**Task 4: Setup and Use a Firewall on Windows/Linux**

To initiate the given task let us telnet to ubuntu VM from windows console and list firewall directory i.e.: /etc/ufw

Command for telnet is:

telnet <IP ADDRESS> <PORTNUMBER> in this case it is 23 and then enter ubuntu’s logon credentials.

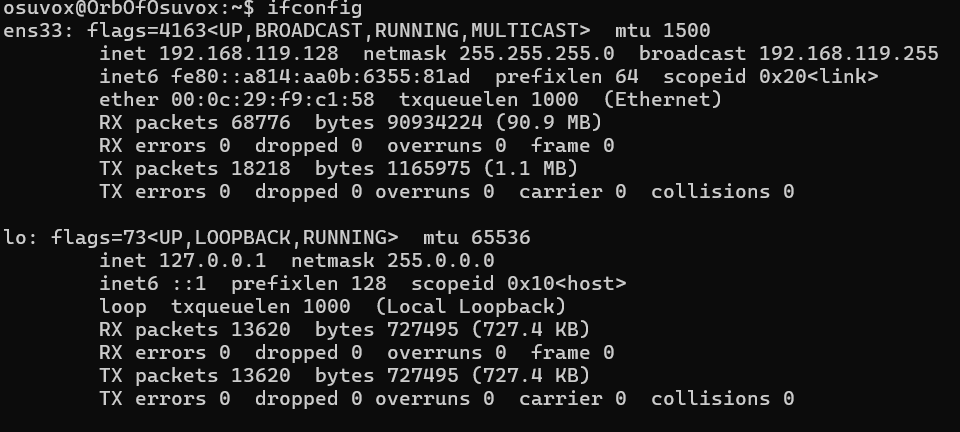


Figure 1 - ifconfig command for listing IP address of the device OS

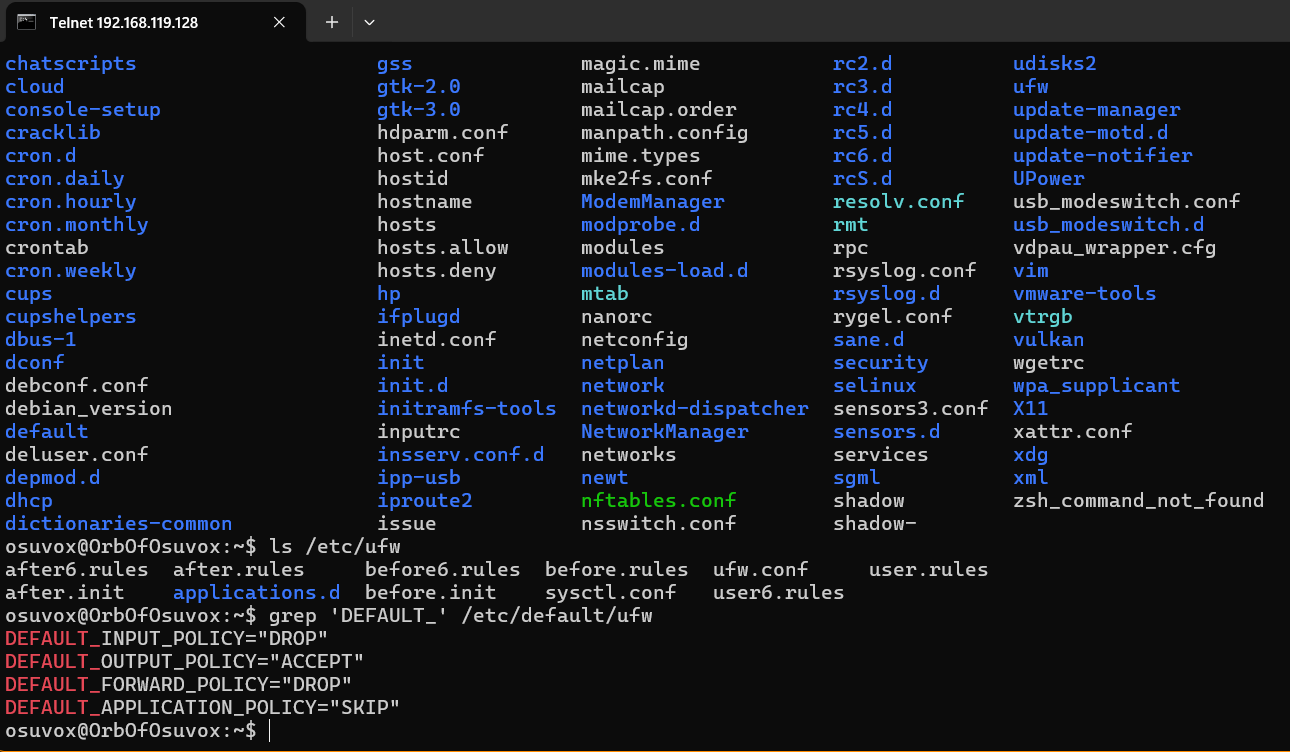


Figure 2 - List of contents in UFW directory by telnet connection from windows to ubuntu

Check for any existing user defined UFW rules. This gives us an idea what the previous person did to the UFW rule sets.

A screenshot of a computer program

AI-generated content may be incorrect.

Figure 3 - UFW commands to identify running firewall rules

Now as per the task indicated let us add rule to deny the usage of telnet or port 23. It can be for individual host or for the whole system. Don’t forget to check the rule after applying it.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 4 - Deny rule added to UFW for Telnet port 22

The rules take in effect after exiting the ongoing telnet connection. The ip address are of windows host.

Now let’s allow shh (port 22) for reliable connection and check the UFW rule has been added (Figure 6).

A screenshot of a computer

AI-generated content may be incorrect.

Figure 5 - Allow rule added to UFW for SHH port 22

A screenshot of a computer

AI-generated content may be incorrect.

Figure 6 - UFW Status verbose to identify active rules

A screenshot of a computer program

AI-generated content may be incorrect.

Figure 7 - UFW rules numbered for easy deletion

A black background with white text

AI-generated content may be incorrect.

Figure 8 - UFW rule deletion for port 22

For deleting rules, we can delete by applied rules or can be deleted by status number as per figure 7 and 8 indicates.

Example: sudo ufw delete <rule number> or sudo delete <applied rule>

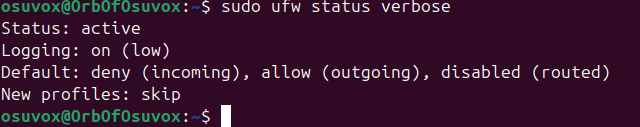


Figure 9 - Original state of UFW in Linux

In **Ubuntu Linux**, a firewall filters traffic using a system called **iptables** (or **nftables** in newer systems), often managed through a user-friendly tool called **UFW (Uncomplicated Firewall)**.

**How it filters traffic:**

1. **Rules-based filtering**: The firewall uses a set of rules to determine what traffic is allowed or blocked.
2. **Traffic inspection**: Each incoming, outgoing, or forwarded packet is inspected based on IP address, port, protocol, etc.
3. **Policy enforcement**: If the packet matches a rule, it is either **accepted**, **rejected**, or **dropped**.

**Example (UFW):**

* ufw allow 22 → allows SSH traffic (port 22).
* ufw deny 80 → blocks HTTP traffic (port 80).

In essence, the firewall acts as a gatekeeper, allowing only traffic that matches predefined safe rules.

**Example Flow**

Let’s say a packet comes to port 22 (SSH):

1. The packet arrives at the network interface.
2. The firewall checks INPUT chain rules.
3. If there’s a rule like ufw allow 22, the packet is **accepted**.
4. Otherwise, if default is DROP, it’s **discarded**.