Name: Muhammad Usman Ali Sadiq

Cyber Security

Company: Digital Empowerment Network

Task 04

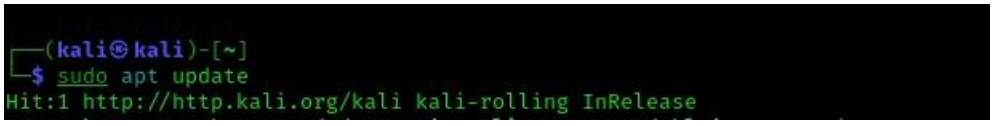
Configuring Firewalls and Intrusion Detection Systems

- **Selecting appropriate firewall and IDS solutions.**
- **Configuring firewall rules and policies.**
- **Setting up IDS to monitor network traffic.**
- **Analyzing IDS alerts and responding to threats.**
- **Regularly updating and maintaining the configurations**

Step 1: Installing and Configuring the Firewall

Install UFW (Uncomplicated Firewall)

1. Open the terminal and update your package list:



Install UFW:

```
┌──(kali㉿kali)-[~]
└─$ sudo apt install ufw

The following packages were automatically installed and are no longer required:
  fonts-liberation2  libboost-iostreams1.83.0  libgeos3.12.2  libgtk2.0-0t64     libmfx1               libpython3.11t64          python3-hatchling  python3-setuptools-scm
  hydra-gtk          libboost-thread1.83.0     libgfapi0      libgtk2.0-bin      libplist3             librados2                 python3-jose       python3-trove-classifiers
  ibverbs-providers  libcephfs2                libgfrpc0      libgtk2.0-common   libpoppler134         librdmacm1t64             python3-lib2to3    python3.11
  libarmadillo12     libgail-common            libgfxdr0      libibverbs1        libpython3.11-dev     libusbmuxd6               python3-pathspec   python3.11-dev
  libassuan0         libgail18t64              libglusterfs0  libimobiledevice6  libpython3.11-minimal linux-image-6.6.15-amd64  python3-pluggy     python3.11-minimal
  libblosc2-3        libgdal34t64              libgspell-1-2  libiniparser1      libpython3.11-stdlib  python3-hatch-vcs         python3-rsa        samba-vfs-modules
Use 'sudo apt autoremove' to remove them.

Installing:
  ufw

Suggested packages:
  rsyslog

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 34
  Download size: 168 kB
  Space needed: 880 kB / 55.0 GB available

Get:1 http://mirror.karneval.cz/pub/linux/kali kali-rolling/main amd64 ufw all 0.36.2-6 [168 kB]
Fetched 168 kB in 3s (55.1 kB/s)
Preconfiguring packages ...
Selecting previously unselected package ufw.
(Reading database ... 411579 files and directories currently installed.)
Preparing to unpack .../archives/ufw_0.36.2-6_all.deb ...
Unpacking ufw (0.36.2-6) ...
Setting up ufw (0.36.2-6) ...

Creating config file /etc/ufw/before.rules with new version

Creating config file /etc/ufw/before6.rules with new version

Creating config file /etc/ufw/after.rules with new version

Creating config file /etc/ufw/after6.rules with new version
update-rc.d: We have no instructions for the ufw init script.
update-rc.d: It looks like a non-network service, we enable it.
Created symlink '/etc/systemd/system/multi-user.target.wants/ufw.service' → '/usr/lib/systemd/system/ufw.service'.
Processing triggers for kali-menu (2024.3.1) ...
Processing triggers for man-db (2.13.0-1) ...
```

Enable UFW

```
┌──(kali㉿kali)-[~]
└─$ sudo ufw enable

Firewall is active and enabled on system startup
```

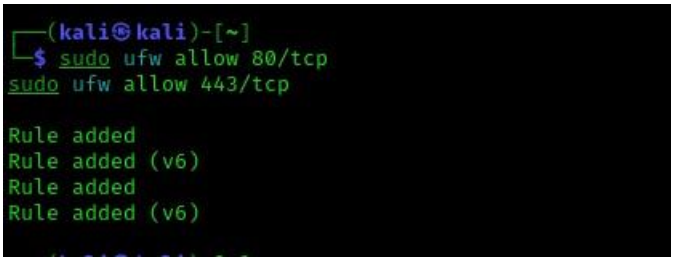
Set Basic Firewall Rules

Now, you can set up firewall rules. For example, allow SSH (port 22) and block all other incoming connections by default.

