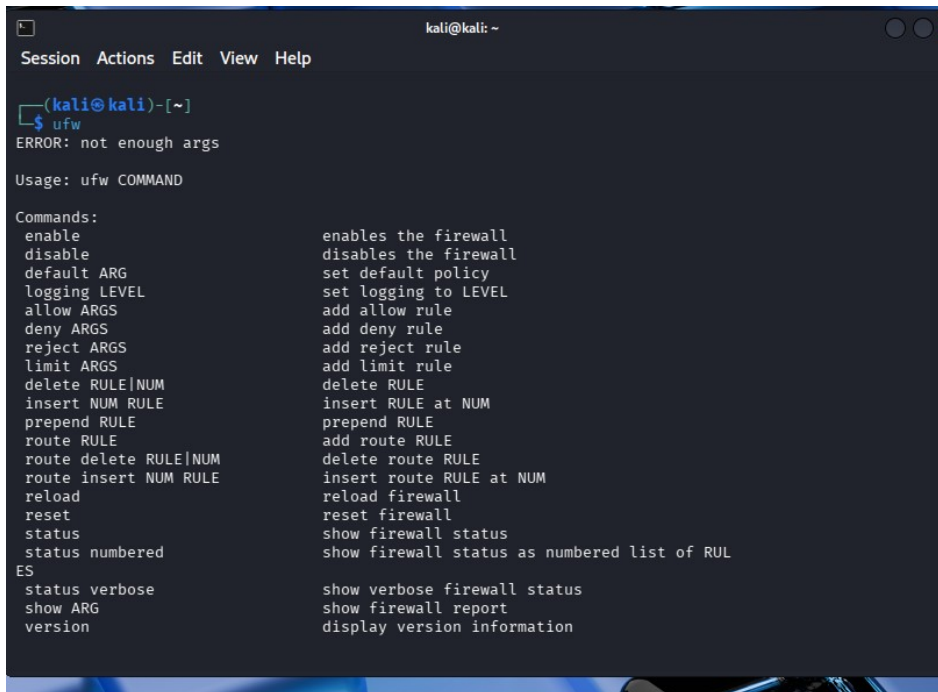


Task – 4

Configuring a firewall (Linux)

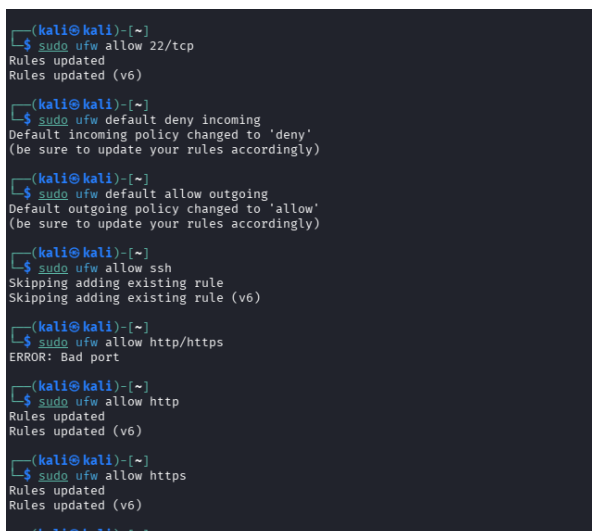
Step 1: Install ufw using any suitable package manager like dnf, pacman, apt, etc... I will be using apt.

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

A terminal window titled 'kali@kali: ~' showing the output of the 'ufw' command. The output displays the usage and a list of commands for the ufw firewall. The commands listed include: enable, disable, default ARG, logging LEVEL, allow ARGS, deny ARGS, reject ARGS, limit ARGS, delete RULE|NUM, insert NUM RULE, prepend RULE, route RULE, route delete RULE|NUM, route insert NUM RULE, reload, reset, status, status numbered, status verbose, show ARG, and version. Each command is followed by a brief description of its function.

```
kali@kali: ~  
Session Actions Edit View Help  
  
(kali@kali)-[~]  
$ ufw  
ERROR: not enough args  
  
Usage: ufw COMMAND  
  
Commands:  
enable                enables the firewall  
disable               disables the firewall  
default ARG            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 RUL  
ES  
status verbose       show verbose firewall status  
show ARG             show firewall report  
version              display version information
```

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

A terminal window titled '(kali@kali)-[~]' showing a series of ufw configuration commands and their outputs. The commands include: 'sudo ufw allow 22/tcp', 'sudo ufw default deny incoming', 'sudo ufw default allow outgoing', 'sudo ufw allow ssh', 'sudo ufw allow http/https', 'sudo ufw allow http', and 'sudo ufw allow https'. The outputs show the rules being updated and the default policies being changed.

```
(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.