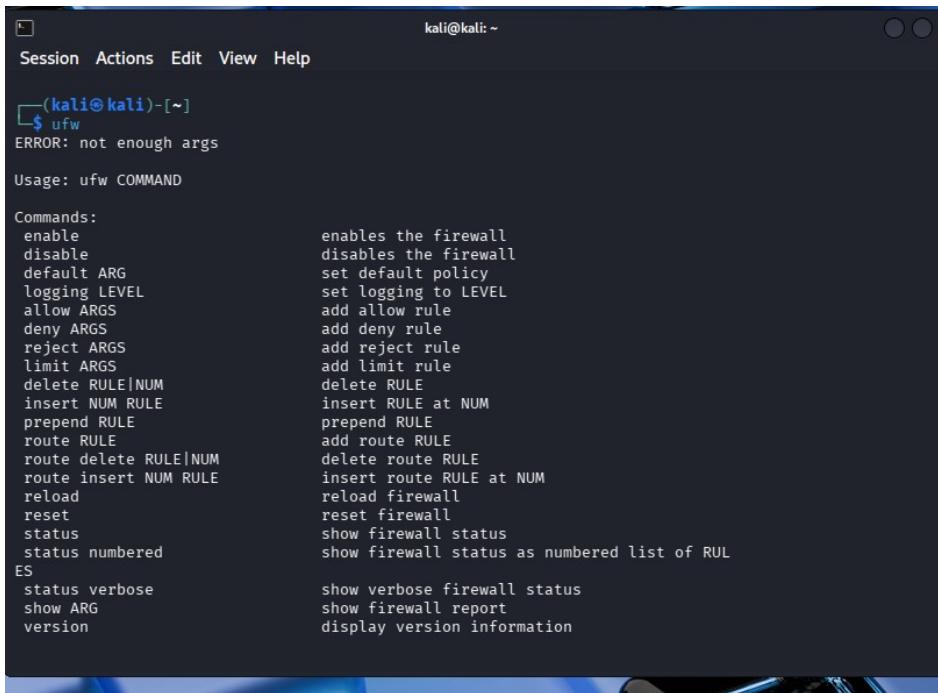


Task – 4

Configuring a firewall (Linux)

Step 1: Install ufw using any suitable package manager like dnf, pacman, apt, etc... I will be using apt.

Step 2: Check whether ufw is properly installed by typing ufw in the terminal:



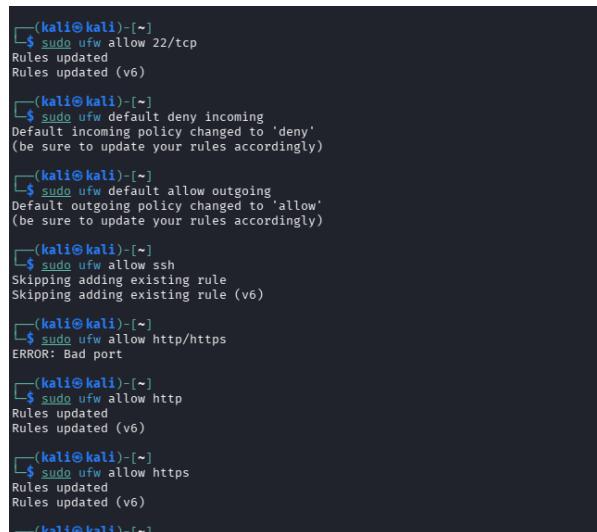
A screenshot of a terminal window titled "kali@kali: ~". The window shows the output of the command "ufw". It starts with an error message "ERROR: not enough args", followed by usage information "Usage: ufw COMMAND", and a detailed list of commands and their descriptions. The commands listed include enable, disable, default, logging, allow, deny, reject, limit, delete, insert, prepend, route, route delete, route insert, reload, reset, status, status numbered, ES, status verbose, show ARG, and version.

```
(kali㉿kali)-[~]
$ ufw
ERROR: not enough args

Usage: ufw COMMAND

Commands:
enable           enables the firewall
disable          disables the firewall
default          set default policy
logging LEVEL   set logging to LEVEL
allow ARGS      add allow rule
deny ARGS       add deny rule
reject ARGS     add reject rule
limit ARGS      add limit rule
delete RULE|NUM delete RULE
insert NUM RULE insert RULE at NUM
prepend RULE    prepend RULE
route RULE      add route RULE
route delete RULE|NUM delete route RULE
route insert NUM RULE insert route RULE at NUM
reload          reload firewall
reset           reset firewall
status          show firewall status
status numbered show firewall status as numbered list of RULES
ES              show verbose firewall status
status verbose  show firewall report
show ARG        display version information
```

Step 3: Exploring different configurations such as allow certain ports, change default ports, allowing services, deny/allow incoming/outgoing requests.



A screenshot of a terminal window titled "(kali㉿kali)-[~]". The window shows several commands run using "sudo ufw". The commands include allowing port 22/tcp, changing the default incoming policy to 'deny', changing the default outgoing policy to 'allow', allowing ssh, allowing http/https, and attempting to allow http (which fails due to a bad port). Each command outputs the number of rules updated.

```
(kali㉿kali)-[~]
$ sudo ufw allow 22/tcp
Rules updated
Rules updated (v6)

(kali㉿kali)-[~]
$ sudo ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)

(kali㉿kali)-[~]
$ sudo ufw default allow outgoing
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)

(kali㉿kali)-[~]
$ sudo ufw allow ssh
Skipping adding existing rule
Skipping adding existing rule (v6)

(kali㉿kali)-[~]
$ sudo ufw allow http/https
ERROR: Bad port

(kali㉿kali)-[~]
$ sudo ufw allow http
Rules updated
Rules updated (v6)

(kali㉿kali)-[~]
$ sudo ufw allow https
Rules updated
Rules updated (v6)

(kali㉿kali)-[~]
```

Step 4: Get the firewall working

```
(kali㉿kali)-[~]
└─$ sudo ufw enable
Firewall is active and enabled on system startup

(kali㉿kali)-[~]
└─$
```

Now, the specified ports will be receiving incoming and outgoing requests, all the others will only be used for outgoing requests. Hence, this system will be under your control as in, no port scan will detect any other ports to perform attack except the ones that are allowed by you, specifically.