Task-4

Configuring and testing basic firewall rules to allow or block traffic:

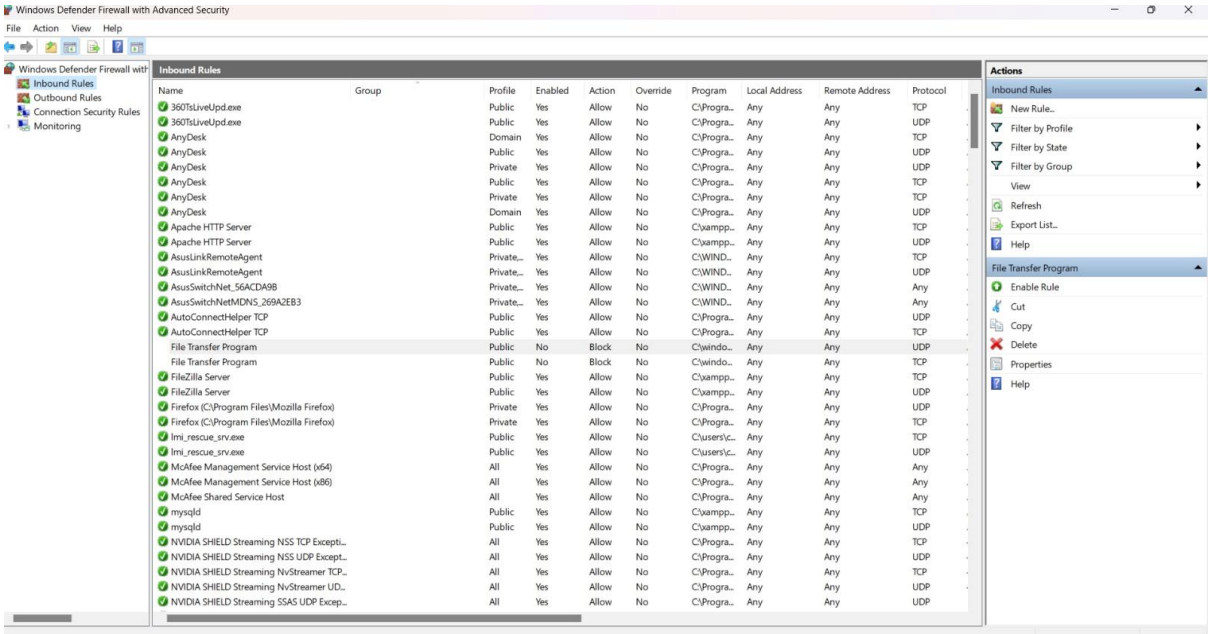
configure basic firewall rules to allow or block traffic and test them on both Windows and Linux systems.

Firewall: A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on pre-defined security rules. It acts as a barrier between a trusted network and untrusted networks, such as the internet. Essentially, it's a gatekeeper that decides which traffic is allowed and which is blocked to protect your computer or network from unauthorized access and malicious activity.

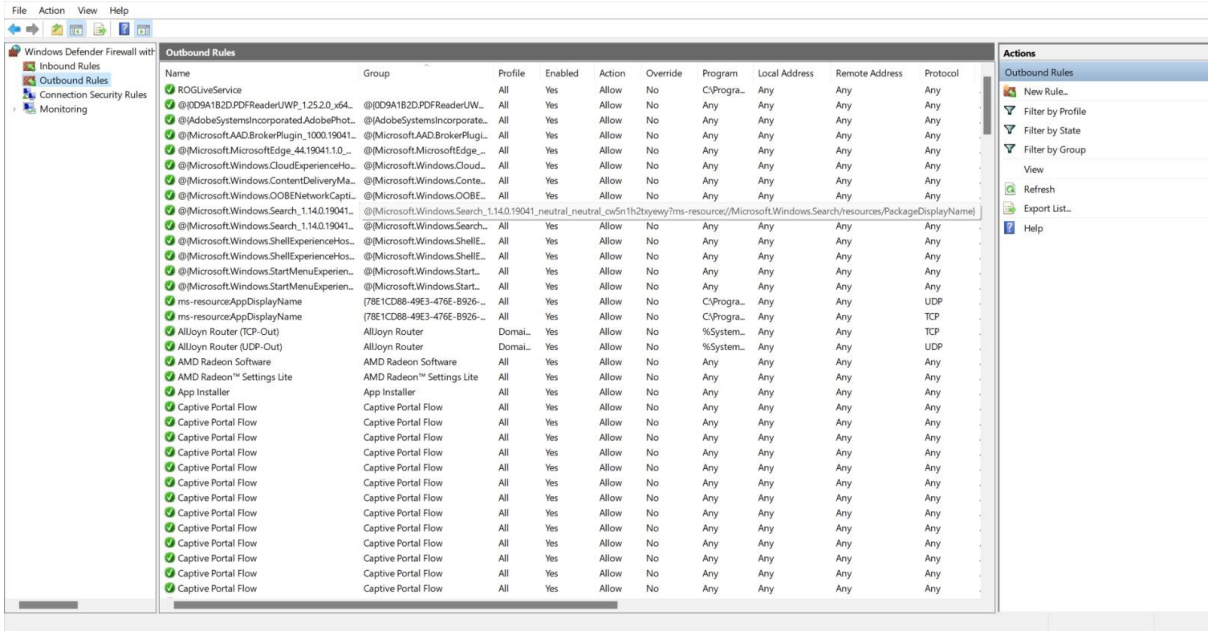
Inbound and Outbound rules: Inbound rules control network traffic coming into a system, while outbound rules manage traffic leaving it. In simpler terms, inbound rules protect your system from external threats by blocking unwanted incoming connections, and outbound rules prevent malicious software from sending data out.

