Testing Zeeks

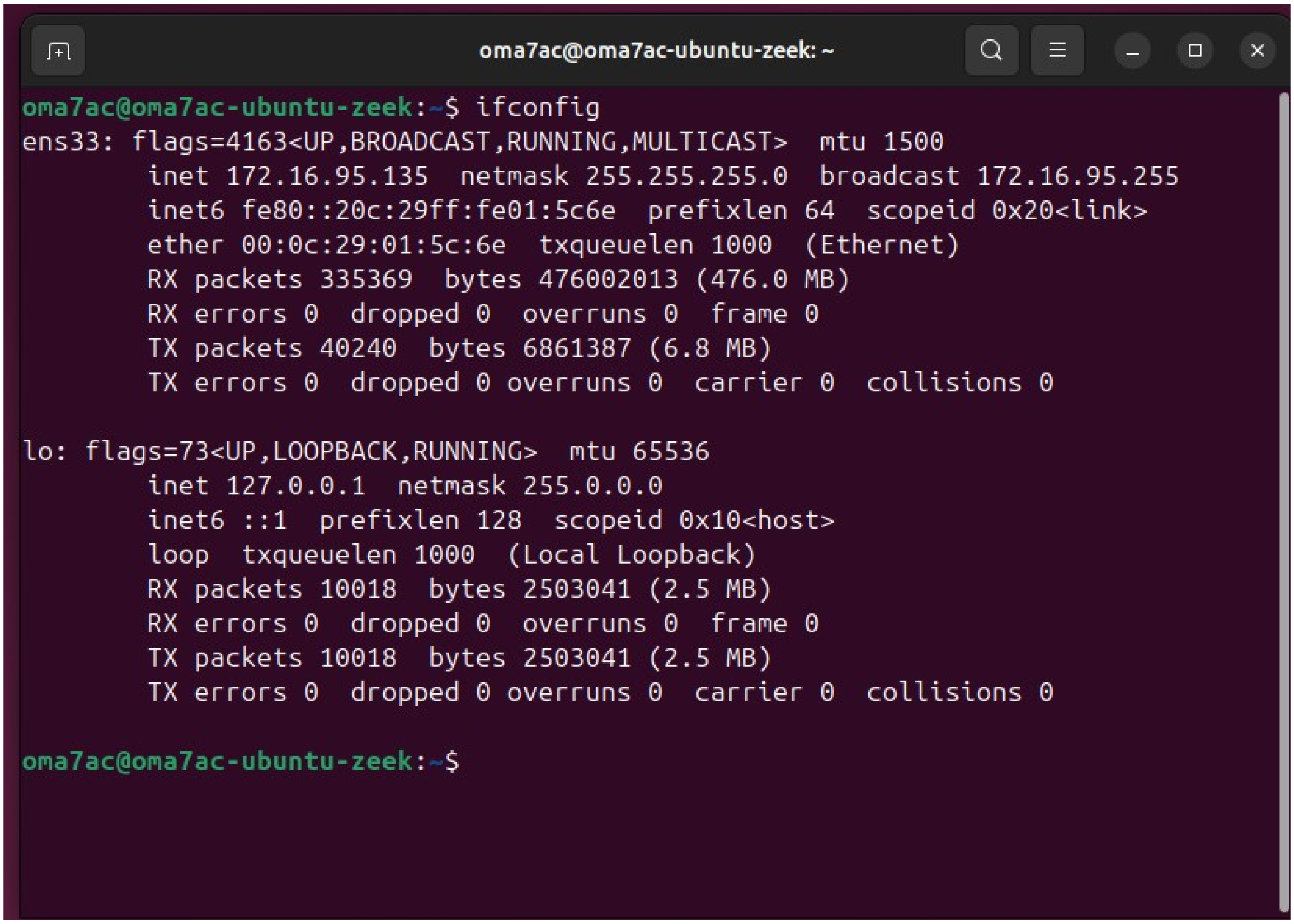
Here’s a simple guide to test Zeek logs on your Ubuntu machine, generate traffic with Nmap from Kali Linux, and view the logs in Elasticsearch.

