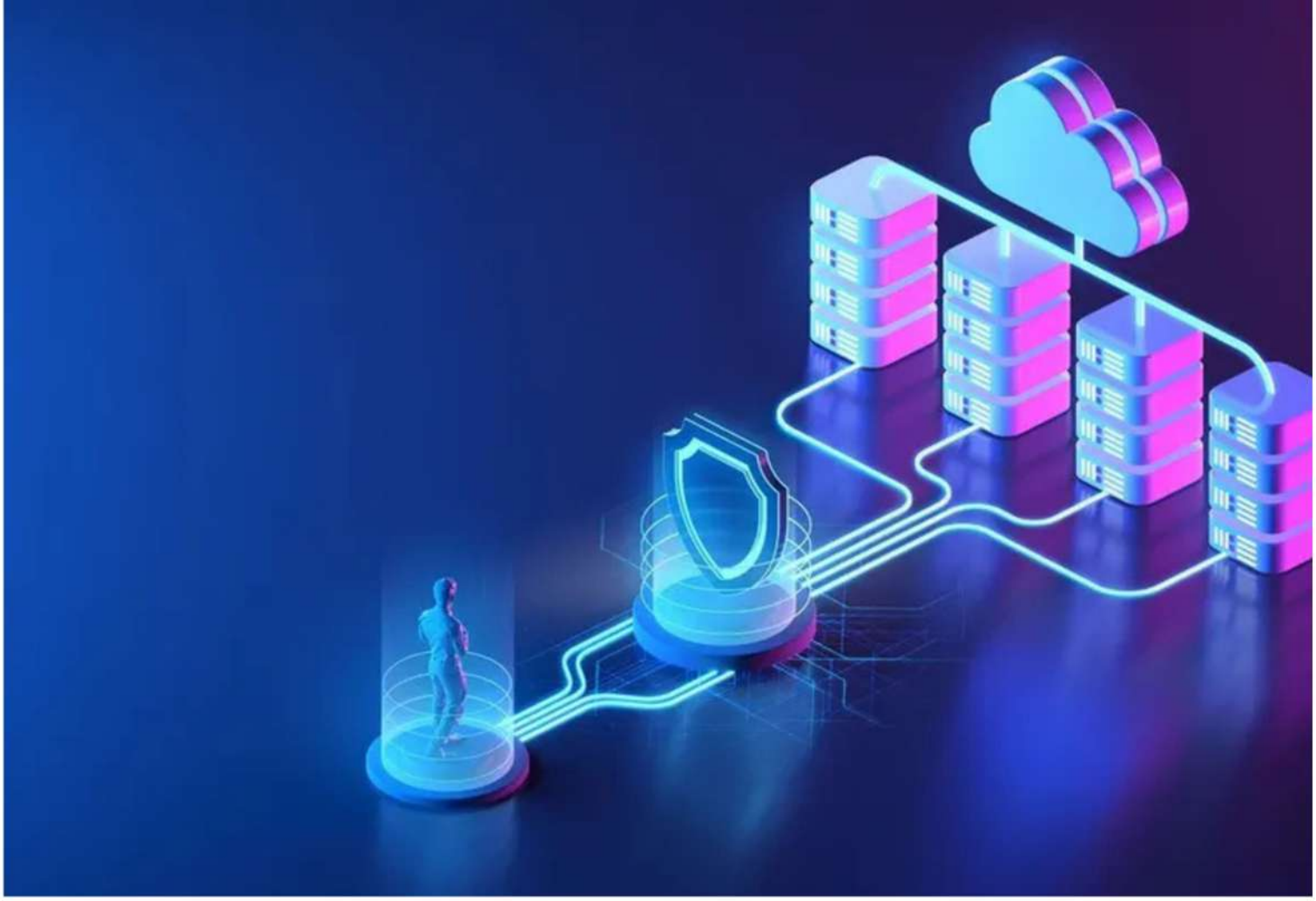
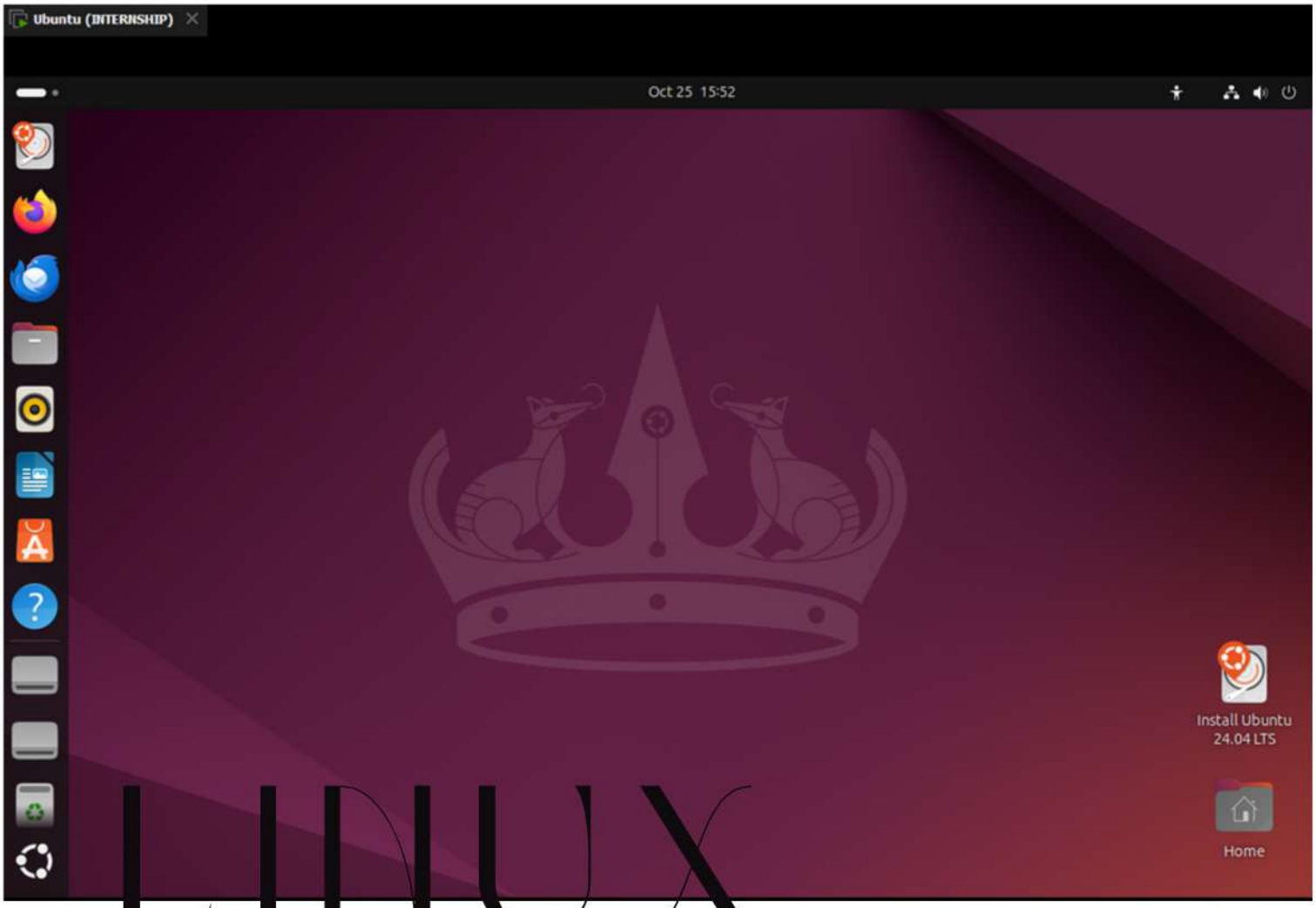
CONFIGURATION AND TRAFFIC FILTERING REPORT