Windows Firewall rules:

Inbound rules:



Outbound rules:



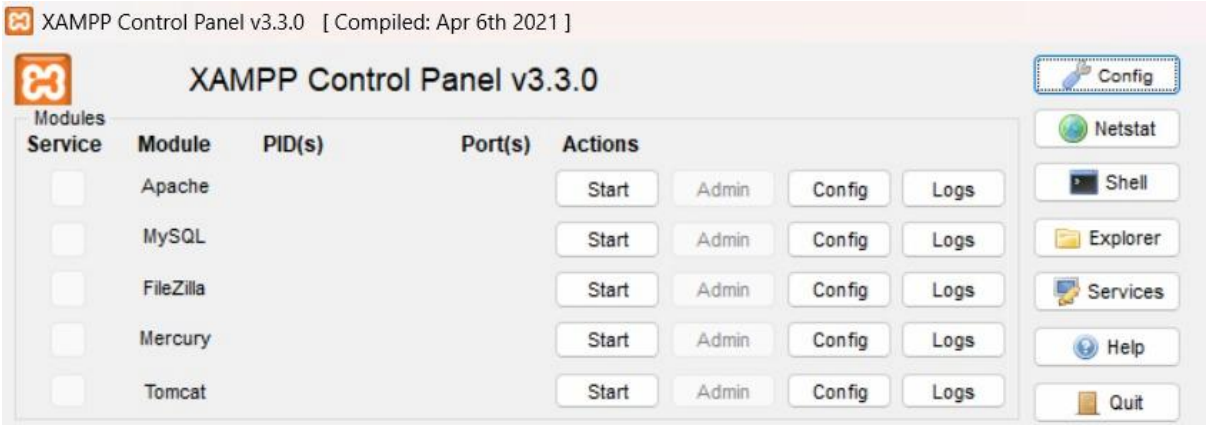
Steps to configure windows firewall rules:

Allow or Block Ports with Windows Defender Firewall:

1. Open Start → Windows Defender Firewall with Advanced Security.
2. Click Inbound Rules → New Rule…
3. Choose Port, then click Next.
4. Choose TCP or UDP, enter the port number(s) you want to allow/block, e.g. 80.
5. Choose Allow the connection or Block the connection, then click Next.
6. Choose when the rule applies (Domain, Private, Public).
7. Name the rule, e.g., Allow HTTP or Block HTTP.
8. Click Finish.

With the help these steps we can configure the inbound and outbound firewall rules to allow and block the traffic.

To Start services like Apache, FTP in windows I have used XAMPP software package.



