

# Cybersecurity Internship Tasks

Name: Safiullah Shahid

Assignment: Task # 4

Position: Cyber Security Intern

Department: Cyber Security

Date of Submission: July 31, 2024

Company: Digital Empowerment

# Configuring Firewalls and Intrusion Detection Systems

## Setting Up firewall:

### Step 1 Install ufw

CMD: `sudo apt-get install ufw`

```
(kali㉿kali)-[~]
$ sudo apt-get install ufw
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
 fonts-noto-color-emoji libabsl20220623 libadwaita-1-0 libaio1 libappstream5 libatk-adaptor libboost-dev libboost1.83-de
 libgphoto2-l10n libndctl6 libnsl-dev libopenblas-dev libopenblas-pthread-dev libopenblas0 libpmem1 libpthread-stubs0-de
 libpython3-all-dev libpython3.12 libpython3.12-dev libre2-10 libstemmer0d libtirpc-dev libunibreak5 libxmlb2 libxsimd-d
 python3-anyjson python3-beniget python3-diskcache python3-gast python3-mistune0 python3-pendulum python3-pyatspi python
 python3-pyrsistent python3-pythran python3-pytzdata python3-zapv2 python3.12-dev xtl-dev zenity zenity-common
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
 ufw
0 upgraded, 1 newly installed, 0 to remove and 637 not upgraded.
Need to get 168 kB of archives.
After this operation, 880 kB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 ufw all 0.36.2-6 [168 kB]
Fetched 168 kB in 1min 11s (2,368 B/s)
Preconfiguring packages ...
Selecting previously unselected package ufw.
(Reading database ... 417102 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
```

### Step 2 Enable Ufw

CMD: `sudo ufw enable`

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

### Step 3 Allow Ufw on SSH

CMD: `sudo ufw allow 22/tcp`

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

#### Step 4 Check Status

CMD: `sudo ufw status verbose`

```
(kali@kali)-[~]
$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To Action From
-- websites.txt LFISuite
22/tcp ALLOW IN Anywhere
22/tcp (v6) ALLOW IN Anywhere (v6)
```

## Setting Up IDS:

#### Step 1 Install Suricata on Victim Machine

CMD: `sudo apt-get install suricata`

```
(kali@kali)-[~]
$ sudo apt-get install suricata
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
 fonts-noto-color-emoji libabsl20220623 libadwaita-1-0 libaio1 libappstream5 libatk-adaptor libboost-dev libboost1.83-dev libdaxctl1
 libgphoto2-l10n libndctl6 libnsl-dev libopenblas-dev libopenblas-pthread-dev libopenblas0 libpmem1 libpthread-stubs0-dev
 libpython3-all-dev libpython3.12 libpython3.12-dev libre2-10 libstemmer0d libtirpc-dev libunibreak5 libxmlb2 libxsimd-dev python3-all-
 python3-anyjson python3-beniget python3-diskcache python3-gast python3-mistune0 python3-pendulum python3-pyatspi python3-pypdf2
 python3-pyrsistent python3-pythran python3-pytzdata python3-zapv2 python3.12-dev xtl-dev zenity zenity-common
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
 file isa-support libevent-2.1-7t64 libevent-core-2.1-7t64 libevent-openssl-2.1-7t64 libevent-pthreads-2.1-7t64 libfdt1 libhttp2
 libhyperscan5 libmagic-dev libmagic-mgc libmagic1t64 libnetfilter-log1 librtt-bus-pci24 librtt-bus-vdev24 librtt-eal24 librtt-ethdev24
 librtt-hash24 librtt-ip-frag24 librtt-kvargs24 librtt-log24 librtt-mbuf24 librtt-mempool24 librtt-meter24 librtt-net-bond24 librtt-net-
 librtt-pci24 librtt-rcu24 librtt-ring24 librtt-sched24 librtt-telemetry24 libxdp1 sse3-support sse4.2-support sslsplit suricata-update
Suggested packages:
 libtcmalloc-minimal4
The following packages will be REMOVED:
 libevent-2.1-7 libevent-core-2.1-7 libevent-openssl-2.1-7 libevent-pthreads-2.1-7 libmagic1
The following NEW packages will be installed:
```

#### Step 2 Check Suricata's status

CMD: `sudo systemctl status suricata`

```
(kali@kali)-[~]
$ sudo systemctl status suricata
o suricata.service - Suricata IDS/IDP daemon
   Loaded: loaded (/usr/lib/systemd/system/suricata.service; disabled; preset: disabled)
   Active: inactive (dead)
     Docs: man:suricata(8)
           man:suricatasc(8)
           https://suricata.io/documentation/
```