INTRODUCTION

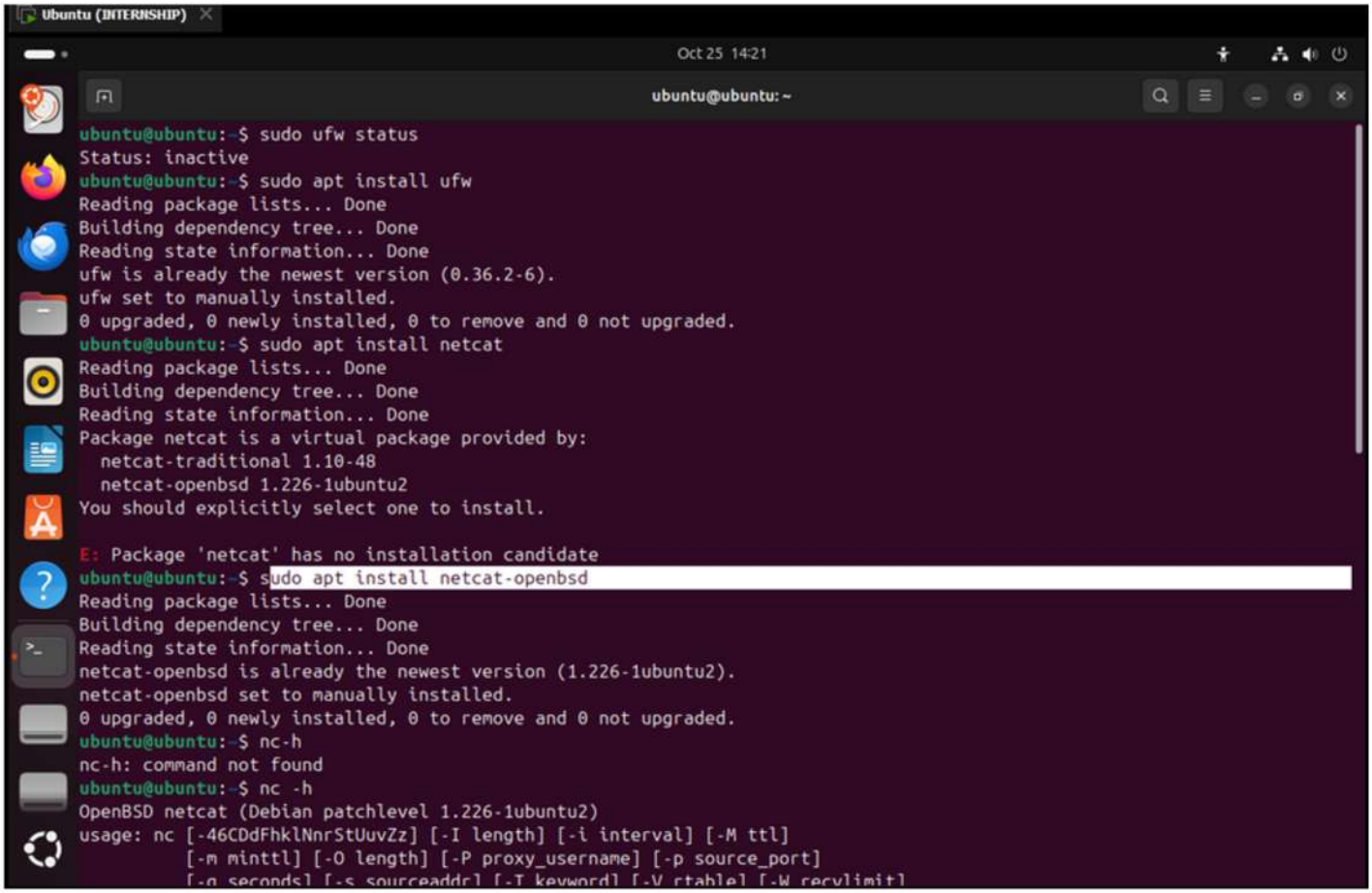
This document details the systematic execution of Task 4, which mandated the configuration and validation of host-based firewall policy across disparate operating system architectures. The core purpose was to establish a controlled security perimeter, thereby demonstrating foundational competency in implementing the Principle of Least Privilege at the network layer. This exercise utilized Uncomplicated Firewall (UFW) on a Linux (Ubuntu) endpoint and the Windows Defender Firewall with Advanced Security on a Windows endpoint. By successfully applying and testing rules that both denied inbound access to an insecure service (Telnet/TCP 23) and permitted access to a secure service (SSH/TCP 22), this procedure provides empirical evidence of the ability to harden endpoints and enforce a security-aware posture within a heterogeneous computing environment.



