Linux Ubuntu Firewall and Security Guide

This document provides a practical guide on how to use the firewall (UFW) and related security features on Linux Ubuntu. It is designed for beginners and intermediate users who want to secure their systems from unauthorized access while understanding essential security practices.

1. Understanding UFW (Uncomplicated Firewall)

UFW is the default firewall configuration tool for Ubuntu. It provides a simplified way to manage firewall rules compared to iptables. UFW is especially useful for servers, desktops, and laptops to control incoming and outgoing traffic.

2. Basic UFW Commands

- Enable UFW: sudo ufw enable
- Disable UFW: sudo ufw disable
- Check UFW status: sudo ufw status
- Reset UFW to defaults: sudo ufw reset
- Allow a port (e.g., SSH): sudo ufw allow 22/tcp
- Deny a port: sudo ufw deny 80/tcp
- Allow specific IP to a port: sudo ufw allow from 192.168.0.100 to any port 22
- Delete a rule by number: sudo ufw status numbered -> sudo ufw delete

3. Advanced UFW Usage

Beyond basic allow/deny rules, UFW supports advanced features such as:
- Restricting access to services from specific subnets (e.g., local network).
- Rate limiting (e.g., to protect against brute-force SSH attacks): sudo ufw limit ssh
- Logging firewall activity for analysis: sudo ufw logging on
- Default policies: sudo ufw default deny incoming; sudo ufw default allow outgoing

4. Checking Open Ports

It is important to monitor which ports are open on your system. Tools like ss and nmap can be used: - ss -tuln: Shows open listening ports and associated services. - sudo nmap -sV localhost: Scans for open ports and service versions.

5. Securing SSH Access

SSH is commonly targeted by attackers. Steps to secure SSH include: - Changing the default SSH port from 22 to another number (edit /etc/ssh/sshd_config). - Allowing only specific users or groups to log in via SSH. - Using SSH key authentication instead of passwords. - Disabling root login over SSH. - Enabling UFW rules to restrict SSH access to specific IPs.

6. Additional Security Practices

- Keep the system updated: sudo apt update && sudo apt upgrade
- Install fail2ban to block repeated brute-force login attempts.
- Use strong, unique passwords and consider a password manager.
- Enable automatic security updates (unattended-upgrades).

- Encrypt sensitive data with tools like gpg or full-disk encryption.
- Monitor logs regularly (/var/log/auth.log, /var/log/syslog).
- Disable unused services and remove unnecessary packages.

Conclusion

By properly configuring UFW and following good security practices, you can significantly reduce the attack surface of your Ubuntu system. Security is an ongoing process, so continuous monitoring and updates are essential.