### Step 3 Setup Suricata Configurations

CMD: `sudo vim /etc/suricata/suricata.yaml`

```
(kali㉿kali)-[~]
$ sudo vim /etc/suricata/suricata.yaml
```

```
# This configuration file generated by Suricata 7.0.6.
suricata-version:0"7.0"FW-UP>with 85526 nqisc noqueue state UNKNOWN group default nl
Link/loopback or ethernet interface bpd or ethernet interface
## inst 1 /6 scope host lo
## Step 1: Inform Suricata about your network:
## inst6 1 /128 scope host noprefixroute
        value lft forever preferred lft forever
vars: <>BROADCAST/MULTICAST,UP,LOWER_UP>with 1500 nqisc fq_codel state UP group dn
# more specific is better for alert accuracy and performance
address-groups:
    /24 bpd
    scope global dynamic noprefixroute 20
    name net 8192m add o e/o 1m o o e/o 1m o o e/o 1m
```

**Go to HOME NET**

## Step 4 Search for your Networks

CMD: ip a s

```
(kali㉿kali)-[~]
$ ip a s
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:48:52:ae brd ff:ff:ff:ff:ff:ff
    inet 192.168.67.133/24 brd 192.168.67.255 scope global dynamic noprefixroute eth0
        valid_lft 1781sec preferred_lft 1781sec
    inet6 fe80::1c3d:3e8c:dcfc:1b85/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

**Step 5** Go to HOME NET and change the ip address to your eth0 ip

```
vars:
  # more specific is better for alert accuracy and performance
  address-groups:
    HOME_NET: "[192.168.67.133/24]"
    #HOME_NET: "[192.168.0.0/16]"
    #HOME_NET: "[10.0.0.0/8]"
    #HOME_NET: "[172.16.0.0/12]"
    #HOME_NET: "any"

    EXTERNAL_NET: " !$HOME_NET"
```

**Step 6** Go to af-packet set to internet interface to your network interface

```
# Linux high speed capture support
af-packet:
- interface: eth0
  # Number of receive threads. "auto" uses the number of cores
  #threads: auto
  # Default clusterid. AF_PACKET will load balance packets based on flow.
  cluster-id: 99
  # Default AF_PACKET cluster type. AF_PACKET can load balance per flow or per hash.
  # This is only supported for linux kernel > 3.4
```

**Step 7** Go to Community id and make it true but it is optional

```
# enable/disable the community id feature.
community-id: false
# Seed value for the ID output. Valid values are 0-65535.
community-id-seed: 0
```

**Step 8** Setup rules

CMD: `sudo nano /etc/suricata/rules/local.rules`

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

Add rule: `alert icmp any any -> $HOME_NET any (msg:"ICMP Ping"; sid:1; rev:1;)`

```
GNU nano 8.1 /etc/suricata/rules/local.rules *
alert icmp any any -> $HOME_NET any (msg:"ICMP Ping"; sid:1; rev:1;)
1: ip <LOOPBACK,UP,LOWER_UP> mtu 65536 dsize noqueue state UNKNOWN group default qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
1: ip <LOOPBACK,UP,LOWER_UP> mtu 65536 dsize noqueue state UNKNOWN group default qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
```

**Step 9** Setup Suricata Configurations

CMD: `sudo vim /etc/suricata/suricata.yaml`

```
(kali㉿kali)-[~]
$ sudo vim /etc/suricata/suricata.yaml
```

Go to **rules-path**

```
rule-files:
- suricata.rules
- /etc/suricata/rules/local.rules
```

### Step 10 Update Suricata and then list sources

CMD: sudo suricata-update list-sources

```
(kali@kali)-[~]
$ sudo suricata-update list-sources
3/9/2024 -- 19:47:22 - <Info> -- Using data-directory /var/lib/suricata.
3/9/2024 -- 19:47:22 - <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml
3/9/2024 -- 19:47:22 - <Info> -- Using /etc/suricata/rules for Suricata provided rules.
3/9/2024 -- 19:47:22 - <Info> -- Found Suricata version 7.0.6 at /usr/bin/suricata.
3/9/2024 -- 19:47:22 - <Warning> -- Source index does not exist, will use bundled one.
3/9/2024 -- 19:47:22 - <Warning> -- Please run suricata-update update-sources.
Name: et/open
  Vendor: Proofpoint
  Summary: Emerging Threats Open Ruleset
  License: MIT
Name: et/pro
  Vendor: Proofpoint
  Summary: Emerging Threats Pro Ruleset
  License: Commercial
  Replaces: et/open
  Parameters: secret-code
  Subscription: https://www.proofpoint.com/us/threat-insight/et-pro-ruleset
Name: etnetera/aggressive
  Vendor: Etnetera a.s.
```

### Step 11 Enable the rule you want to add

CMD: sudo suricata-update enable-source oisf/trafficid