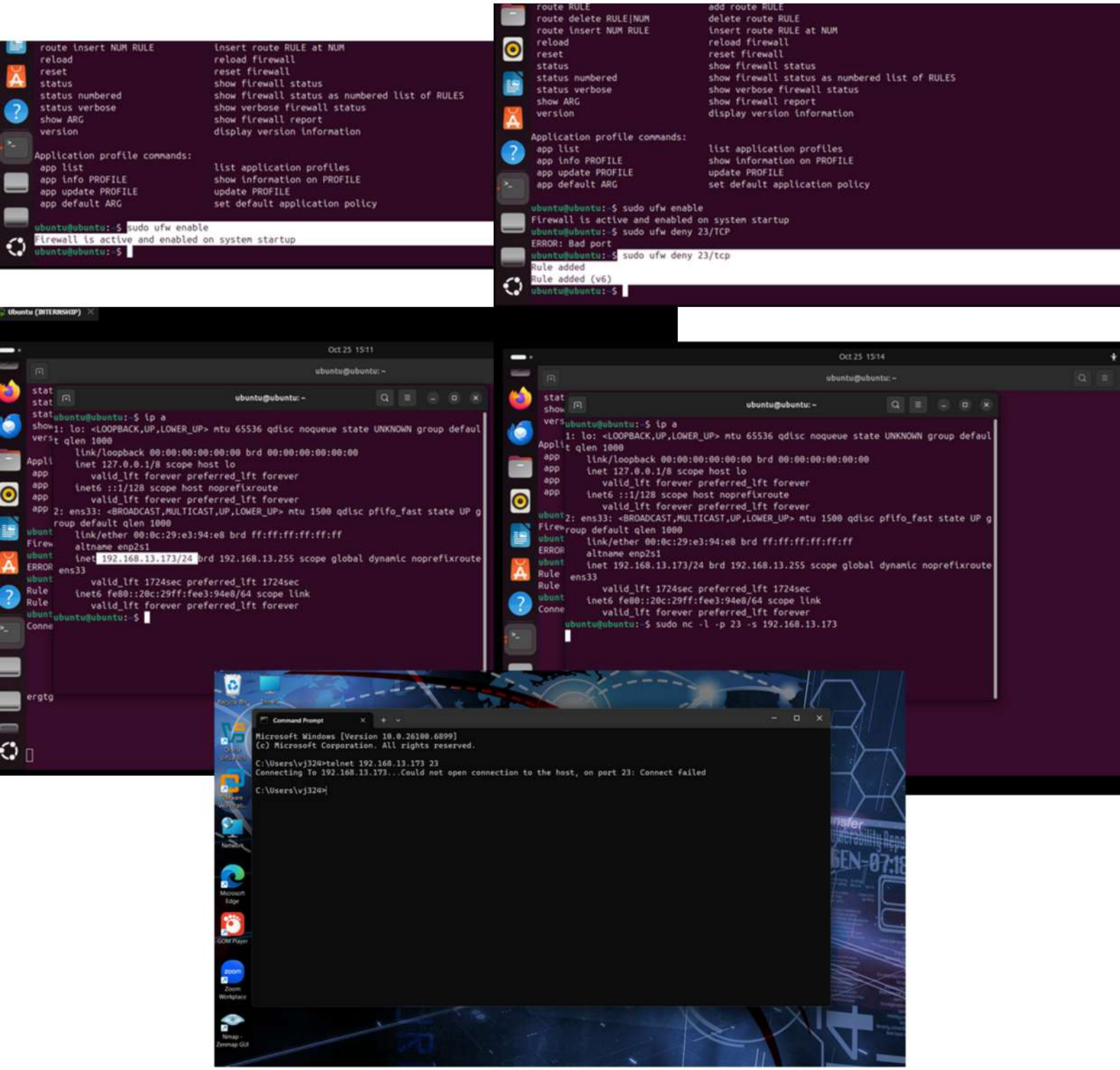
LINUX FIREWALL

UNCOMPLICATED FIREWALL (UFW) CONFIGURATION

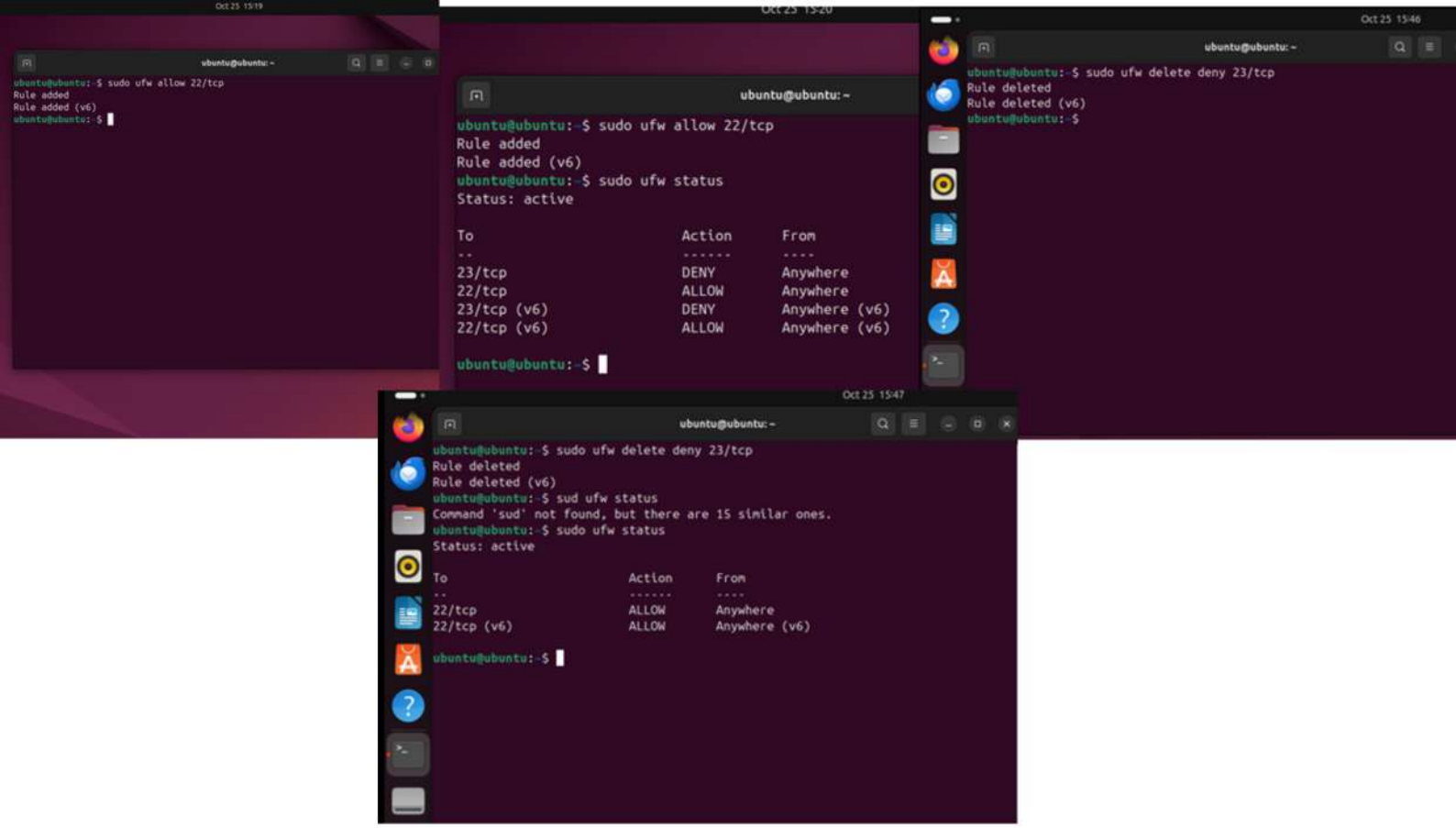
The UFW utility simplifies the management of the Linux kernel's netfilter framework. The following commands and steps were executed sequentially to demonstrate control over inbound traffic.



