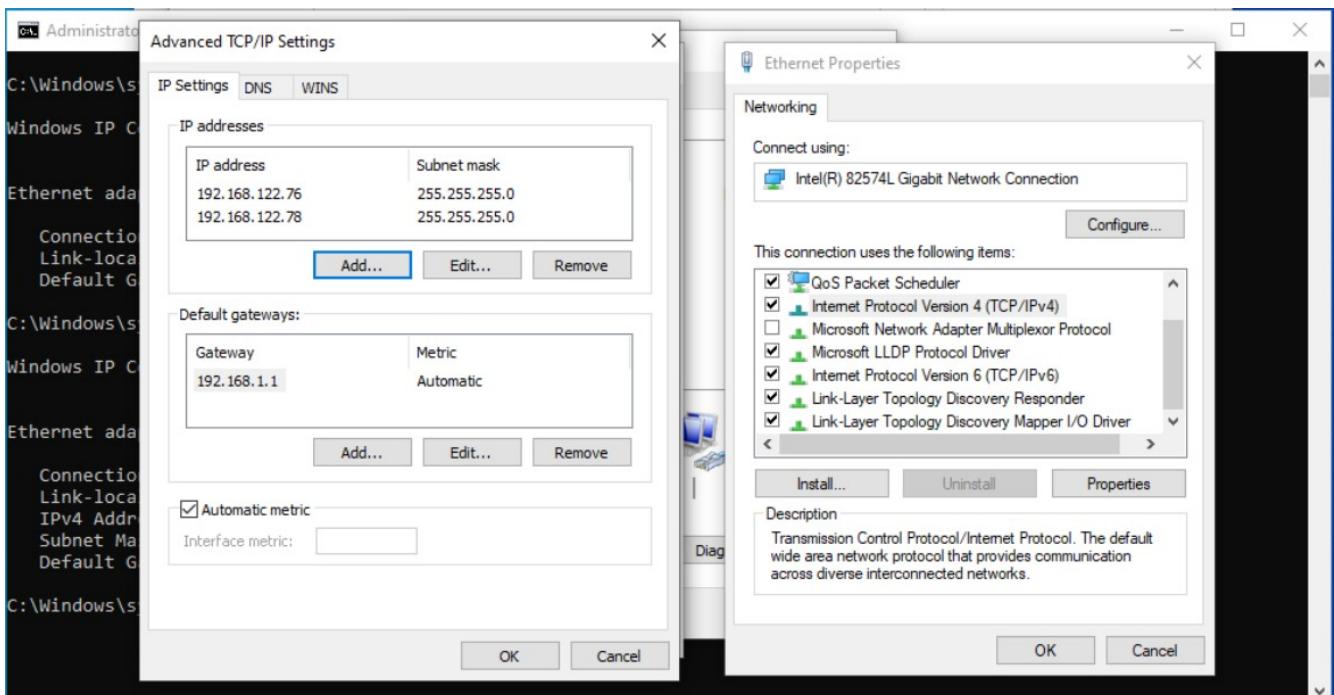
Ethernet adapter Ethernet:

  Connection-specific DNS Suffix . :
  Link-local IPv6 Address . . . . . : fe80::8f13:9f7c:6388:b43a%3
  IPv4 Address. . . . . : 192.168.122.76
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 192.168.122.1

C:\Windows\system32>
```

2- Configure IP address manually.





This screenshot shows the homepage of the Hide My IP website. At the top, there are navigation links: 'MY IP', 'IP LOOKUP', 'HIDE MY IP', 'VPNS ▾', and 'TOOLS ▾'. Below this is a list of services: 'Locate a Phone', 'Find Phone Location', 'Identify Phone Number Owner', 'Best VPN Providers', 'Find Owner of IP Address', and 'See Who Owns This Num'. The main content area displays the user's IP information: 'My IP Address is: IPv4: 197.63.96.251' and 'IPv6: Not detected'. It also shows 'My IP Information: ISP: TE Data, City: Damietta' and a red button 'HIDE MY IP ADDRESS NOW'. To the right, there is a map showing locations like Alexandria, Tanta, and Cairo, with a callout 'Click for more details'.

3- Ping Command

ping 192.168.1.1

```
C:\Windows\system32>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=1ms TTL=63
Reply from 192.168.1.1: bytes=32 time=1ms TTL=63
Reply from 192.168.1.1: bytes=32 time=2ms TTL=63
Reply from 192.168.1.1: bytes=32 time=1ms TTL=63