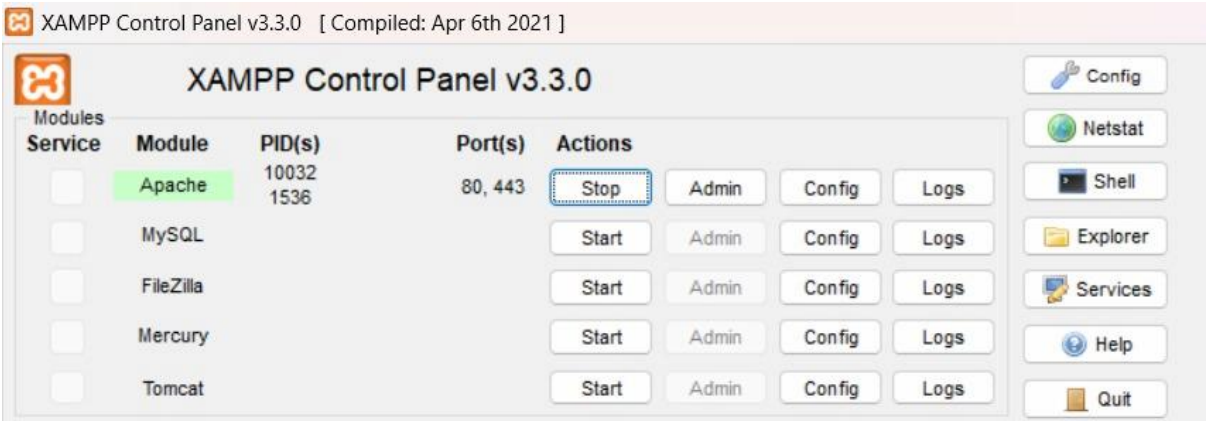
Typical services started by XAMPP:

- Apache → serves HTTP(S) requests on ports 80/443
- MySQL/MariaDB → database server on port 3306
- ProFTPD or FileZilla FTP Server (optional) → provides FTP access on port 21

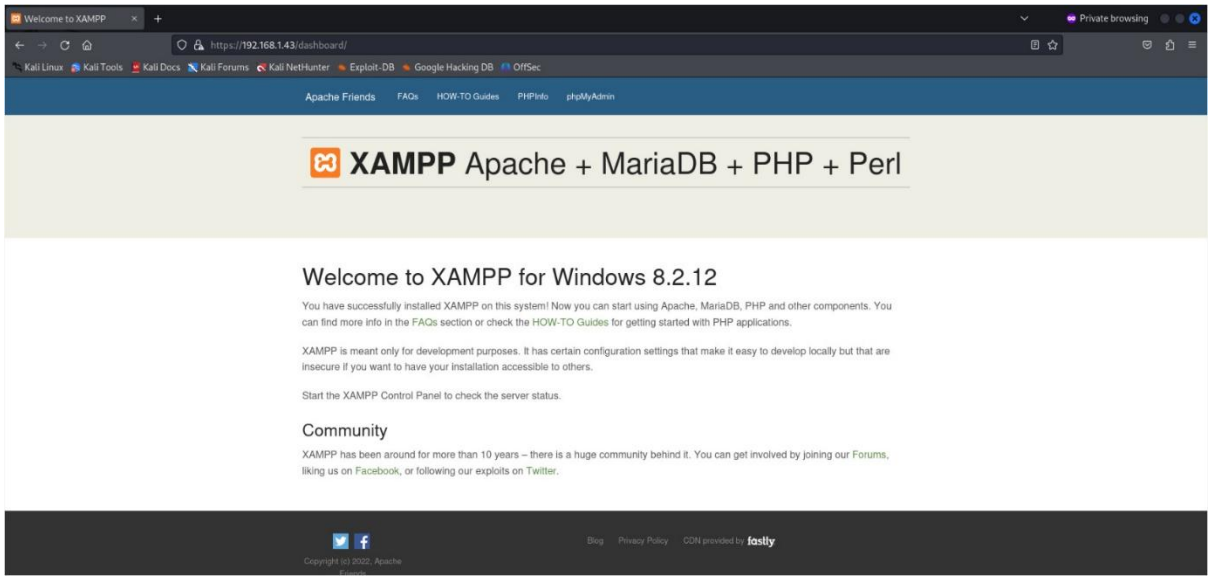
Firewall rules:

**** Before blocking port 80 -(IP address of windows is 192.168.1.43)-**

After starting the Apache service in XAMPP on a Windows system, you can access the XAMPP welcome page from another device — for example, a Linux system — by opening a web browser and typing the Windows system's IP address (e.g., http://192.168.1.43) in the address bar.