```
(kali@kali)-[~]
$ sudo suricata-update enable-source oisf/trafficid
3/9/2024 -- 19:53:24 - <Info> -- Using data-directory /var/lib/suricata.
3/9/2024 -- 19:53:24 - <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml
3/9/2024 -- 19:53:24 - <Info> -- Using /etc/suricata/rules for Suricata provided rules.
3/9/2024 -- 19:53:24 - <Info> -- Found Suricata version 7.0.6 at /usr/bin/suricata.
3/9/2024 -- 19:53:24 - <Warning> -- Source index does not exist, will use bundled one.
3/9/2024 -- 19:53:24 - <Warning> -- Please run suricata-update update-sources.
3/9/2024 -- 19:53:24 - <Info> -- Creating directory /var/lib/suricata/update/sources
3/9/2024 -- 19:53:24 - <Info> -- Enabling default source et/open
3/9/2024 -- 19:53:24 - <Info> -- Source oisf/trafficid enabled
```

### Step 12 Update the change in suricata

CMD: sudo suricata-update

```
(kali@kali)-[~]
$ sudo suricata-update
3/9/2024 -- 19:54:42 - <Info> -- Using data-directory /var/lib/suricata.
3/9/2024 -- 19:54:42 - <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml
3/9/2024 -- 19:54:42 - <Info> -- Using /etc/suricata/rules for Suricata provided rules.
3/9/2024 -- 19:54:42 - <Info> -- Found Suricata version 7.0.6 at /usr/bin/suricata.
3/9/2024 -- 19:54:42 - <Info> -- Loading /etc/suricata/suricata.yaml
3/9/2024 -- 19:54:42 - <Info> -- Disabling rules for protocol pgsql
3/9/2024 -- 19:54:42 - <Info> -- Disabling rules for protocol modbus
3/9/2024 -- 19:54:42 - <Info> -- Disabling rules for protocol dnp3
3/9/2024 -- 19:54:42 - <Info> -- Disabling rules for protocol enip
3/9/2024 -- 19:54:42 - <Warning> -- No index exists, will use bundled index.
3/9/2024 -- 19:54:42 - <Warning> -- Please run suricata-update update-sources.
3/9/2024 -- 19:54:42 - <Info> -- Fetching https://openinfosecfoundation.org/rules/trafficid/trafficid.rules.
```

### Step 13 Run Suricata

CMD: `sudo systemctl start suricata`

```
(kali@kali)-[~]  
$ sudo systemctl start suricata
```

### Step 14 View Logs

CMD: `sudo tail -f /var/log/suricata/fast.log`

```
(kali@kali)-[~]  
$ sudo tail -f /var/log/suricata/fast.log  
08/31/2024-00:45:18.675744 [**] [1:2022973:1] ET INFO Possible Kali Linux hostname in DHCP Request Packet [**] [Classification: Potential Corporate Privacy Violation  
[Priority: 1] {UDP} 192.168.56.102:68 → 192.168.56.100:67  
08/31/2024-00:50:18.678704 [**] [1:2022973:1] ET INFO Possible Kali Linux hostname in DHCP Request Packet [**] [Classification: Potential Corporate Privacy Violation  
[Priority: 1] {UDP} 192.168.56.102:68 → 192.168.56.100:67  
08/31/2024-00:55:18.696616 [**] [1:2022973:1] ET INFO Possible Kali Linux hostname in DHCP Request Packet [**] [Classification: Potential Corporate Privacy Violation  
[Priority: 1] {UDP} 192.168.56.102:68 → 192.168.56.100:67  
08/31/2024-01:00:18.698995 [**] [1:2022973:1] ET INFO Possible Kali Linux hostname in DHCP Request Packet [**] [Classification: Potential Corporate Privacy Violation  
[Priority: 1] {UDP} 192.168.56.102:68 → 192.168.56.100:67  
08/31/2024-01:15:19.464736 [**] [1:2022973:1] ET INFO Possible Kali Linux hostname in DHCP Request Packet [**] [Classification: Potential Corporate Privacy Violation  
[Priority: 1] {UDP} 192.168.56.102:68 → 192.168.56.100:67  
08/31/2024-01:20:19.466531 [**] [1:2022973:1] ET INFO Possible Kali Linux hostname in DHCP Request Packet [**] [Classification: Potential Corporate Privacy Violation  
[Priority: 1] {UDP} 192.168.56.102:68 → 192.168.56.100:67
```