In this task, I performed the firewall setup on a Linux system using UFW (Uncomplicated Firewall). First, I checked the firewall status using the command sudo ufw status, which showed it was inactive. Then, I installed UFW using sudo apt install ufw. After that, I installed Netcat using sudo apt install netcat openbsd to test the network connections. Finally, I verified the Netcat installation by running nc -h command.



After installing UFW, I enabled the firewall using the command sudo ufw enable. Then, I created a rule to block the Telnet port by using sudo ufw deny 23/tcp. Once the rule was added, I checked my local IP address, which was 192.168.13.173. I tested the connection using Netcat, and the terminal only showed a blinking cursor, indicating that the port was blocked. To confirm this, I went to my local Windows machine and tried connecting through Telnet using the command telnet 192.168.13.173 23, which showed a “connection failed” message, proving that the firewall rule was successfully working.



After testing the blocked Telnet port, I added a new rule using sudo ufw allow 22/tcp to allow SSH connections. Then I checked the firewall status, and both the deny rule for port 23 and the allow rule for port 22 were displayed. Later, I removed the deny rule using sudo ufw delete deny 23, and after checking the status again, the rule was successfully deleted. This confirmed that the firewall rules were applied and managed correctly. In conclusion, this task helped me understand how to enable, configure, and test basic firewall rules in Linux using UFW to control network access and improve system security.

Thank you.

WINDOWS FIREWALL

UNCOMPLICATED FIREWALL (UFW) CONFIGURATION

In this part of the task, I performed the firewall configuration on a Windows system using Windows Defender Firewall with Advanced Settings. The main objective was to create and test a rule that blocks Telnet connections on port 23 and verify that the firewall successfully prevents unauthorized access.

Windows Defender Firewall with Advanced Security on Local Computer

Windows Defender Firewall with Advanced Security provides network security for Windows computers.

Overview

Domain Profile
- Windows Defender Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Private Profile is Active
- Windows Defender Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Public Profile
- Windows Defender Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Windows Defender Firewall Properties

Getting Started

Authenticate communications between computers

Inbound Rules

Name	Group	Profile	Enabled	Action	Override	Program
Apache HTTP Server		Public	Yes	Allow	No	C:\xamp...
Apache HTTP Server		Public	Yes	Allow	No	C:\xamp...

New Inbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

Steps: Rule Type, Program, Action, Profile, Name

What type of rule would you like to create?

- **Program** — Rule that controls connections for a program.
- **Port** — Rule that controls connections for a TCP or UDP port.
- **Predefined:** — Rule that controls connections for a Windows experience.
- **Custom** — Custom rule.

Protocol and Ports

Specify the protocols and ports to which this rule applies.

Steps: Rule Type, Protocol and Ports, Action, Profile, Name

Does this rule apply to TCP or UDP?
- TCP
- UDP

Does this rule apply to all local ports or specific local ports?
- All local ports
- Specific local ports: 23

Example: 80, 443, 5000-5010

Name

Specify the name and description of this rule.

Steps: Rule Type, Protocol and Ports, Action, Profile, Name

Name: Block_telnet

Description (optional): TASK4

< Back | Finish | Cancel

Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

Steps: Rule Type, Protocol and Ports, Action, Profile, Name

What action should be taken when a connection matches the specified conditions?

- **Allow the connection** — This includes connections that are protected with IPsec as well as those are not.
- **Allow the connection if it is secure** — This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.
  - Customize...
- **Block the connection**