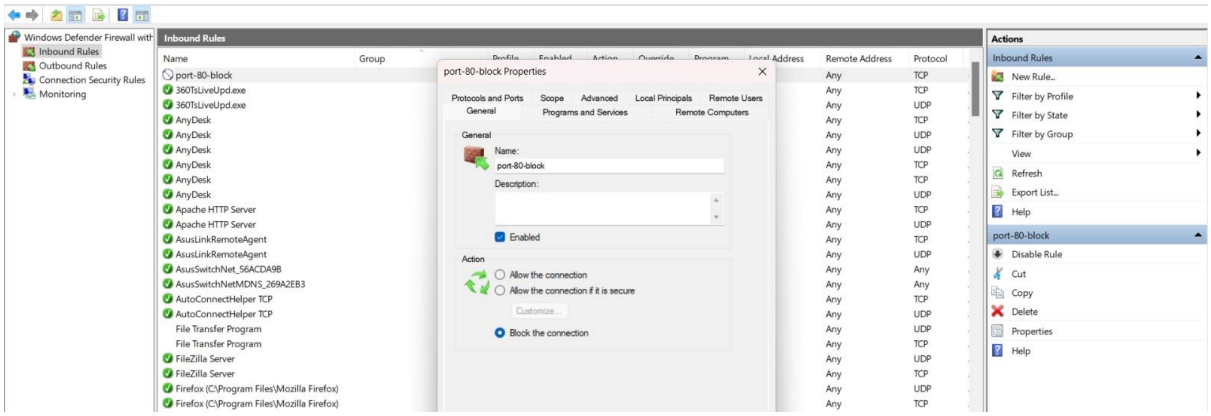
- Starting Apache service-



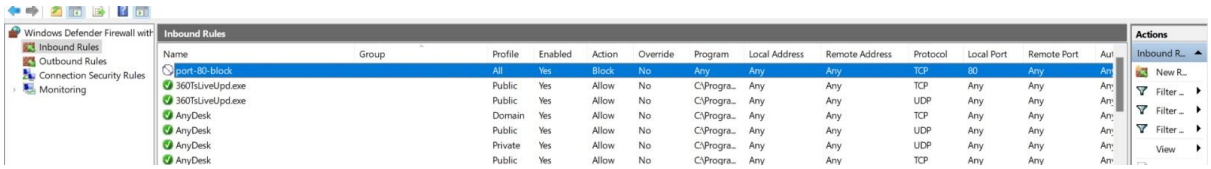
-Accessing the XAMPP welcome page from Linux system-

Configuring rule:

1.Blocking Port 80 (HTTP):

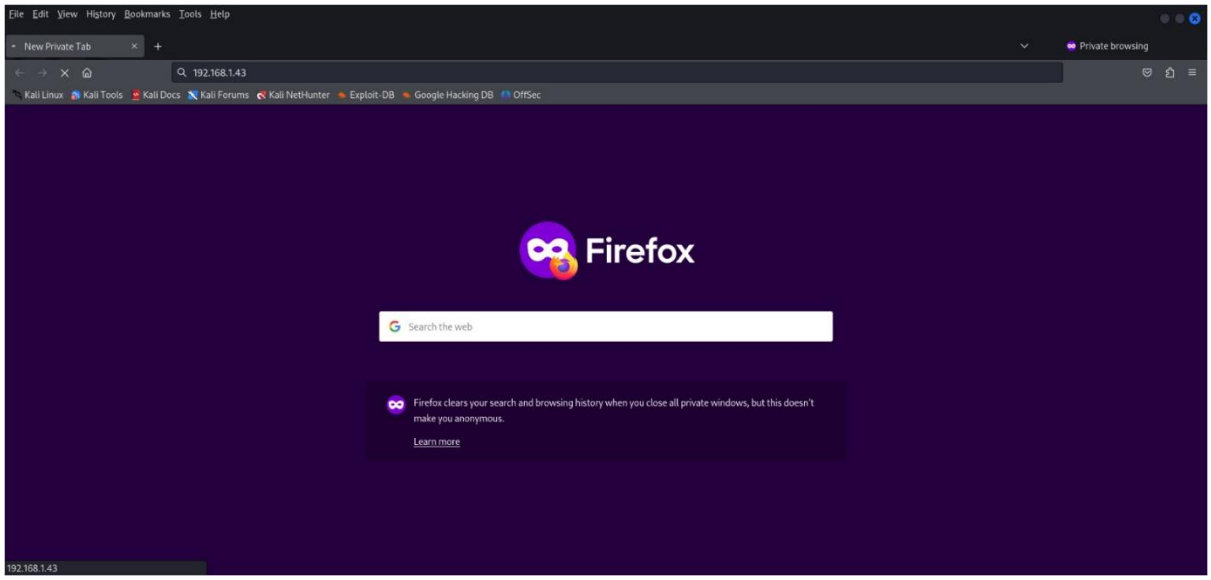


- Configuring rule as Port-80-block-



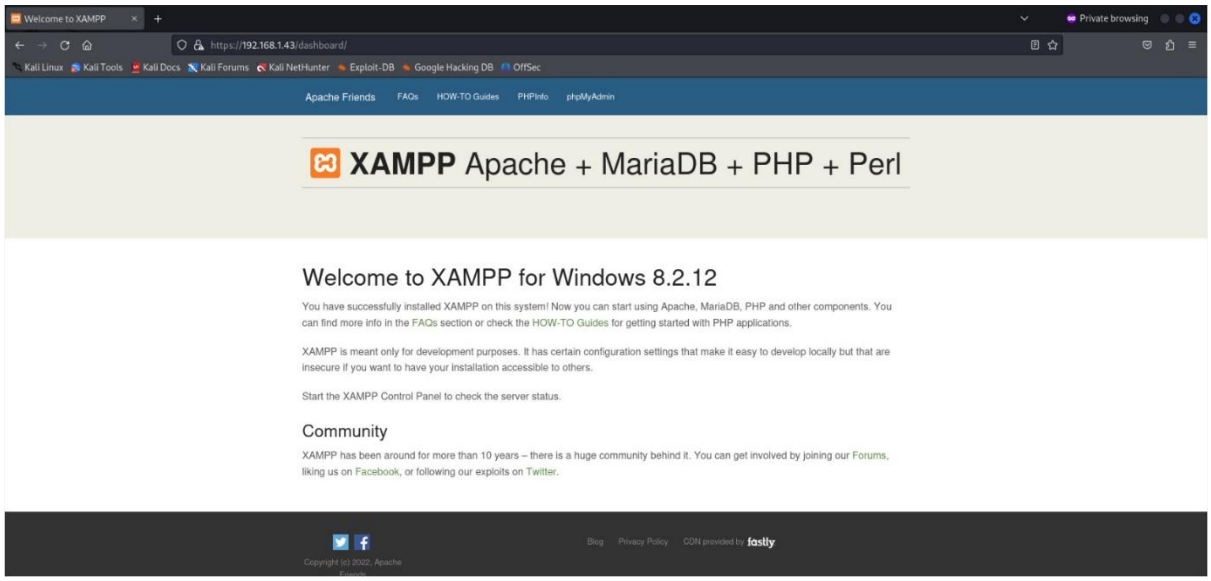
If you block incoming traffic on port 80 (HTTP) with your firewall on the Windows system running XAMPP, devices on the network — like another Linux machine — will not be able to access the XAMPP web page, because the

firewall will reject or drop all requests to port 80, preventing HTTP connections from reaching Apache.



-Not be able to access the XAMPP web page-

If you block only port 80 (HTTP) but leave port 443 (HTTPS) open on the Windows system running XAMPP, devices on the network — like another Linux system — can still access the XAMPP web page using HTTPS by typing https://192.168.1.43 in the browser, because the firewall allows incoming traffic on port 443.