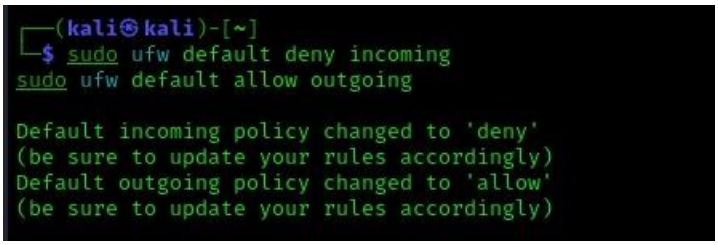
Allow SSH:

```
┌──(kali㉿kali)-[~]
└─$ sudo ufw allow ssh

Rule added
Rule added (v6)
```

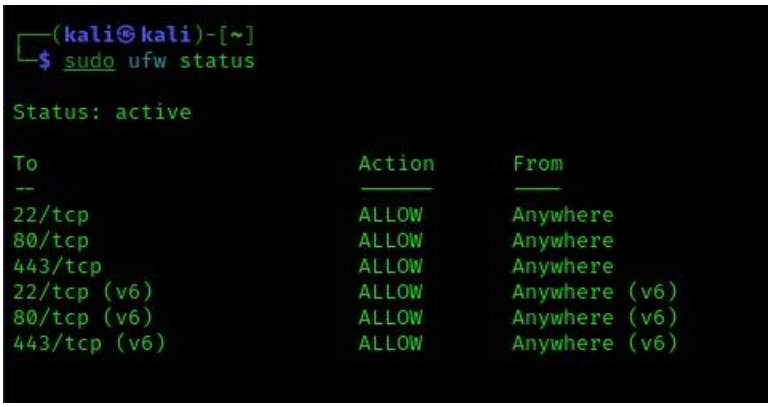
Allow HTTP (port 80) and HTTPS (port 443):



Deny all other incoming traffic and allow outgoing traffic:



Check the status of UFW rules:

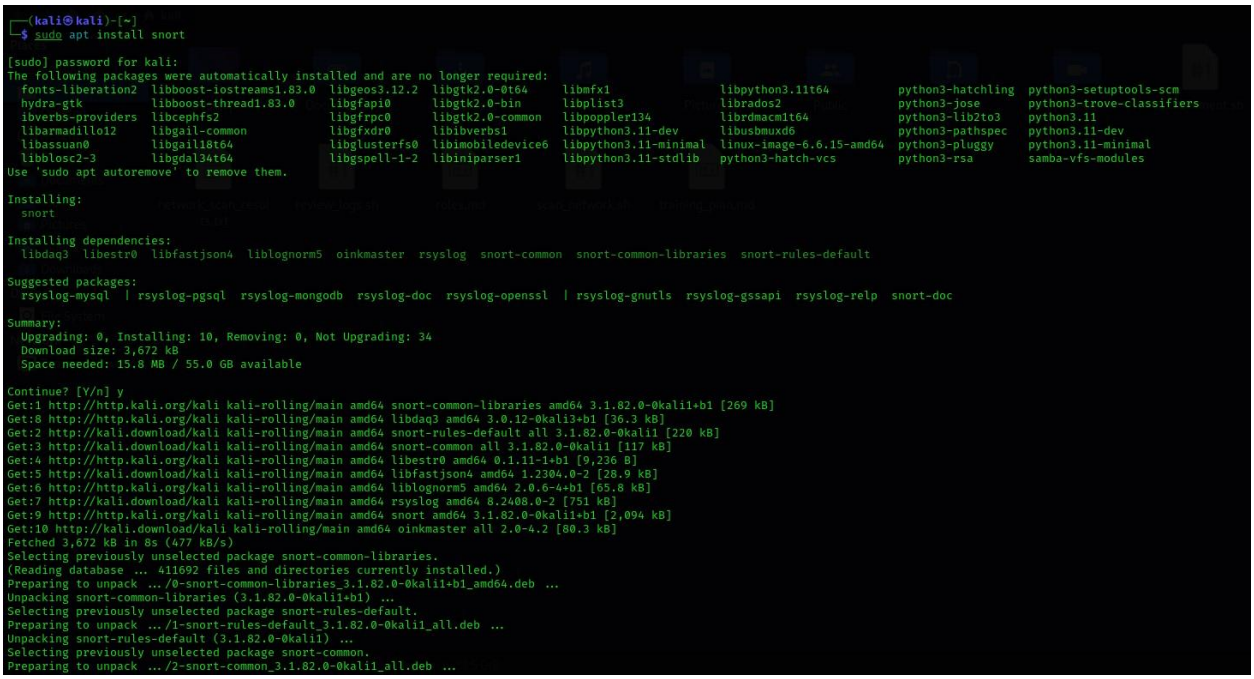


Step 2: Installing and Configuring IDS (Snort)

Install Snort

Snort is a popular open-source IDS. To install it, follow these steps:

Install Snort:



Configure Snort

Once Snort is installed, it needs to be configured to monitor network traffic.

1. Edit the Snort configuration file:

Set the network you want to monitor: Find the line that defines HOME_NET and set it to your network range:

```
var HOME_NET 192.168.1.0/24
```

Update the rule paths if necessary. By default, Snort's rules are located in /etc/snort/rules.

Running Snort

You can run Snort in different modes such as intrusion detection or packet logging.

- To run Snort in IDS mode:

```
┌──(kali㉿kali)-[~]
└─$ sudo snort -A console -q -c /etc/snort/snort.conf -i eth0
```

This command will display alerts on the console based on the rules configured in Snort.

Step 3: Analyzing IDS Alerts

Viewing Alerts

Snort generates alerts and logs them in specific directories. You can view these alerts in the console if running in alert mode, or you can check the log files:

1. Snort logs are usually stored in /var/log/snort/. Use the following command to view them:

```
┌──(kali㉿kali)-[~]
└─$ sudo cat /var/log/snort/alert
```

You can also check specific packet logs or capture files using:

```
┌──(kali㉿kali)-[~]
└─$ sudo snort -r /path/to/logfile.pcap
```

Step 4: Regular Maintenance

Updating Firewall Rules

Firewall rules should be updated regularly depending on new network policies or changes in the environment.

- To remove a rule, use:

```
┌──(kali㉿kali)-[~]
└─$ sudo ufw delete allow ssh
Rule deleted
Rule deleted (v6)
```

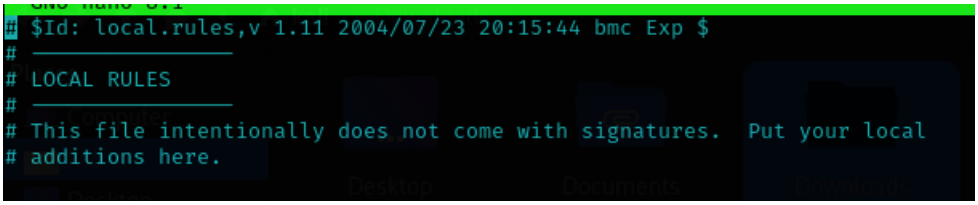
To list all firewall rules:

```
┌──(kali㉿kali)-[~]
└─$ sudo ufw status numbered

Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 80/tcp                     ALLOW IN    Anywhere
[ 2] 443/tcp                    ALLOW IN    Anywhere
[ 3] 80/tcp (v6)                ALLOW IN    Anywhere (v6)
[ 4] 443/tcp (v6)               ALLOW IN    Anywhere (v6)
```

Updating Snort Rules

Snort rules can be updated manually or using tools like **PulledPork**.

- To update the rules manually:



- Add your custom rules here.
- Restart Snort after making rule changes: