1. The history on boot loader for Linux , what is the default boot loader currently for Linux

   Maggie or Bini…….

2 **Maggie or Bini do it……**

4. what is runlevel in Linux, how much runlevels Linux has? What are their different? /etc/rc.d (red hat)

Init script: spans all other processes

/etc/inittab -> Used to set default run level

It's checked by runlevel

- ✓ A runlevel is a present operating state on a unix-like OS
- ✓ A system can be booted into (started up into) any of several runlevels, each of which is represented by a single digit integer. Each runlevel designates a different system config and allows access to a different combination of processes (i.e., instances of executing programs)
- ✓ There are differences in the runlevels according to the operating system. Seven runlevels are supported in the standard Linux kernel (core of the OS). They are:
  - 0 - System halt; no activity, the system can be safely powered down
    - Transitional state ; shutdown
  - 1 – Single user; rarely used
    - For low level maintenance.
    - Network is not configured.
  - 2 – Multiple users, no NFS (network filesystem); also used rarely.
    - GUI Login(For debian and derivatives)
  - 3 – Multiple users, command line (i.e. all text mode) interfaces the standard runlevel for most Linux-based server hardware
    - Console login, Fedora,Red hat
    - Network
  - 4 – user can define whatever they desire
    -
  - 5 – Multiple users, GUI; the standard runlevel for most Linux based desktop systems. Fedora ,Red hat ,Manderiea
  - 6 – Reboot; used when restarting the system

5. research on how linux manages passwd. What is Linux current first defense trend on password file management?

6. Research on Suid , sgid , sticky bit and Fork , exec , alias ,

There are special permission apart from the normal file permissions read, write and execute which we set with *chmod* and *chown* commands. They are SUID, SHID, Sticky Bit, alias, SUDO, SELinux font granular file nd folder management by Linux administrator.

- ✓ SUID (Set owner User ID up on execution)- is a special type of file permission type given to a file. Normally in Linux/Unix when a program runs, it inherits access permissions from the logged in user. SUID is defined as giving temporary permissions to a user to run a program/file with the permissions of the file owner rather that the user who runs it. In simple words users will get file owners permissions as well as owner UID and GID when executing a file/program command
- ✓ SGID (Set Group ID up on execution) is a type of file permissions given to a file/folder. Same as SUID but in this case, with the permission of the file group permissions to become member of that group to execute the file. (get file group's permission when executing a Folder/File/program/command)
- ✓ Sticky bit – when set ON, the deletion of the folder is only possible by the owner of the folder. This prevents users with write permission from deleting the folder. It's a security measure to a void deletion critical folder and their contents tho having full permission

- ✓ Fork – creating a new process by duplicating the calling process. Referred as child process. Child process Is an exact duplicate of the parent process except; the child has its own unique process ID, child's parent process ID is the same as the parent's process ID

- ✓ Exec – replaces the current program in the current process, without forking a new process. Not something used in everyday script

7. **Maggie or Bini**