https://192.168.1.43

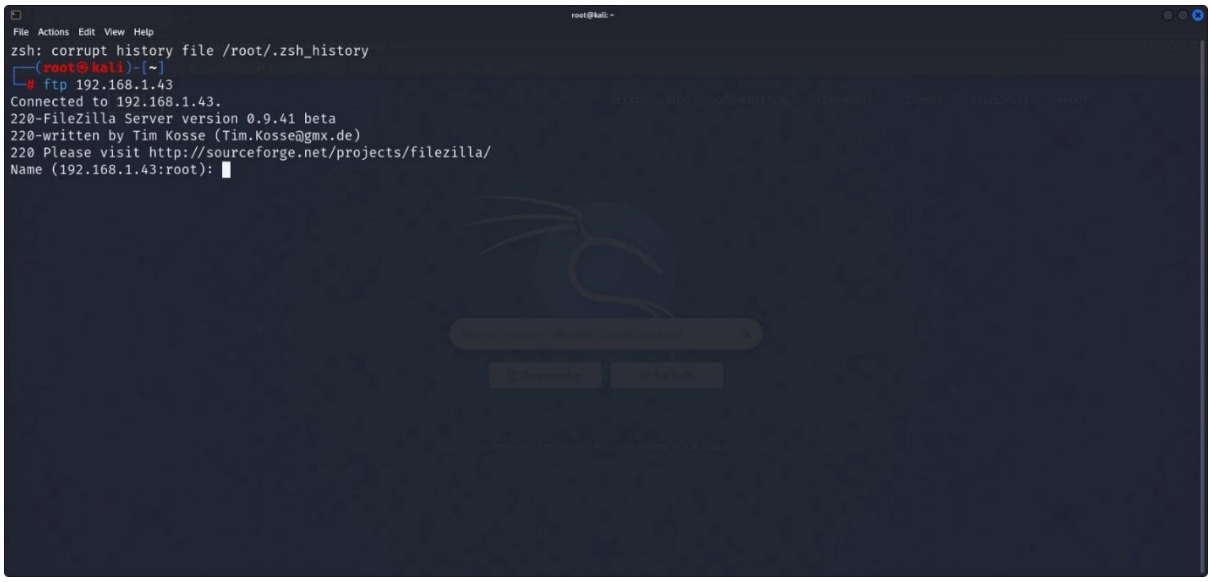
Before blocking port 21:

After starting the FTP service (such as FileZilla FTP Server) in XAMPP on a Windows system, you can connect to it from another device — for example, a Kali Linux system — by using the command:

ftp 192.168.1.43

This connects the Linux system to the Windows FTP server over port 21, allowing file transfer operations if credentials are correct and the firewall allows FTP traffic.

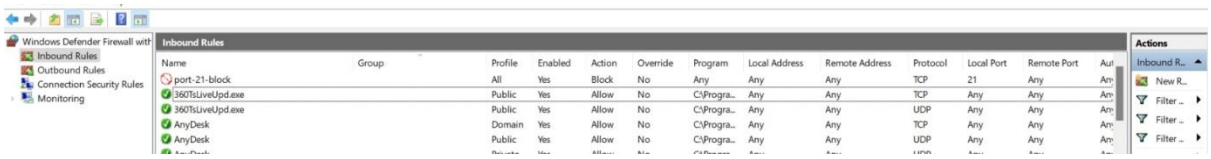
- Starting FTP service-



-Connecting windows system through FTP-

Configuring rule:

2.Blocking Port 21 (File Transfer Protocol):



- Configuring rule as Port-21-block-

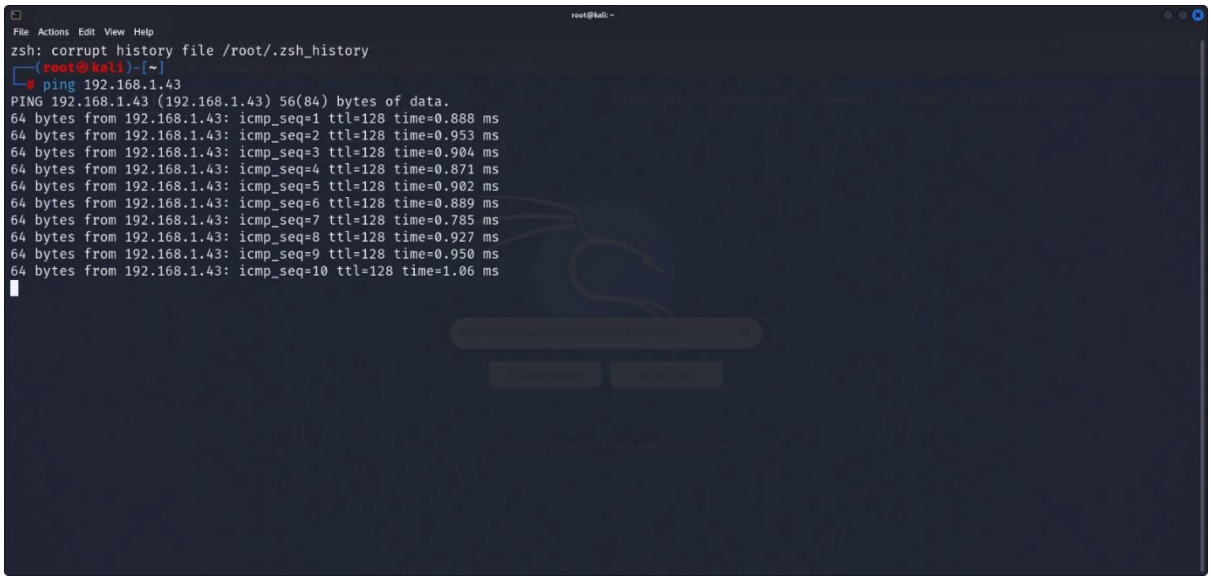
If you block port 21 (FTP) on the Windows system firewall, devices on the network — such as a Kali Linux machine — will not be able to connect via FTP, because the firewall will block incoming FTP connection requests, preventing access to the FTP service running in XAMPP.

