Task 10

30/01/2026
ABISIN RAJ
I began by installing UFW on my Fedora system and disabling the default firewalld to avoid conflicts. Once UFW was enabled, I focused on reducing the system's attack surface by configuring specific security rules.

First, I explicitly blocked port 22 to prevent unauthorized SSH access. I applied this denial rule to both IPv4 and IPv6 protocols, ensuring no remote connections could be established. Second, after observing active network traffic, I identified and blocked the IP address 91.108.23.100 (Telegram) to demonstrate the ability to filter external connections., the Telegram application automatically attempted to re-establish connectivity by switching to an alternative IP address, demonstrating its failover capability.

I verified the final setup using the status command, confirming that SSH is disabled, the specific IP is blocked, and the system is operating under a secure default deny policy.

Commnads i used today

sudo dnf install ufw

sudo systemctl stop firewalld

sudo systemctl disable firewalld

sudo ufw enable

sudo ufw deny ssh

sudo ufw deny from 91.108.23.100

sudo ufw status verbose