**Name: Shangirne Kharbanda**

**Registration Number: 20BAI1154**

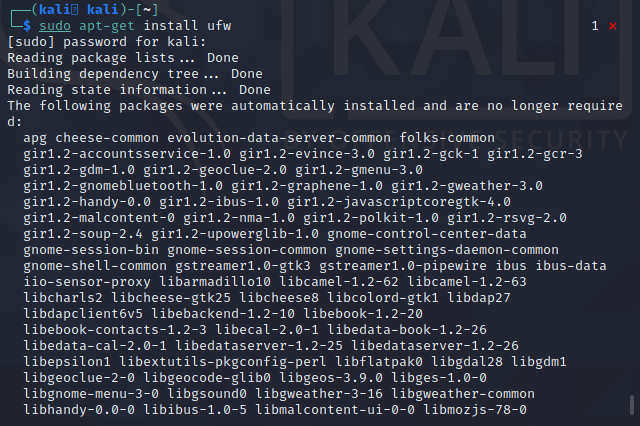
**ISM LAB – 9**

**UFW**

In this lab, we will configure an Uncomplicated Firewall(UFW) in our Linux machine. We will follow a series of steps to achieve this.

Step 1. Installation

First, we will install the UFW in our Kali machine.



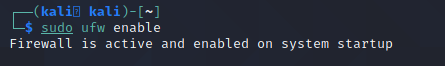
Step 2. Checking Status of UFW

Now we check its status.



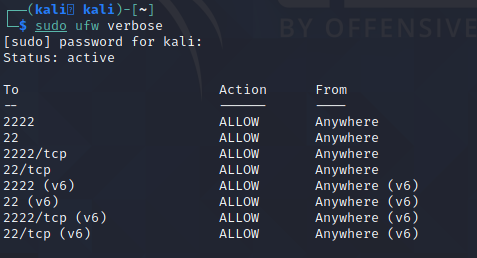
Step 3. Enabling the firewall

Enable the firewall as shown in the following screenshot



Step 4. Enabling verbose output

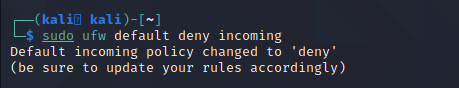
Enable verbose output using command sudo ufw verbose



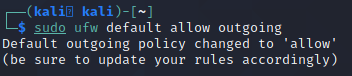
Now we will configure UFW rules.

Step 5. Configuring Traffic Rules

To deny incoming traffic, we use the following command

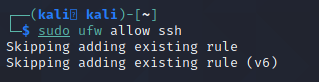


To allow outgoing traffic by default, we use the following command.



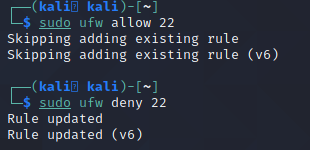
Step 6. SSH Rules

To allow ssh traffic, we use the following command.



Step 7. Port rules

We can allow or deny traffic on any port like port 22 which is the port for SSH by using the following commands shown in the screenshot.



Step 8. Allowing or denying HTTP/HTTPS traffic

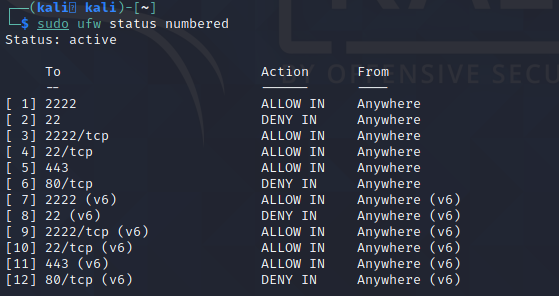
We can allow or deny HTTP/HTTPS by using the commands shown in the screenshot below.

As HTTPS is more secure, we can enable that and deny HTTP as HTTP is less secure and does not use TLS 1.3 while HTTPS does.



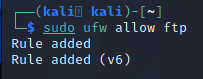
Step 9. Numbering of the rules

We can output the numbered rules using the command in the following screenshot.



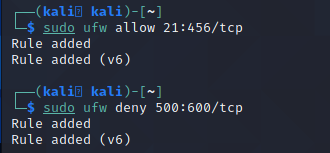
Step 10. Adding of additional rules like FTP

We can add additional rules like allowing or denying FTP as shown below.



Step 11. Port number rules

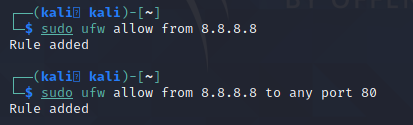
We can allow or deny traffic on a certain port number, like denying TCP traffic on a certain port. We can achieve this by following the command shown in the below screenshot.



Step 12. IP Rules

We can also allow or deny traffic coming from a specific IP address using the UFW.

We can achieve this by following the commands in the below screenshot.



We can deny traffic from the Metasploitable 2 machine to our port 80 as well.



Step 13. Subnet Rules

We can allow or deny traffic in a particular subnet.

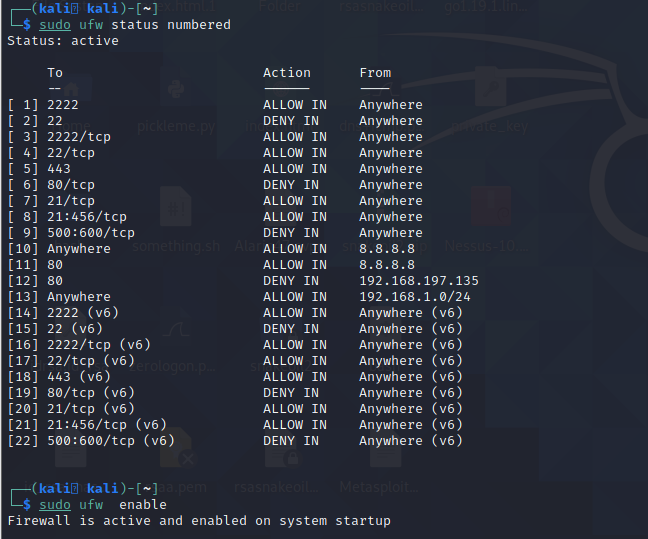
For example 192.168.1.0/24 has a CIDR notation of /24 which means it has 256 IP addresses available and 254 usable host IP addresses.

When we allow traffic in that subnet range of 192.168.1.1 – 192.168.1.254.



Step 14. Checking the final rule list and enabling the rules

We can check the final rule list and enable the rules by following what is given in the following screenshot.



Step 14. Deleting the Rules from the rule set

We can delete any rule from the rule set created by typing in the following command shown in the following screenshot.