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\Windows\system32>
```

ping yahoo.com

```
C:\Windows\system32>ping yahoo.com

Pinging yahoo.com [98.137.11.163] with 32 bytes of data:
Reply from 98.137.11.163: bytes=32 time=267ms TTL=47
Reply from 98.137.11.163: bytes=32 time=282ms TTL=47
Reply from 98.137.11.163: bytes=32 time=292ms TTL=47
Reply from 98.137.11.163: bytes=32 time=401ms TTL=47

Ping statistics for 98.137.11.163:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 267ms, Maximum = 401ms, Average = 310ms

C:\Windows\system32>
```

```
ping 192.168.1.1 -t
```

```
C:\Windows\system32>ping 192.168.1.1 -t

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=435ms TTL=63
Reply from 192.168.1.1: bytes=32 time=3ms TTL=63
Reply from 192.168.1.1: bytes=32 time=379ms TTL=63
Reply from 192.168.1.1: bytes=32 time=6ms TTL=63
Reply from 192.168.1.1: bytes=32 time=1ms TTL=63
Reply from 192.168.1.1: bytes=32 time=2ms TTL=63
Reply from 192.168.1.1: bytes=32 time=3ms TTL=63
Reply from 192.168.1.1: bytes=32 time=2ms TTL=63
Reply from 192.168.1.1: bytes=32 time=1ms TTL=63
Reply from 192.168.1.1: bytes=32 time=2ms TTL=63

Ping statistics for 192.168.1.1:
    Packets: Sent = 13, Received = 13, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 435ms, Average = 64ms
Control-C
^C
C:\Windows\system32>
```

```
ping 192.168.1.1 -n 7
```

```
C:\Windows\system32>ping 192.168.1.1 -n 7

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=2ms TTL=63
Reply from 192.168.1.1: bytes=32 time=4ms TTL=63
Reply from 192.168.1.1: bytes=32 time=9ms TTL=63
Reply from 192.168.1.1: bytes=32 time=2ms TTL=63
Reply from 192.168.1.1: bytes=32 time=1ms TTL=63
Reply from 192.168.1.1: bytes=32 time=1ms TTL=63
Reply from 192.168.1.1: bytes=32 time=14ms TTL=63

Ping statistics for 192.168.1.1:
    Packets: Sent = 7, Received = 7, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 14ms, Average = 4ms
C:\Windows\system32>
```

```
Ping 163.121.12.40 -l 2000 -n 6
```

```
C:\Windows\system32>ping 163.121.12.40 -l 2000 -n 6
Pinging 163.121.12.40 with 2000 bytes of data:
Request timed out.

Ping statistics for 163.121.12.40:
  Packets: Sent = 6, Received = 0, Lost = 6 (100% loss),
C:\Windows\system32>
```

4- MAC address

```
C:\Windows\system32>getmac
Physical Address      Transport Name
=====
52-54-00-25-2D-1A    \Device\Tcpip_{0DB0CEE5-4C13-4F0A-9A6B-A6375FBAA1A0}
C:\Windows\system32>
```

5- ARP Command

```
Administrator: Command Prompt  
C:\Windows\system32>arp -a  
  
Interface: 192.168.122.76 --- 0x3  
 Internet Address      Physical Address      Type  
 192.168.122.1          52-54-00-f4-f3-ff    dynamic  
 192.168.122.255        ff-ff-ff-ff-ff-ff    static  
 224.0.0.22              01-00-5e-00-00-16    static  
 224.0.0.251             01-00-5e-00-00-fb    static  
 224.0.0.252             01-00-5e-00-00-fc    static  
 239.255.255.250         01-00-5e-7f-ff-fa    static  
 255.255.255.255         ff-ff-ff-ff-ff-ff    static  
  
C:\Windows\system32>
```

6- Opened ports and sessions

```
Administrator: Command Prompt  
C:\Windows\system32>netstat -n  
  
Active Connections  
  
 Proto  Local Address          Foreign Address          State  
 TCP    192.168.122.76:57715  98.66.133.185:443    ESTABLISHED  
  
