Privilege Escalation

This rules have to be followed while operating a server or a system

→ never use root account by default
→ set the root ssh login to deny by default so nobody can root login via ssh

→ if you need extra permission then use the sudo command

→ sudo takes a command and execute it as a root

→ the sudo program looks the sudoers file and see whu is authorized to do what

→ if any user other that root is allowed to do anything in sudoers file he can perform this command with his password

→ a timeout config should be made to expires his sudo privileges

sudo takes log of

→ what command is used
→ who run this command
→ the directory the command is run from
→ time of the command that is executed

sudoers file take the
→ permission information
→ what permission to give whom
→ the hosts from where the command is given
→ the commands a specific user can run