FIREWALL (ufw)

there are several software based firewall in linux operating system they are ufw that is used in the ubuntu based os and the firewalld that is used in the centos based system.it actually based on two things the ip filter and the **iptables** .ip tables is a packet filtering mechanism and ip tables is a firewall however the iptabes is hard to understand and difficult to implement thats why we use this firewall but you can use the iptables if you want

ufw stands for uncomplicated firewall.
To get the status for what the ufw doing or is it enable or disable

=>ufw status

to enable it

=> **ufw enable**

to see the default firewall rule the command is

=>**ufw status verbose**

to see the iptables rules that is created by the ufw the command is

=> **ufw show raw**

to open a port in the ufw

=> **ufw allow 53/udp** [thats the dns thats why it udp]

if we want to enable ssh
we can directly apply it in this command

=>ufw allow ssh

it will allow the ssh

suppose we want to allow communication from another system of ip address of 192.168.0.22 and it will connect through the ssh and it can access other port too

command is
=>ufw allow from 192.168.0.22 to any port on port 22

if we want to deny the http port by firewall which is port 80 [https is 443]

then we can deny the acess using this command

=>ufw deny 80

after changing the firewall rules if we want to know which one is affected the command is

=>ufw status numbered

it will show a list of the firewall that we make changes

FIREWALL (firewalld)

likw the ubuntu system the redhat and the centos system also use a software based firewall which is firewalld

to see the state that are fierwall has we use this comamnd

=>firewall-cmd –state

to start the firewall

=>systemctl start firewalld

stop the firewall

=>systemctl stop firewalld

it will show the firewall status

in the centos/Red Hat based system there is a concept of zone like public zone work zone so if we want to make any port avilabe to everyone we can add it to the public zone.you can make any coustom zone and add different port with it then all the

to get the default zone

=>firewall-cmd --get-zones

This command will give you the default zone

in the standered zone the public zone is the only zone that is populated

to get al the default services this command is used

=> **firewall-cmd –get-services**

this will give you all the default services that is affected by the firewall

to add a services in a firewall

to add a port parmanently

=>firewall-cmd –permanent –add-port=<port>/(tcp/udp)

for adding the ssh port which is 22 permanently

=>firewall-cmd –permanent –add-port=22/tcp

to make this change in effect we must reload the firewall

=>firewall-cmd –reload

to add a service in public or accessible for all the command is

=>firewall-cmd –zone=public –add-service=http

[firewall is used to stop service that is not needed to decrease the attack surface]