-FTP Connection Failed-

Configuring rule:

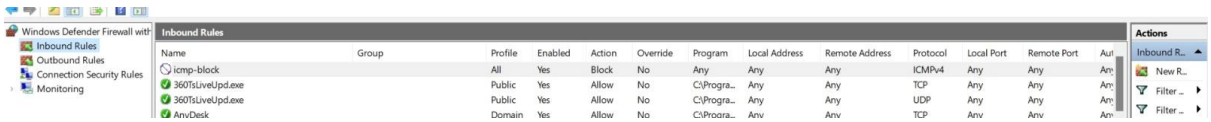
3.Blocking ICMP Protocol:

The ICMP (Internet Control Message Protocol) is used when you run the ping command from a Linux system to a Windows system. It helps test network connectivity by sending echo request and reply messages. If the Windows firewall blocks ICMP requests, the ping will fail even if the system is reachable on other protocols.



-Reply messages-

Configuring the rule: Blocking the ICMP Protocol



After blocking the ICMP protocol on the Windows system's firewall, you will not be able to ping the Windows machine from Kali Linux, because the firewall will drop the ICMP echo requests, causing the ping command to fail with timeouts.

- No reply message-

Linux Firewall Configuration:

UFW stands for Uncomplicated Firewall.

It’s a user-friendly command-line tool on Linux systems (especially Ubuntu) for managing a firewall based on iptables (the Linux kernel’s packet filtering framework).

- It simplifies configuring a firewall: no need to write complex iptables rules manually.
- Designed for beginners and sysadmins who want quick, basic firewall setup.
- Lets you allow or block incoming/outgoing network traffic by specifying ports, IP addresses, and protocols**.**

IP address of Kali Linux System (192.168.1.44)

Configuring UFW rules:

Allowing FTP and SSH Protocols and Blocking HTTP and HTTPS Protocols

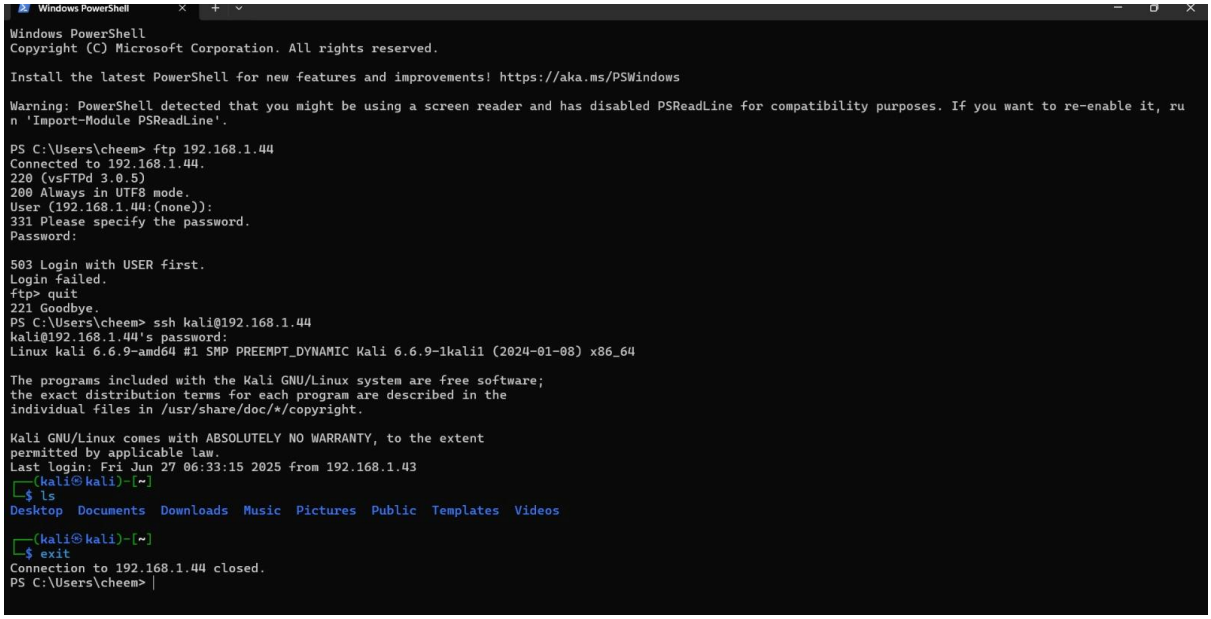
Commands:

```
File  Actions  Edit  View  Help

┌──(root㉿kali)-[~]
└─# ufw allow 21
Rule added
Rule added (v6)

┌──(root㉿kali)-[~]
└─# ufw allow 22
Rule added
Rule added (v6)

┌──(root㉿kali)-[~]
└─# ufw deny out 80
Rule added
Rule added (v6)

┌──(root㉿kali)-[~]
└─# ufw deny out 443
Rule added
Rule added (v6)
```

```
┌──(root㉿kali)-[~]
└─# ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 21                         ALLOW IN    Anywhere
[ 2] 22                         ALLOW IN    Anywhere
[ 3] 80                         DENY OUT    Anywhere                   (out)
[ 4] 443                        DENY OUT    Anywhere                   (out)
[ 5] 21 (v6)                    ALLOW IN    Anywhere (v6)
[ 6] 22 (v6)                    ALLOW IN    Anywhere (v6)
[ 7] 80 (v6)                    DENY OUT    Anywhere (v6)              (out)
[ 8] 443 (v6)                   DENY OUT    Anywhere (v6)              (out)
```

