User use recognizable words. 4 not use

User authorisations & authorization The normal user authentication is based upon the user being able to provide the correct username and password. The username is not something that has to be kept secret as it is readable by anyone on the system however the password is encrypted and should only be known by the user.

The algorithm used to encrypt the password is a one way password which cannot be reversed. Instead when a user enters their password it is encrypted using the same algorithm and compared against the original. Traditionally in UNIX the password was kept in the /etc/passwd file which was readable by all users on the system.

Modern Linux distributions use a shadow password file with restricted read permissionPasswords: It’s the most important security feature and basic mean of authentication its important to set secure ungues sable password security is most critical means to protect a system a good password is always desireable not to be compromised the system Linux Have some characteristics of password storing mechanism. i) In a file that is readable only by root. ii) ii) In a one way hash format. This how you can make your password strong1 Use of shadow passwords. 2 not use only words or numbers.

3 not use recognizable words. 4 not use hacker terminology. 5 not use personal Information. 6 not invert recognizable words. 7 Make the password at least eight characters long.

8 Mix upper and lower case letters. 9 Mix letters and numbers. 10 Include non-alphanumeric characters File Systems SecurityFile systems security is

important to keep a system safe. By changingimportant file like server configuration, network configuration and systemconfiguration a computer can be compromised. A file system is the methods and data structures that is use by operating system uses to keep the track of files on a disk or partition that is, the way the files are organized on the disk. The central concepts of Linux file systems are super block, inode, data block, directory block, and indirection block. The super block contains information about the file system as a whole, such as its size. An inode contains all information about a file, except its name.

The name is stored in the directory, together with the number of the inode. A directory entry consists of a filename and the number of the inode which represents the file. NFS (Network File System) Security. NFS is a very widely-used file sharing protocol. It allows servers running nfsd and mountd to export entire file systems to other machines using NFS filesystem support built in to their kernels or some other client support if they are not Linux machines. mountd keeps track of mounted file systems in /etc/mtab, and can display them with show amount.

if you must use NFS, make sure that you export to only those machines that you really need. Don’t export your entire root directory export only directories you need to exportSecuring NFSBefore implementing an NFS server first we have to secure thePORTMAP services. The PORTMAP service is a dynamic port assignmentdaemon for RPC services. It has weak authentication mechanisms and hasthe ability to assign a wide range of ports for the services it controls. For these reasons, it is difficult to secure Linux provides a number of way to secure the PORTMAP, for this we have to

do following things? Protect portmap With TCP Wrappers.? Protect portmap With iptables FirewallsFirewalls are used to control what information is allowed into and out of your local network.

the firewall host is connected to the Internet and your local LAN, and the only access from your LAN to the Internet is through the firewall. This way the firewall can control what is coming in and going out from the Internet and your LAN. There are a number of types of firewalls and methods of setting them up.

Linux machines make good firewalls. Firewall code can be built right into 2. 0 and higher kernels. The user-space tools ipfwadm for 2. 0 kernels and ipchains for 2. 2 kernels, allows you to change, on the fly, the types of network traffic you allow.

You can also log particular types of network traffic . Firewalls are a very useful and important technique in securing your network