C:\Windows\system32>
```

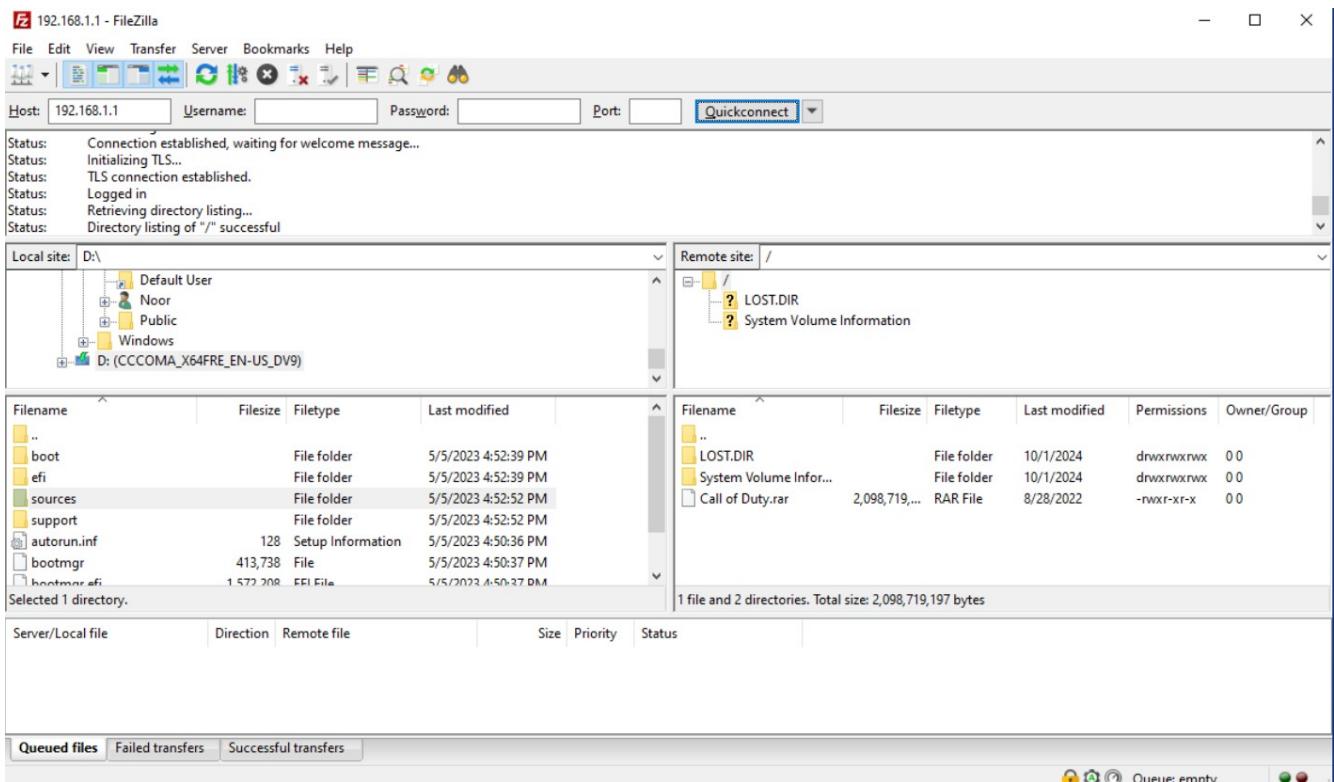
7- Domain name System:

```
C:\Administrator: Command Prompt  
C:\Windows\system32>nslookup google.com  
DNS request timed out.  
    timeout was 2 seconds.  
Server:  UnKnown  
Address: 192.168.122.1  
  
Non-authoritative answer:  
Name:   google.com  
Addresses: 2a00:1450:4006:80e::200e  
          142.250.201.14  
  