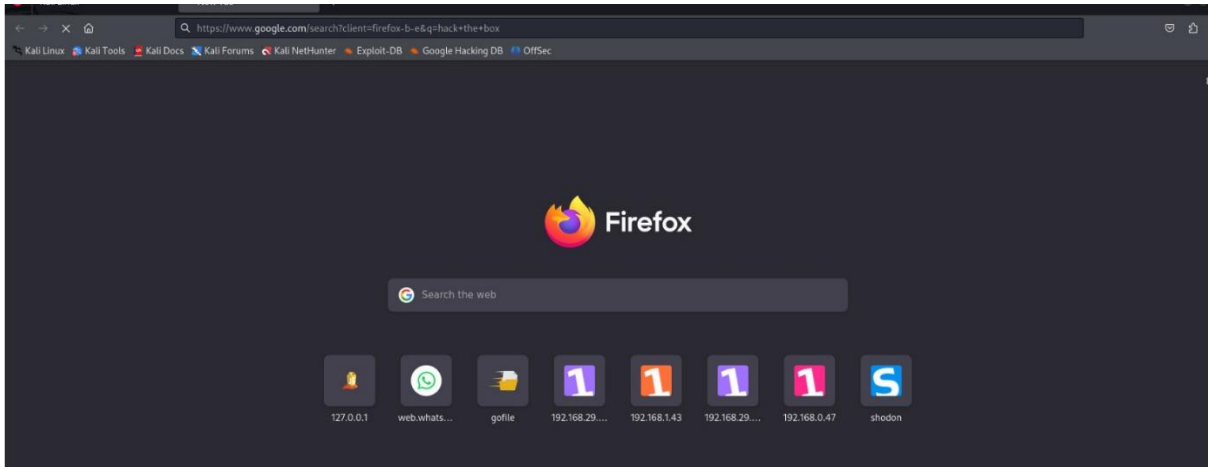
After you allowing After you allowing FTP (port 21) and SSH (port 22) in your UFW firewall rules on a Linux system, you can connect to that Linux system from a Windows machine using PowerShell.

- **Use FTP (ftp 192.168.1.44).**
- **Use SSH (ssh kali@192.168.1.44 -p 22)**



-Connected to Linux System through FTP and SSH-

After you denying HTTP (port 80) and HTTPS (port 443) in your UFW firewall rules on a Linux system, the Linux system will not be able to access websites over HTTP or HTTPS in a web browser, because the outgoing traffic to those ports will be blocked by the firewall, preventing the browser from loading web pages.



- Unable to load HTTP, HTTPS websites-