# Securing/Hardening Linux

**Note:** I advise you to take backup of the files before making any changes to it, if in case something goes wrong you can revert it.

1. Physical System Security
   1. Configure the BIOS to disable booting from CD/DVD, External Devices, Floppy Drive in BIOS.
   2. Next, enable BIOS password & also protect GRUB with password to restrict physical access of your system.
      1. Check Grub version: **grub-install -V**
      2. Create a password for GRUB, be a root user and open command prompt, type below command. When prompted type grub password twice and press enter. This will return MD5 hash password. Please copy or note it down. **grub-mkpasswd-pbkdf2**
      3. Paste the encrypted long string into the file /etc/grub.d/40\_custom together with the set superusers command. Remember to keep the commented lines at the beginning:

**set superusers="root"**

**password\_pbkdf2 root grub.pbkdf2.sha512.10000.9CA4611006FE96BC77A...**

* + 1. In /etc/grub.d

vim 40\_custom

Append the following part

**set superusers="root"**

**password\_pbkdf2 root grub.pbkdf2.sha512.10000.05**

* + 1. Now you need to open the /boot/grub.

grub-mkconfig -o /boot/grub/grub.cfg

* + 1. Check if the above superuser and credentials is implemented in /boot/grub/grub.cfg
    2. Reboot system and try it pressing ‘p‘ to enter password to unlock and enable next features.

1. Minimize Packages to Minimize Vulnerability

https://www.tecmint.com/list-all-running-services-under-systemd-in-linux/

* 1. Do you really want all sort of services installed?

It’s recommended to avoid installing useless packages to avoid vulnerabilities in packages. This may minimize risk that compromise of one service may lead to compromise of other services. Find and remove or disable unwanted services from the server to minimize vulnerability.

Use the ‘**systemctl**‘ command to find out services which are running.

**systemctl list-units --type=service**

Use the ‘**ss**‘ command to find out sockets which are in use.

Use below mentioned command to remove those services

**sudo apt-get remove package-name**

1. Check Listening Network Ports
   1. Use the ‘**ss**‘ command to find out ports which are in use.
2. Enabling SSH securely
   1. Use “sudo” to execute commands. sudo are specified in /etc/sudoers file also can be edited with the “visudo” utility which opens in VI editor.
   2. It’s also recommended to change default SSH 22 port number with some other higher level port number. Open the main SSH configuration file and make some following parameters to restrict users to access.
      1. Disable root login

**gedit /etc/ssh/sshd\_config**

**Edit file to desire setting**

**systemctl restart ssh**

* + 1. Allow Specific Users

**gedit /etc/ssh/sshd\_config**

**AllowUsers <username>**

**systemctl restart ssh**

* + 1. Use Protocol 2

**gedit /etc/ssh/sshd\_config**

**Protocol 2**

**systemctl restart ssh**

* + 1. Connection Timeout Idle Value

**gedit /etc/ssh/sshd\_config**

**ClientAliveInterval 180**

**systemctl restart ssh**

* + 1. Configure a Limit for Password Attempts

**gedit /etc/ssh/sshd\_config**

**MaxAuthTries 3**

**systemctl restart ssh**

* + 1. Disable User SSH Passwordless Connection Requests

**gedit /etc/ssh/sshd\_config**

**PermitEmptyPasswords no**

**systemctl restart ssh**

* + 1. Setup SSH Passwordless Authentication

**gedit /etc/ssh/sshd\_config**

**PasswordAuthentication no**

**systemctl restart ssh**

1. Keep System updated
   1. **apt install unattended-upgrades**
   2. **dpkg-reconfigure --priority=low unattended-upgrades**
2. Disable USB usage
   1. nano /etc/modprobe.d/blacklist.conf
      1. blacklist usb\_storage
      2. save and close
   2. nano /etc/rc.local
      1. modprobe -r usb\_storage
   3. exit 0
3. Enable SELinux
   1. apt install policycoreutils selinux-basics
   2. selinux-activate
   3. sestatus
   4. nano /etc/selinux/config
      1. SELINUX=enforcing
      2. Save and close
   5. Reboot
4. Password policies
   1. sudo /etc/login.defs
      1. Enforce users to change password every 30 days or less

PASS\_MAX\_DAYS 30

* + 1. sudo apt-get -y install libpam-pwquality cracklib-runtime
    2. sudo vim /etc/pam.d/common-password

change line 25 from

password requisite pam\_pwquality.so retry=3

to

password requisite pam\_pwquality.so retry=3 minlen=8 maxrepeat=3 ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1 difok=3 gecoscheck=1 reject\_username enforce\_for\_root

* + 1. sudo reboot
  1. To view the current password expiry/aging details, the command is:
     1. sudo chage –l username

**Options used.**

retry=3: Prompt a user 3 times before returning with error.

minlen=8 : The password length cannot be less than this parameter

maxrepeat=3: Allow a maximum of 3 repeated characters

ucredit=-1 : Require at least one uppercase character

lcredit=-1 : Must have at least one lowercase character.

dcredit=-1 : must have at least one digit

difok=3 : The number of characters in the new password that must not have been present in the old password.

gecoscheck=1: Words in the GECOS field of the user’s passwd entry are not contained in the new password.

reject\_username: Rejects the password if contains the name of the user in either straight or reversed form.

enforce\_for\_root: Enforce pasword policy for root user

Audit: https://github.com/finalduty/cis\_benchmarks\_audit