< Back | Next > | Cancel

Inbound Rules

Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol
Block_telnet		All	Yes	Block	No	Any	Any	Any	TCP
Apache HTTP Server		Public	Yes	Allow	No	C:\xampp...	Any	Any	TCP
Apache HTTP Server		Public	Yes	Allow	No	C:\xampp...	Any	Any	UDP
brave.exe		Public	Yes	Block	No	C:\users\v...	Any	Any	TCP
brave.exe		Public	Yes	Block	No	C:\users\v...	Any	Any	UDP
brave.exe		Private	Yes	Block	No	C:\users\v...	Any	Any	TCP
brave.exe		Private	Yes	Block	No	C:\users\v...	Any	Any	UDP
Microsoft Office Outlook		Public	Yes	Allow	No	C:\Progra...	Any	Any	UDP
mysqld		Public	Yes	Allow	No	C:\xampp...	Any	Any	UDP
mysqld		Public	Yes	Allow	No	C:\xampp...	Any	Any	TCP
NVIDIA SHIELD Streaming NSS TCP Excepti...		All	Yes	Allow	No	C:\Progra...	Any	Any	TCP
NVIDIA SHIELD Streaming NSS UDP Except...		All	Yes	Allow	No	C:\Progra...	Any	Any	UDP
NVIDIA SHIELD Streaming NvStreamer TCP...		All	Yes	Allow	No	C:\Progra...	Any	Any	TCP
NVIDIA SHIELD Streaming NvStreamer UD...		All	Yes	Allow	No	C:\Progra...	Any	Any	UDP
NVIDIA SHIELD Streaming SSAS UDP Excep...		All	Yes	Allow	No	C:\Progra...	Any	Any	UDP
NVIDIA SHIELD Streaming SSAU UDP Exce...		All	Yes	Allow	No	C:\Progra...	Any	Any	UDP
Packet Tracer Executable		Private	Yes	Block	No	C:\progra...	Any	Any	UDP
Packet Tracer Executable		Private	Yes	Block	No	C:\progra...	Any	Any	TCP
Packet Tracer Executable		Public	Yes	Allow	No	C:\progra...	Any	Any	TCP
Packet Tracer Executable		Public	Yes	Allow	No	C:\progra...	Any	Any	UDP
SHAREit		All	Yes	Allow	No	C:\Progra...	Any	Any	Any
VMware Authd Service		Domain	Yes	Allow	No	C:\Progra...	Any	Any	Any
VMware Authd Service (private)		Private	Yes	Allow	No	C:\Progra...	Any	Local subnet	Any
VpnCoreDeamon		Public	Yes	Allow	No	C:\Progra...	Any	Any	TCP
VpnCoreDeamon		Public	Yes	Allow	No	C:\Progra...	Any	Any	UDP
zoom.exe		Public	Yes	Allow	No	C:\users\v...	Any	Any	TCP
zoom.exe		Private	Yes	Block	No	C:\users\v...	Any	Any	TCP
zoom.exe		Public	Yes	Allow	No	C:\users\v...	Any	Any	UDP
zoom.exe		Private	Yes	Block	No	C:\users\v...	Any	Any	UDP
@{GAMELOFTSA.AsphaltBAirborne_8.2.102...	@{GAMELOFTSA.AsphaltBAir...	Domai...	Yes	Allow	No	Any	Any	Any	Any
@{Microsoft.AAD.BrokerPlugin_1000.19580...	@{Microsoft.AAD.BrokerPlugi...	Domai...	Yes	Allow	No	Any	Any	Any	Any
@{Microsoft.AAD.BrokerPlugin_1000.19580...	@{Microsoft.AAD.BrokerPlugi...	Domai...	Yes	Allow	No	Any	Any	Any	Any
@{Microsoft.Win32WebViewHost_10.0.226...	@{Microsoft.Win32WebView...	All	Yes	Allow	No	Any	Any	Any	Any
@{Microsoft.Windows.CloudExperienceHo...	@{Microsoft.Windows.Cloud...	Domai...	Yes	Allow	No	Any	Any	Any	Any

Command Prompt

```
Microsoft Windows [Version 10.0.26100.6899]
(c) Microsoft Corporation. All rights reserved.

C:\Users\vj324>telnet 127.0.0.1 23
Connecting To 127.0.0.1...Could not open connection to the host, on port 23: Connect faile

C:\Users\vj324>
```

Are you sure you want to delete these rules?

Yes | No

WINDOWS FIREWALL

After completing the Linux part, I performed the same firewall configuration on Windows. I opened Windows Defender Firewall with Advanced Settings and created a new inbound rule. I selected “Port,” clicked “Next,” chose “TCP,” and entered the specific local port as 23. Then, I selected “Block the connection” and named the rule “Block Telnet” with the description “Task 4.” Once the rule was created, it appeared in the list as Block Telnet. I tested the connection using the IP address 127.0.0.1 in Command Prompt, and the connection failed, confirming that the rule was successfully applied. Later, I deleted the Block Telnet rule to restore the original firewall settings.