### 1. Physical System Security

### 2. Disk Partitions

/

/boot

/usr

/var

/home

/tmp

/opt

### 3. Minimize Packages to Minimize Vulnerability

# /sbin/chkconfig --list |grep '3:on'

# chkconfig serviceName off

# yum -y remove package-name

# sudo apt-get remove package-name

### 4. Check Listening Network Ports

# netstat -tulpn

### 5. Use Secure Shell(SSH)

# yum yf

# vi /etc/ssh/sshd\_config

##### Disable root Login

PermitRootLogin no

##### Only allow Specific Users

AllowUsers username

##### Use SSH Protocol 2 Version

Protocol 2

### 6. Keep System updated

# yum updates

# yum check-update

### 7. Lockdown Cronjobs

# echo ALL >>/etc/cron.deny

### 8. Disable USB stick to Detect

Create a file ‘**/etc/modprobe.d/no-usb**‘ and adding below line will not detect **USB** storage.

install usb-storage /bin/true

### 9. Turn on SELinux

You can view current status of **SELinux** mode from the command line using

‘**system-config-selinux**‘, ‘**getenforce**‘ or ‘**sestatus**‘ commands.

# sestatus

If it is disabled, enable **SELinux** using the following command.

# setenforce enforcing

### 10. Remove KDE/GNOME Desktops

# yum groupremove "X Window System"

### 11. Turn Off IPv6

# vi /etc/sysconfig/network

NETWORKING\_IPV6=no

IPV6INIT=no

### 12. Restrict Users to Use Old Passwords

Open **‘/etc/pam.d/common-password**‘ file under **Ubuntu/Debian/Linux Mint**.

# vi /etc/pam.d/common-password

Add the following line to ‘**auth**‘ section.

auth sufficient pam\_unix.so likeauth nullok

Add the following line to ‘**password**‘ section to disallow a user from re-using last **5** password of his or her.

password sufficient pam\_unix.so nullok use\_authtok md5 shadow remember=5

Only last **5** passwords are remember by server. If you tried to use any of last **5** old passwords, you will get an error like.

Password has been already used. Choose another.

### 13. How to Check Password Expiration of User

#chage -l username

To change password aging of any user, use the following command.

#chage -M 60 username

#chage -M 60 -m 7 -W 7 userName

### 14. Lock and Unlock Account Manually

# passwd -l accountName

# su - accountName

This account is currently not available.

To unlock or enable access to an locked account, use the command as. This will remove (**!**) string with encrypted password.

# passwd -u accountName

### 15. Enforcing Stronger Passwords

# vi /etc/pam.d/system-auth

And add line using credit parameters as (**lcredit**, **ucredit**, **dcredi**t and/or **ocredit** respectively lower-case, upper-case, digit and other)

/lib/security/$ISA/pam\_cracklib.so retry=3 minlen=8 lcredit=-1 ucredit=-2 dcredit=-2 ocredit=-1

### 16. Enable Iptables (Firewall)

### 17. Disable Ctrl+Alt+Delete in Inittab

# Trap CTRL-ALT-DELETE

#ca::ctrlaltdel:/sbin/shutdown -t3 -r now

### 18. Checking Accounts for Empty Passwords

# cat /etc/shadow | awk -F: '($2==""){print $1}'

### 19. Display SSH Banner Before Login

### 20. Monitor User Activities

### 21. Review Logs Regularly

Move logs in dedicated log server, this may prevents intruders to easily modify local logs. Below are the Common Linux default log files name and their usage:

1. **/var/log/message** – Where whole system logs or current activity logs are available.
2. **/var/log/auth.log** – Authentication logs.
3. **/var/log/kern.log** – Kernel logs.
4. **/var/log/cron.log** – Crond logs (cron job).
5. **/var/log/maillog** – Mail server logs.
6. **/var/log/boot.log** – System boot log.
7. **/var/log/mysqld.log** – MySQL database server log file.
8. **/var/log/secure** – Authentication log.
9. **/var/log/utmp** or **/var/log/wtmp** : Login records file.
10. **/var/log/yum.lo**g: Yum log files.

### 22. Important file Backup

### 23. NIC Bonding

### 24. Keep /boot as read-only

# vi /etc/fstab

Add the following line at the bottom, save and close it.

LABEL=/boot /boot ext2 defaults,ro 1 2

### 25. Ignore ICMP or Broadcast Request

Ignore ICMP request:

net.ipv4.icmp\_echo\_ignore\_all = 1

Ignore Broadcast request:

net.ipv4.icmp\_echo\_ignore\_broadcasts = 1

Load new settings or changes, by running following command

#sysctl -p