

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:

```
(kali@kali)-[~]  
$ sudo apt update  
Hit:1 http://http.kali.org/kali kali-rolling InRelease
```

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 libgsoap10 libgtk2.0-bin libplist3 librados2 python3-jose python3-trove-classifiers
 libverbs-providers libcephfs2 libgfs0 libgtk2.0-common libpoppler134 librdmacm1t64 python3-lib2to3 python3-trove-classifiers
 libarmadillo12 libgail-common libgfsxdr0 libibverbs1 libpython3.11-dev libusbmuxd6 python3-pathspect python3.11-dev
 libassuan0 libgail18t64 libglusterfs0 libmobiledevice6 libpython3.11-minimal linux-image-6.6.15-amd64 python3-pluggy python3.11-minimal
 libblosc2-3 libgdal34t64 libgspell1-1-2 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):

```
(kali㉿kali)-[~]  
$ sudo ufw allow 80/tcp  
sudo ufw allow 443/tcp  
  
Rule added  
Rule added (v6)  
Rule added  
Rule added (v6)
```

Deny all other incoming traffic and allow outgoing traffic:

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

Check the status of UFW rules:

```
(kali㉿kali)-[~]  
$ sudo ufw status  
  
Status: active  
  
To Action From  
--  
22/tcp ALLOW Anywhere  
80/tcp ALLOW Anywhere  
443/tcp ALLOW Anywhere  
22/tcp (v6) ALLOW Anywhere (v6)  
80/tcp (v6) ALLOW Anywhere (v6)  
443/tcp (v6) ALLOW Anywhere (v6)
```

Step 2: Installing and Configuring IDS (Snort)

Install Snort

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

Install Snort:

```
(kali@kali)-[~]
$ sudo apt install snort

[sudo] password for kali:
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 libgfat10 libgtk2.0-bin liblist3 librados2 python3-jose python3-trove-classifiers
libverbs-providers libcephfs2 libgfrpc0 libgtk2.0-common libpoppler134 librdmacm1t64 python3-lib2to3 python3-trove-classifiers
libamadillo12 libgail-common libgfrpc0 liblibverbs1 libpython3.11-dev libusbmuxd6 python3-lib2to3 python3-trove-classifiers
libassuan0 libgail18t64 libglusterfs0 libmobiledevice6 libpython3.11-minimal linux-image-6.6.15-amd64 python3-pluggy python3.11-minimal
liblouis2-3 libgdal34t64 libgssapi-1-2 libiniparser1 libpython3.11-stdlib python3-hatch-vcs python3-rsa samba-vfs-modules

Use 'sudo apt autoremove' to remove them.

Installing:
snort

Installing dependencies:
libdaq3 libestr0 libfastjson4 liblognorm5 oinkmaster rsyslog snort-common snort-common-libraries snort-rules-default

Suggested packages:
rsyslog-mysql | rsyslog-psql rsyslog-mongodb rsyslog-doc rsyslog-openssl | rsyslog-gnutls rsyslog-gssapi rsyslog-relp snort-doc

Summary:
Upgrading: 0, Installing: 10, Removing: 0, Not Upgrading: 34
Download size: 3,672 kB
Space needed: 15.8 MB / 55.0 GB available

Continue? [Y/n] y
Get:1 http://http.kali.org/kali kali-rolling/main amd64 snort-common-libraries amd64 3.1.82.0-0kali1+b1 [269 kB]
Get:2 http://http.kali.org/kali kali-rolling/main amd64 libdaq3 amd64 3.0.12-0kali1+b1 [36.3 kB]
Get:3 http://http.kali.org/kali kali-rolling/main amd64 snort-rules-default all 3.1.82.0-0kali1 [220 kB]
Get:4 http://http.kali.org/kali kali-rolling/main amd64 libestr0 amd64 0.1.11-1+b1 [9,236 B]
Get:5 http://http.kali.org/kali kali-rolling/main amd64 libfastjson4 amd64 1.2304.0-2 [28.9 kB]
Get:6 http://http.kali.org/kali kali-rolling/main amd64 liblognorm5 amd64 2.0.6-4+b1 [65.8 kB]
Get:7 http://http.kali.org/kali kali-rolling/main amd64 rsyslog amd64 8.2408.0-2 [751 kB]
Get:8 http://http.kali.org/kali kali-rolling/main amd64 snort amd64 3.1.82.0-0kali1+b1 [2,094 kB]
Get:9 http://http.kali.org/kali kali-rolling/main amd64 oinkmaster all 2.0-4.2 [80.3 kB]
Get:10 http://http.kali.org/kali kali-rolling/main amd64 snort-common all 3.1.82.0-0kali1+b1 [2,094 kB]
Fetched 3,672 kB in 8s (477 kB/s)
Selecting previously unselected package snort-common-libraries.
(Reading database ... 411692 files and directories currently installed.)
Preparing to unpack .../0-snort-common-libraries_3.1.82.0-0kali1+b1_amd64.deb ...
Unpacking snort-common-libraries (3.1.82.0-0kali1+b1) ...
Selecting previously unselected package snort-rules-default.
Preparing to unpack .../1-snort-rules-default_3.1.82.0-0kali1+b1_all.deb ...
Unpacking snort-rules-default (3.1.82.0-0kali1+b1) ...
Selecting previously unselected package snort-common.
Preparing to unpack .../2-snort-common_3.1.82.0-0kali1+b1_all.deb ...
Unpacking snort-common (3.1.82.0-0kali1+b1) ...
```

Configure Snort

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

1. Edit the Snort configuration file:

```
(kali@kali)-[~]
$ sudo nano /etc/snort/snort.conf
```

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:

```
(kali㉿kali)-[~]  
$ sudo nano /etc/snort/rules/local.rules
```

```
cat /etc/snort/rules/local.rules  
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $  
#  
# LOCAL RULES  
#  
# This file intentionally does not come with signatures.  Put your local  
# additions here.
```

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

```
(kali㉿kali)-[~]  
$ sudo systemctl restart snort
```