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

Objective: Configure and test basic firewall rules to allow or block traffic.

Introduction:

**Uncomplicated Firewall**, a tool designed to simplify the process of managing a firewall on Linux systems, particularly those based on Ubuntu and Debian.

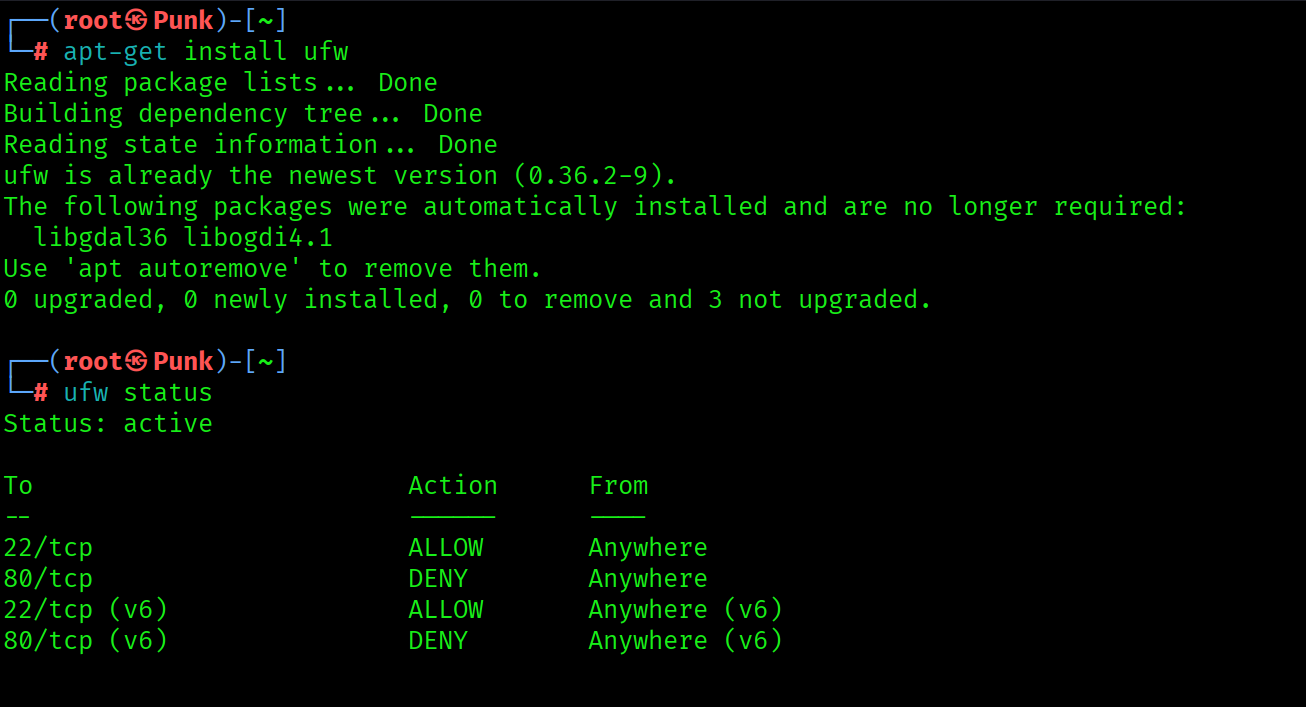
**Purpose of UFW**

UFW provides a **user-friendly interface** for configuring firewall rules, acting as a front-end to the more complex ip tables system built into the Linux kernel. It allows administrators to allow or block network traffic based on ports, IP addresses, or specific services, thereby helping to protect servers from unauthorized access and cyber threats.

Using UFW (Uncomplicated Firewall)

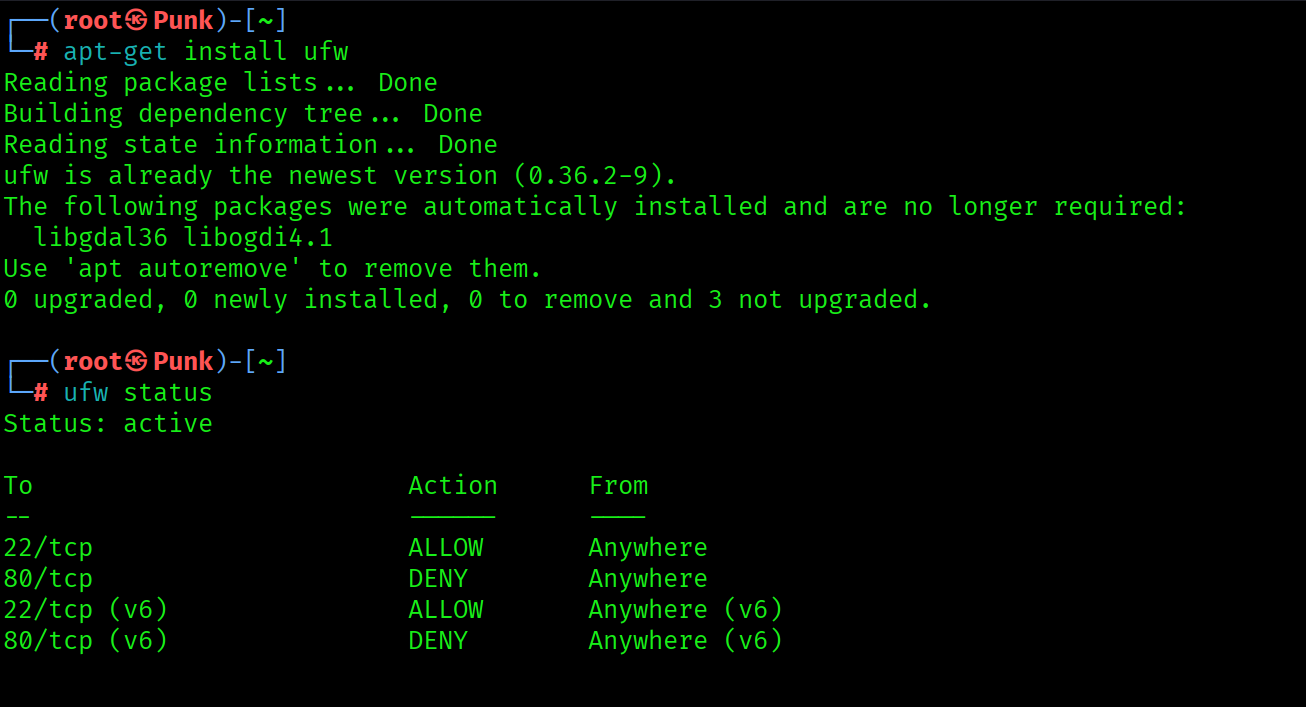
1. Install UFW:

* sudo apt-get update
* sudo apt-get install ufw



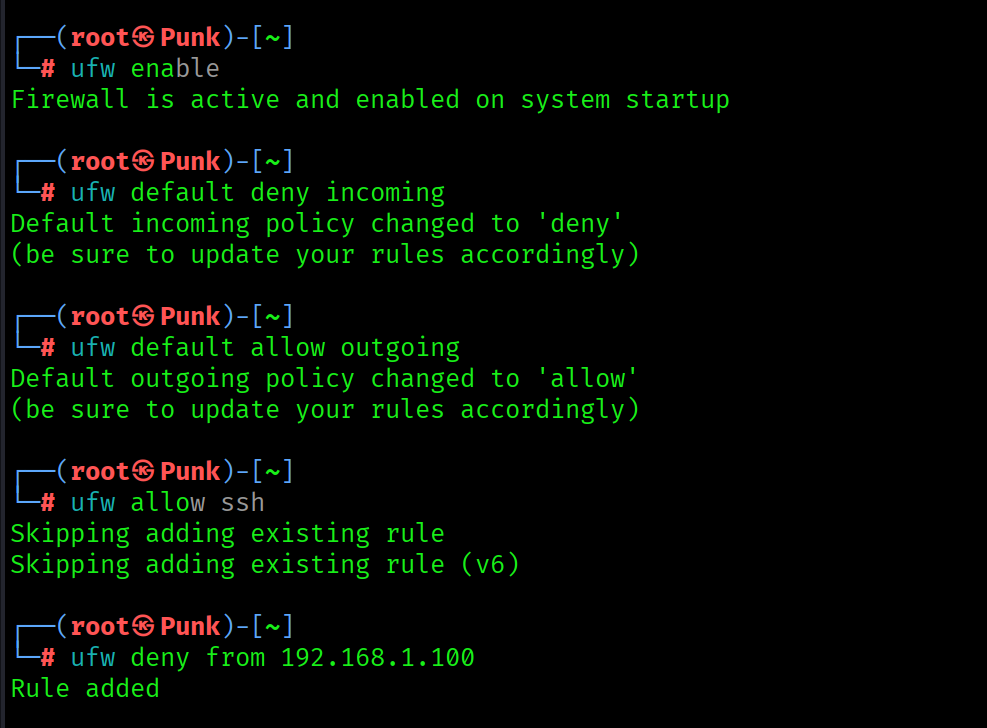
1. Check firewall status:

* sudo ufw status



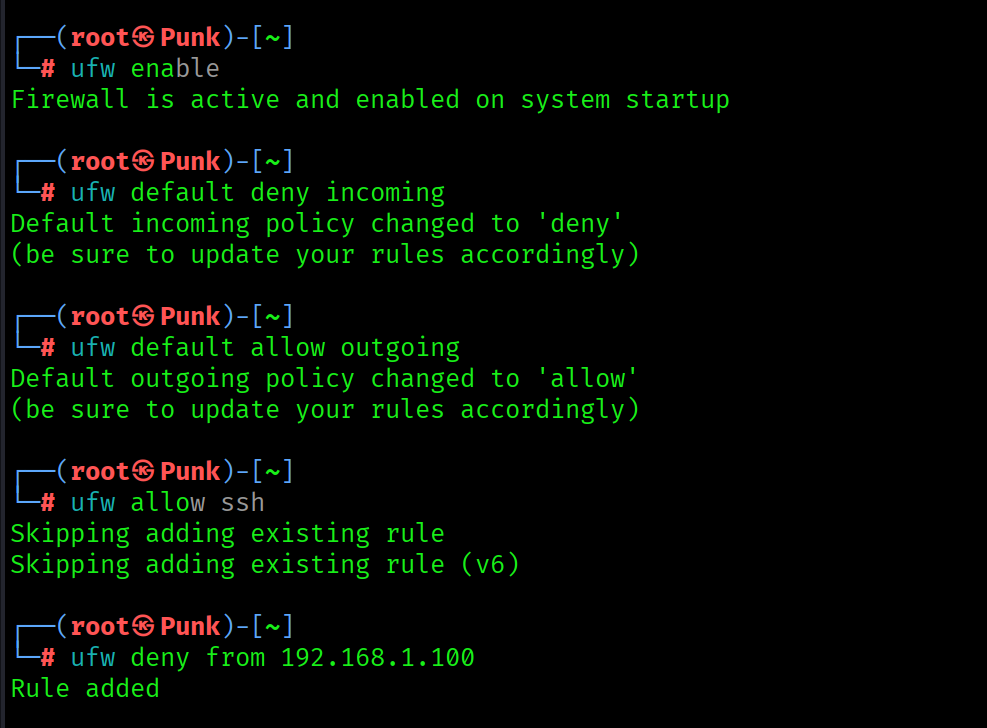
1. Enable UFW:

* sudo ufw enable



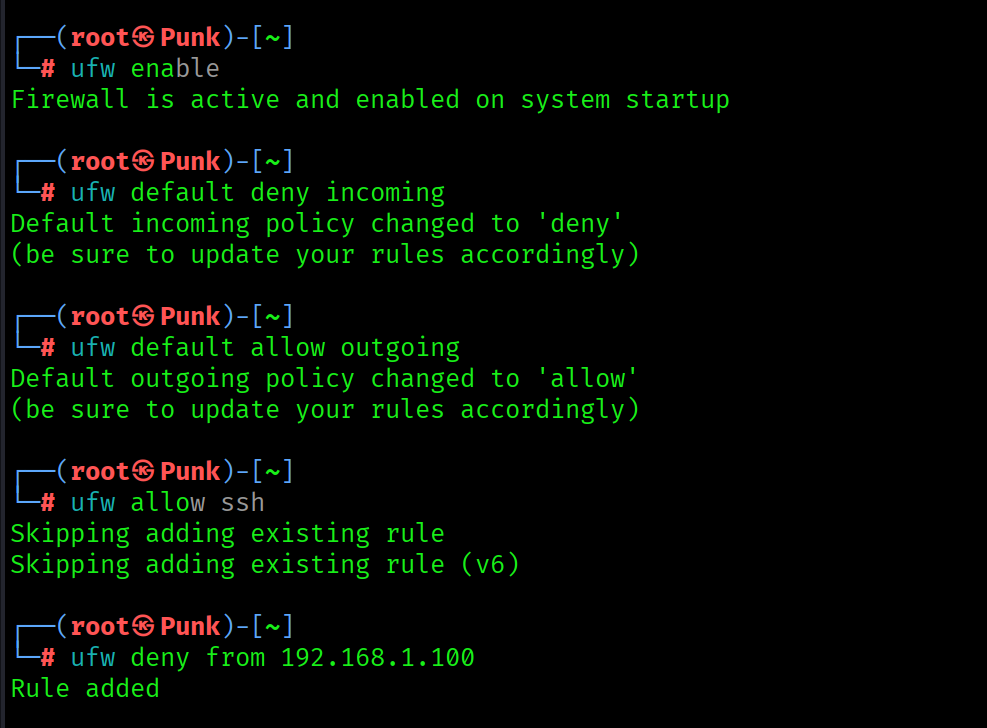
1. Set default policies:
2. Deny all incoming traffic:

* sudo ufw default deny incoming



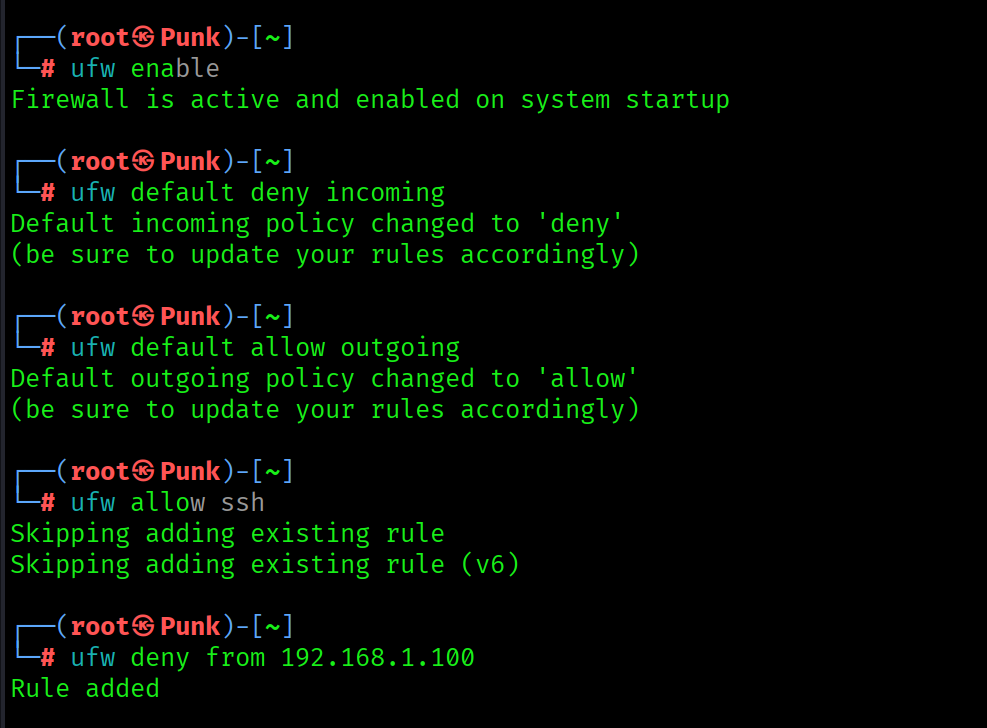
1. Allow all outgoing traffic:

* sudo ufw default allow outgoing



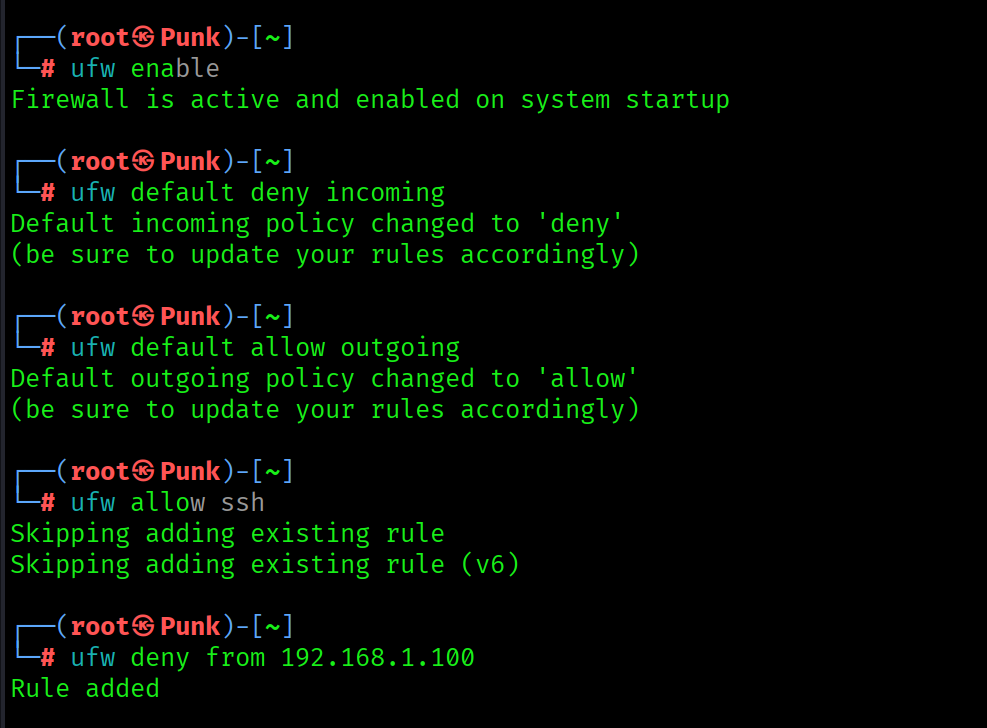
1. Allow specific services or ports:

* sudo ufw allow ssh



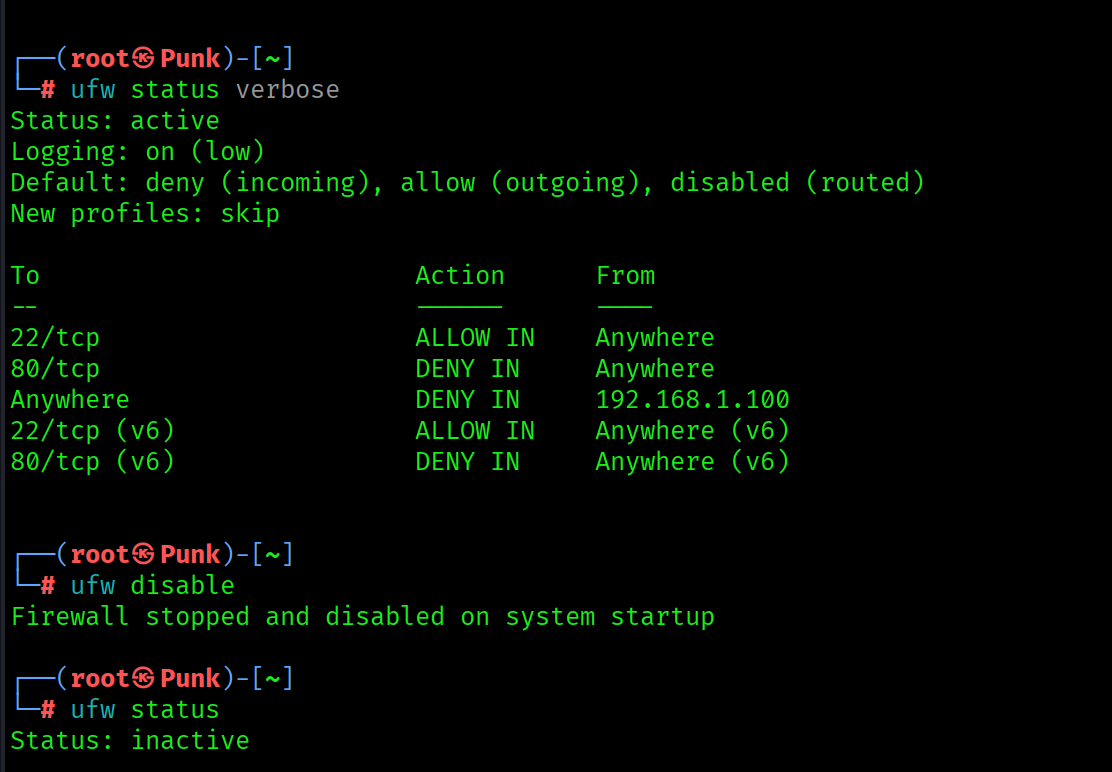
1. Deny specific IP addresses:

* sudo ufw deny from 192.168.1.100



1. Check firewall status with detailed info:

* sudo ufw status verbose



1. Disable UFW (if needed):

* sudo ufw disable

