

Basic Linux Security Checklist

1. Disable unnecessary services

- Shutdown service scripts in /etc/init.d/
- Disable service startup on boot (chkconfig, update-rc.d, etc)
- Remove scripts/services if listed in /etc/rc.d/rc.local
- Confirm with netstat

2. Restrict root access

- Disable root login via ssh (/etc/ssh/sshd_config)
- Disable root login via console (/etc/securetty)
- Configure sudo for necessary users

3. Configure local firewall

- Block all unnecessary services (iptables)
- Remove iptables startup rules (ie, /etc/sysconfig/iptables)

4. Configure TCP Wrappers

- Edit /etc/hosts.deny to deny everything
- Edit /etc/hosts.allow to allow minimum services to minimum sources

5. Disable SSH version 1

- (CentOS) edit /etc/ssh/sshd_config, comment out "Protocol 2,1", uncomment "Protocol 2"