UNIT-1-LAB

Activity-1

Experiment: Basic Firewall Configuration

Windows Defender Firewall filters incoming and outgoing network traffic using predefined rules. By default, it allows most standard traffic and only asks permission when an application tries to connect in a non-standard way. However, it does not automatically block known malicious IP addresses. To improve security, we can manually add firewall rules and also automate rule creation using a script that blocks a list of known malicious IPs.

Software Requirements:

- Python 3.x
- Windows OS
- PowerShell
- Internet Connection
- Visual Studio Code / Any Python IDE

Manual Firewall Configuration (Inbound Rule):

This part explains how to manually block a specific IP using the Windows Firewall GUI.

Steps:

1. Open **Windows Defender Firewall with Advanced Security**.
2. Click on **Inbound Rules**.
3. Click **New Rule,**on the right panel.
4. Select **Custom** and click **Next**.
5. Choose **All Programs** → Click **Next**.
6. Protocol and Ports: Keep default → Click **Next**.
7. Scope:
    - Under **Remote IP address**, select **These IP addresses**.
    - Click **Add** and enter the IP you want to block (example: 1.2.3.4).
    - Click **OK** → Next.

8. Action: Select **Block the connection** → Next.
9. Profile: Select **Domain, Private, Public** → Next.
10. Name the rule (example: Manual_Block_IP) → Finish.

This rule will now block all incoming traffic from that specific IP.

Automated Firewall Configuration (Using Python Script):

Instead of blocking one IP, the script downloads a list of malicious IPs and blocks all of them automatically.

Problem Statement:

Write a Python program that downloads a list of malicious IP addresses from a trusted online source and automatically creates firewall rules to block those IPs from accessing the system.

Program: (File name: firewall.py)

```
import requests, csv, subprocess

# source: Abuse CH

response = requests.get(

   "https://feodotracker.abuse.ch/downloads/ipblocklist.csv"

).text

rule = 'netsh advfirewall firewall delete rule name="BadIP"'

subprocess.run(["PowerShell", "-Command", rule])

mycsv = csv.reader(

   filter(lambda x: not x.startswith("#"), response.splitlines())

)

for row in mycsv:

  ip = row[1]

   if ip != "dst_ip":

   print("Added Rule to block:", ip)

  rule = "netsh advfirewall firewall add rule name='BadIP' Dir=Out Action=Block RemoteIP=" + ip
```

subprocess.run(["PowerShell", "-Command", rule])

Sample Output:

Added Rule to block: 45.9.148.221

Added Rule to block: 103.17.48.5

Added Rule to block: 185.234.219.12

Execution Steps:

1. Open **Command Prompt** and select **Run as Administrator**.
   (Firewall rules require admin rights.)
2. Navigate to the folder where firewall.py is saved.
   Example: cd C:\Users\YourName\Desktop
3. Make sure Python is installed: python --version
4. install required library (if not already installed):- python -m pip install requests
5. Execute the program: python firewall.py
6. **Output will appear in Command Prompt like:**

   Added Rule to block: 45.9.148.221

   Added Rule to block: 103.17.48.5

For every IP, you will see:

- "Added Rule to block: <IP>"
- PowerShell/Command Prompt will also show **OK** message for successful rule creation.

7. Cross-verify the rules:
   - Open **Windows Defender Firewall with Advanced Security**
   - Go to **Outbound Rules**
   - Search for rule name: **BadIP**
   - You will see many blocked IP addresses listed