**Hardening of Linux System.**

Local solutions:

1. Configure the **BIOS** to disable booting from **CD/DVD**, **External Devices**, **Floppy Drive** in **BIOS**
2. With the help of ‘**netstat**‘ networking command you can view all open ports and associated programs. As I said above use ‘**chkconfig**‘ command to disable all unwanted network services from the system.
3. **Telnet** and **rlogin** protocols uses plain text, not encrypted format which is the security breaches. **SSH** is a secure protocol that use encryption technology during communication with server.
4. Always keep system updated with latest releases patches, security fixes and kernel when it’s available.
5. **Cron** has it’s own built in feature, where it allows to specify who may, and who may not want to run jobs. This is controlled by the use of files called **/etc/cron.allow** and **/etc/cron.deny**. To lock a user using cron, simply add user names in **cron.deny** and to allow a user to run cron add in **cron.allow** file. If you would like to disable all users from using cron, add the ‘**ALL**‘ line to **cron.deny** file.
6. It’s highly recommended to enable **Linux firewall** to secure unauthorised access of your servers. Apply rules in **iptables** to filters **incoming**, **outgoing** and **forwarding** packets. We can specify the source and destination address to allow and deny in specific **udp/tcp** port number.
7. Move logs in dedicated log server, this may prevents intruders to easily modify local logs.

### Keep /boot as read-only

## Set Up Password Aging For Linux Users For Better Security

## Configure Iptables and TCPWrappers based Firewall on Linux

## Linux Kernel /etc/sysctl.conf Hardening

## Turn Off IPv6 only if you are NOT using it on Linux

Source :- <https://www.cyberciti.biz/tips/linux-security.html>

<https://www.tecmint.com/linux-server-hardening-security-tips/>

Official Security solutions:

1. The root account must be the only account having unrestricted access to the system.
2. The operating system must disable account identifiers (individuals, groups, roles, and devices) if the password expires.
3. The delay between logon prompts following a failed console logon attempt must be at least four seconds
4. Auditing must be configured to produce records containing information to establish what type of events occurred, where the events occurred, the source of the events, and the outcome of the events. These audit records must also identify individual identities of group account users.
5. The audit system must take appropriate action when the audit storage volume is full.
6. All uses of the chown,chmod command must be audited.
7. All uses of the passwd, su, sudo, ssh-keyen, crontab command must be audited
8. The operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/passwd.
9. The system must not have accounts configured with blank or null password.
10. Accounts subject to three unsuccessful logon attempts within 15 minutes must be locked for the maximum configurable period.
11. The system must not have unnecessary accounts.
12. There must be no .shosts, vshosts.equiv files on the system.
13. The file permissions, ownership, and group membership of system files and commands must match the vendor value
14. All files and directories must have a valid owner
15. The umask must be set to 077 for all local interactive user accounts.
16. If the cron.allow file exists it must be owned by root.
17. The operating system must not allow an unattended or automatic logon to the system via a graphical user interface.
18. USB mass storage must be disabled
19. The operating system must enable SELinux
20. Systems with a Basic Input/Output System (BIOS) must require authentication upon booting into single-user and maintenance modes.
21. The operating system must enable the SELinux targeted policy.
22. The x86 Ctrl-Alt-Delete key sequence must be disabled
23. The system must not allow removable media to be used as the boot loader unless approved.
24. The system must use a virus scan program.
25. All network connections associated with a communication session must be terminated at the end of the session or after 10 minutes of inactivity from the user at a command prompt, except to fulfill documented and validated mission requirements.
26. SNMP community strings must be changed from the default.
27. The operating system must enable an application firewall, if available.
28. The rsh-server,ypserv,nis,telnet-server package must not be installed.
29. The operating system must prevent the installation of software, patches, service packs, device drivers, or operating system components from a repository without verification they have been digitally signed using a certificate that is issued by a Certificate Authority (CA) that is recognized and approved by the organization.
30. The operating system must be a vendor supported release.
31. A File Transfer Protocol (FTP),Trivial File Transfer Protocol (TFTP) server package must not be installed unless needed.
32. The SSH daemon must not allow authentication using an empty password.
33. The operating system must not allow users to override SSH environment variables.
34. The operating system must not allow a non-certificate trusted host SSH logon to the system.
35. The system must not permit direct logons to the root account using remote access via SSH.
36. The SSH daemon must be configured to only use the SSHv2 protocol.
37. Remote X connections for interactive users must be encrypted.

Reference : <https://www.stigviewer.com/stig/red_hat_enterprise_linux_7/>