C:\Windows\system32>
```

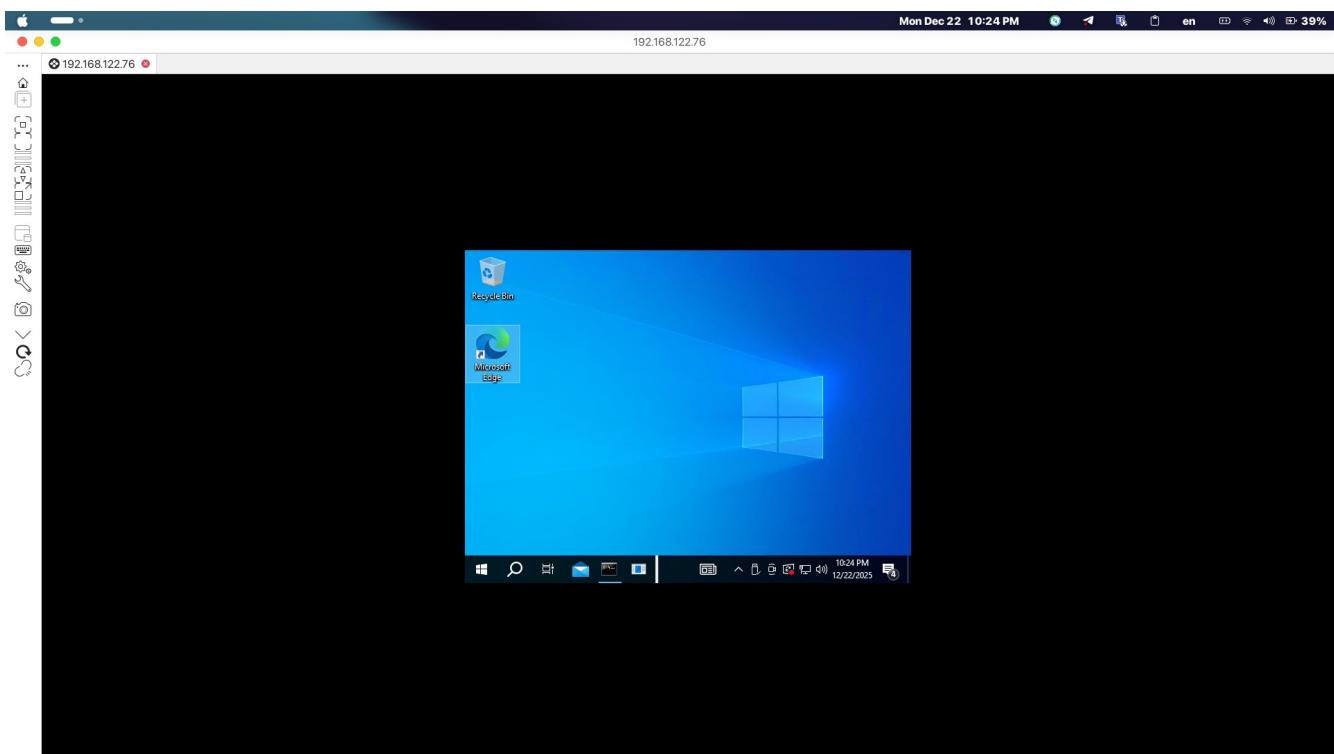
nslookup 87.248.113.14

```
C:\Administrator: Command Prompt  
C:\Windows\system32>nslookup 87.248.113.14  
DNS request timed out.  
    timeout was 2 seconds.  
Server:  UnKnown  
Address: 192.168.122.1  
  
Name:   et23-1.bas1-1-edg.amb.yahoo.com  
Address: 87.248.113.14  
  
C:\Windows\system32>
```

8- Dealing with FTP protocol: Connecting to the FTP server in my router



9-Using Remote Administration



10- Dealing with Electronic Mail Service

The screenshot shows the 'User Logon' page of the EmailArchitect Web Access interface. At the top, a message says 'You have entered a secure system'. Below it, there is a form for entering a User Id ('system') and a Password ('*****'). There are 'Continue' and 'Mobile' buttons, and a 'Forgot Password?' link. On the left, a sidebar lists 'User Logon' and 'Language'. The status bar at the bottom indicates 'Internet Explorer 11 is now out of support. Switch to Microsoft's recommended browser - the faster, more secure Microsoft Edge.' The taskbar shows the date and time as 12/22/2025 at 10:39 PM.

The screenshot shows the 'Domain Management' page for the domain '[it.local]'. The left sidebar includes options like 'Domains', 'Services', 'Certificates', 'GFilters', 'Storages', 'DBConnector', 'Archive', 'Journal', 'Password', and 'License'. The main content area shows the domain settings for '[it.local]'. It includes fields for 'Active' status (checked), 'DNS Check' (checkbox checked), 'Type' (radio buttons for 'Local' and 'Remote' selected 'Local'), 'Max Users' (set to 250), 'Quotas for Each User' (set to 100 MB), and a 'Nobody Alias' field. A note states: 'If this field was specified, all emails to non-existed user of current domain will be forwarded to this email address.' Below this is a 'Remote domain' section with a dropdown menu set to 'Forward to a local domain'. Sub-options include 'Forward to a local domain', 'Forward to an email address', and 'Forward to a remote host'. A note for 'Forward to a local domain' says: 'All email to this domain will be forwarded to the same user of specified local domain.' A note for 'Forward to an email address' says: 'All email to this domain will be forwarded to the specified email address.' A note for 'Forward to a remote host' says: 'All email to this domain will be relayed to...' A confirmation dialog at the bottom asks 'Do you want AutoComplete to remember web form entries? [Learn about AutoComplete]' with 'Yes' and 'No' buttons. The taskbar shows the date and time as 12/22/2025 at 10:41 PM.

<http://localhost/emailarchitect/admin/user.asp?sid=f663ddb4b942200f790a35e431567b30&action=save>

EmailArchitect Web Access [Logout]

User Management

change user profile ...

Domains - [iti.local] - Help

General | User Management | Block Sender | Incoming Filters | Outgoing Filters | Spam Keywords | Email Signature | Journal | Back |

User: noor@iti.local
Latest Logon: 12/22/2025 10:42:15 PM
Active: Storage Information
Not Default MBX Path:
MBX Path: C:\Program Files (x86)\EmailArchitect\data\iti.local\user\noor\mbx
First Name: noor (optional)
Last Name: elmobashar (optional)
Department: OS (optional)
Password:
If you don't want to change password, do not input any value in 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
 Domain Administrator
Domain Administrator can manage current domain users, block list and filters via Web Access.

Windows Taskbar: Type here to search, 10:42 PM, 12/22/2025

<http://localhost/emailarchitect/mail/mbx.asp?sid=2b962cacdef8cf9ff75a2447e425ac2&mbx=Inbox>

EmailArchitect Web Access [Logout]

Inbox

noor@iti.local - [Help] - [Logout]

Create Email

Inbox

- Sent Items
- Deleted Items
- Drafts
- Junk*

Manage Folder

Find Mail

Contacts

Options

Journal

Inbox

Goto 1 / 1 Page(s)

Date ▾ Size

Delete | Mark as Unread | Block | Goto Inbox

0 message(s) First Prev Next Last

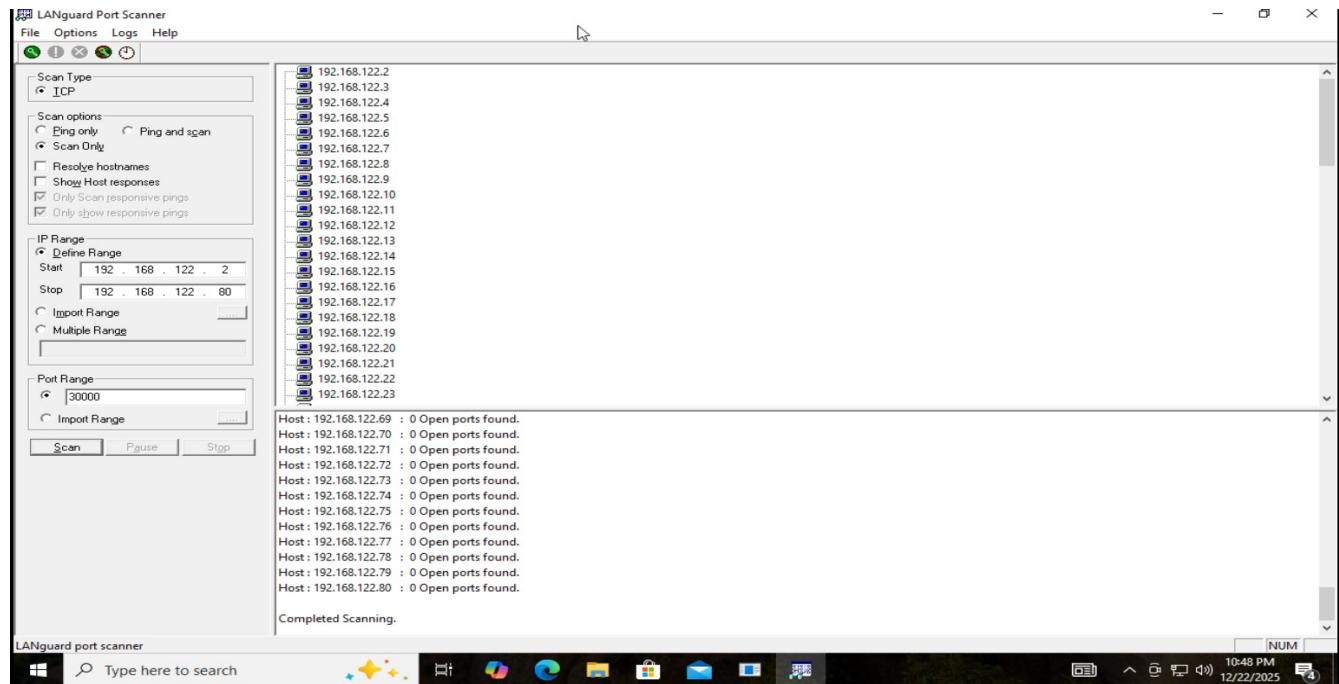
100 M

Would you like to store your password for localhost? [More info](#)

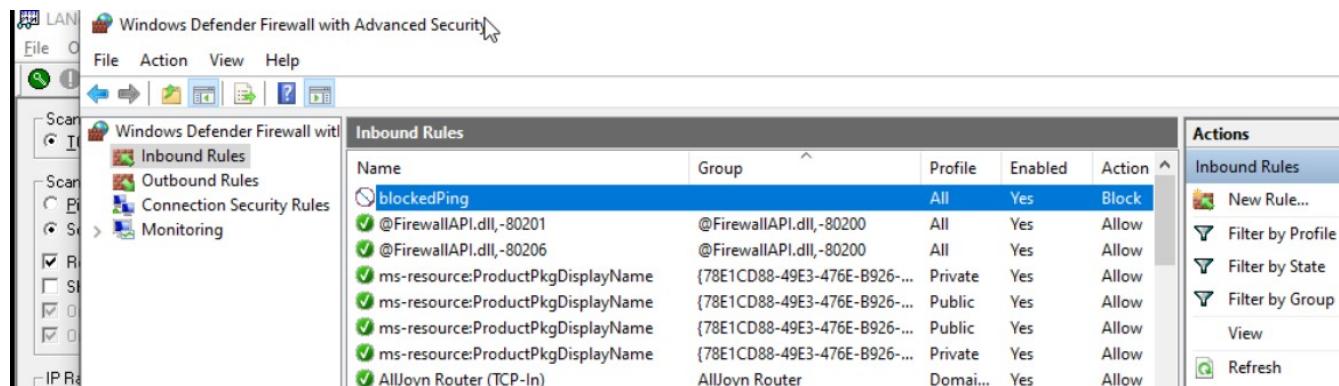
Yes Not for this site

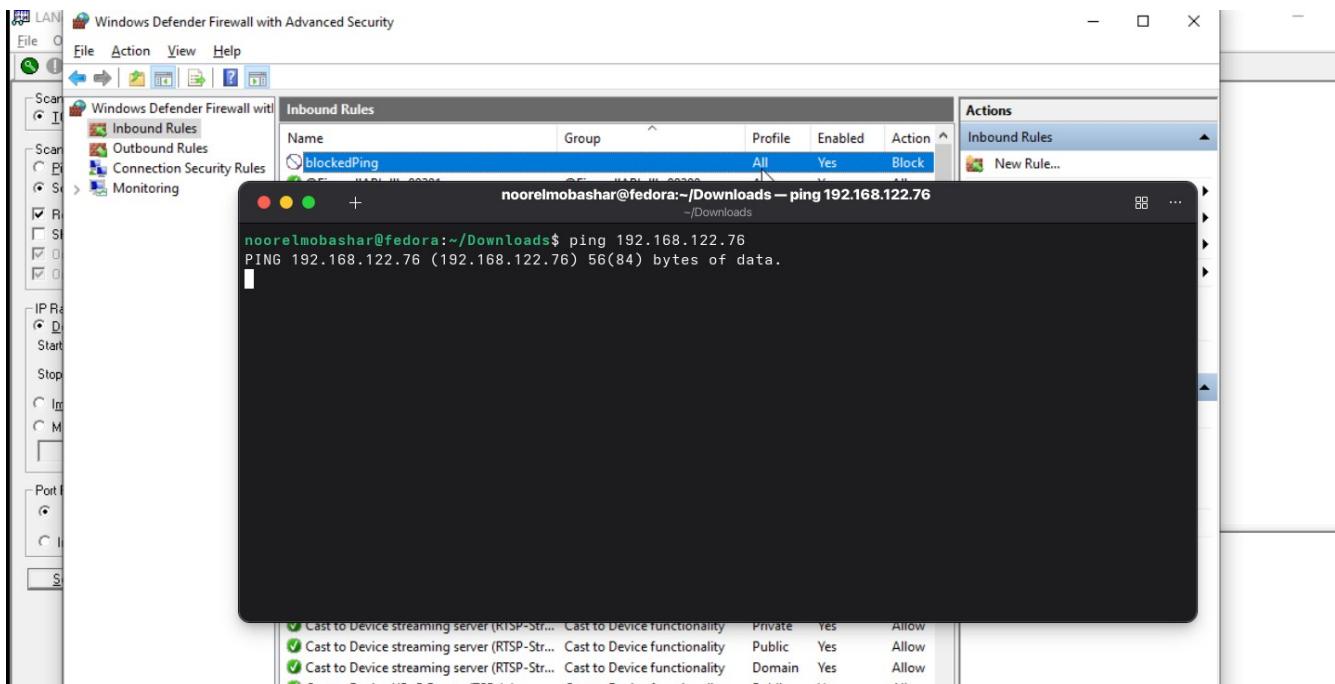
Windows Taskbar: Type here to search, 10:42 PM, 12/22/2025

8- Port Scanning



12- Advanced Firewall Options:





12- check malicious software

The screenshot shows the VirusShare analysis interface for a PDF file. The file name is `e4619cb4532ce7c3c26694ed85ca3ec3a3fb6e6ed8c8b6ba62530da0b6e44164 work_life_balance_presentation (1).pdf`. The analysis results show that no security vendors flagged the file as malicious. The file is 2.70 KB and was last analyzed a moment ago. The 'DETECTION' tab is selected, showing a table of security vendor analysis results:

Security vendor	Result	Analysis Engine	Result
Acronis (Static ML)	Undetected	AhnLab-V3	Undetected
AllCloud	Undetected	ALYac	Undetected
Antiy-AVL	Undetected	Arcabit	Undetected
Arctic Wolf	Undetected	Avast	Undetected
AVG	Undetected	Avira (no cloud)	Undetected
Baidu	Undetected	BitDefender	Undetected
Bkav Pro	Undetected	ClamAV	Undetected
CMC	Undetected	CrowdStrike Falcon	Undetected
CTX	Undetected	Cynet	Undetected

13- check malicious website and links

The screenshot shows a web-based security analysis interface. At the top, there's a navigation bar with a search field containing "http://www.facebook.com/" and a "Sign in" button. Below the search bar is a large green circular icon with a "0" and "/98" text, labeled "Community Score". To the right of this is a status summary: "No security vendors flagged this URL as malicious" with a "Reanalyze" button, "Status 200", "Content type text/html; charset=utf-8", and "Last Analysis Date 4 minutes ago". Below the main header are tabs for "DETECTION", "DETAILS", and "COMMUNITY (27)". A teal banner below the tabs encourages joining the community. The main content area is titled "Crowdsourced context" and includes a legend for threat levels: HIGH 0, MEDIUM 0, LOW 1, INFO 0, and SUCCESS 0. A single threat entry is listed: "Palebot Trojan Harvests Palestinian Online Credentials" from ArcSight Threat Intelligence, marked as LOW 1. It provides a link to the original source: <https://www.virustotal.com/gui/domain/3e723b591bdb95ce8fc9b7032dc572ca97351d0da5efc73459c1fba438e43b/detection>. Below this is a table titled "Security vendors' analysis" showing results for Abusix, ADMINUSLabs, AlienVault, and Antiy-AVL, all of which are marked as "Clean". There's also a "Do you want to automate checks?" button.

14- check compromised password and data leakages

The screenshot shows the HaveIbeenPwned.com website. The main title is "Email Breach History" with a subtitle "Timeline of data breaches affecting your email address". A prominent red box highlights "1 Data Breach" found for the user's email. Below this, a message says "Oh no — pwned! This email address has been found in a data breach. Review the details below to see where your data was exposed." At the bottom left, there's a "Stay Protected" section with a "Notify Me" button. On the right, a circular timeline marker indicates a breach in "Jun 2020". Below the timeline is a detailed breach entry for "Appen". It states: "In June 2020, the AI training data company Appen suffered a data breach exposing the details of almost 5.9 million users which were subsequently sold online. Included in the breach were names, email addresses and passwords stored as bcrypt hashes. Some records also contained phone numbers, employers and IP addresses. The data was provided to HIBP by dehashed.com." A "Compromised data:" link is at the bottom of this entry.