Step 1: Check Your Ubuntu IP Address

First, you need to find the IP address of your Ubuntu machine where Zeek is running. Open a terminal on your Ubuntu machine and type:

```
ifconfig
```

This will show your network details. Look for the interface (like ens33) and find the IP address. In my case (see Figure 1.1), my Ubuntu IP is 172.16.95.135.



```
oma7ac@oma7ac-ubuntu-zeek:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.95.135  netmask 255.255.255.0  broadcast 172.16.95.255
        inet6 fe80::20c:29ff:fe01:5c6e  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:01:5c:6e  txqueuelen 1000  (Ethernet)
        RX packets 335369  bytes 476002013 (476.0 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 40240  bytes 6861387 (6.8 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 10018  bytes 2503041 (2.5 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 10018  bytes 2503041 (2.5 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

oma7ac@oma7ac-ubuntu-zeek:~$
```

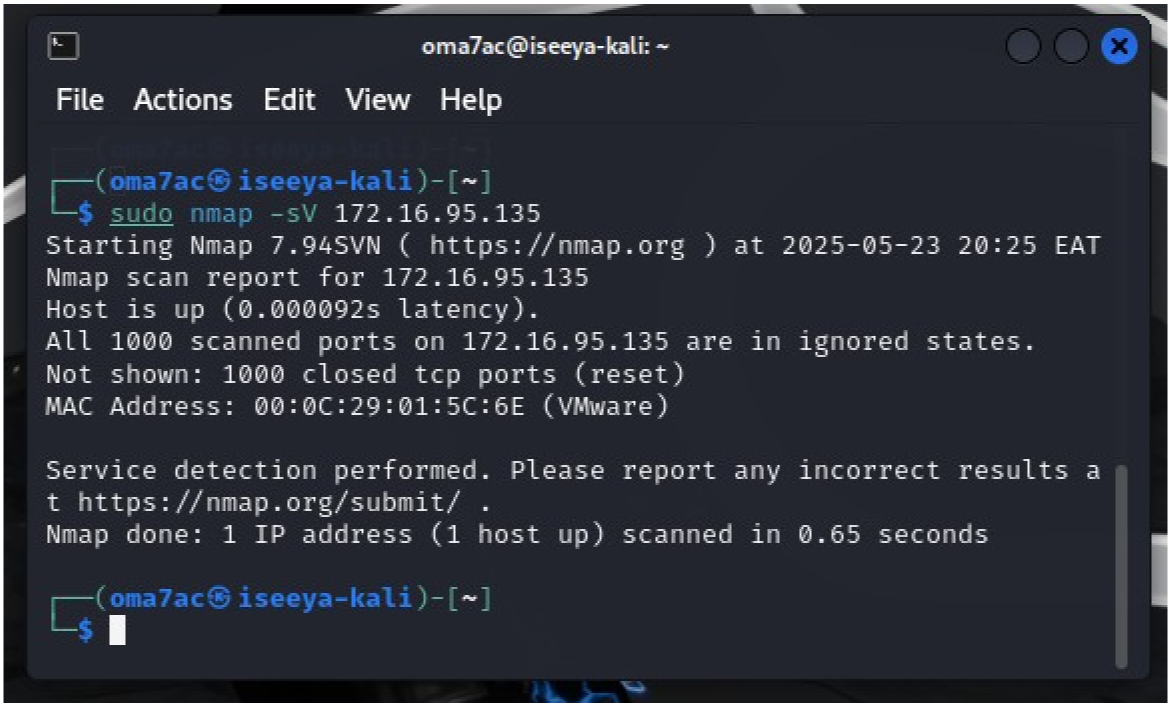
Figure 1.1: My IP address

Step 2: Go to Kali Linux and Run Nmap

Now, go to your Kali Linux machine. Open a terminal and run an Nmap scan against the Ubuntu IP to generate traffic. Use this command (replace with your Ubuntu IP):

```
sudo nmap -sV 172.16.95.135
```

This scans the IP and checks for open ports. In my test (see Figure 1.2), I ran this at 20:17 EAT and 20:25 EAT. It showed the host was up.



```
┌──(oma7ac㉿iseeya-kali)-[~]
└─$ sudo nmap -sV 172.16.95.135
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-23 20:25 EAT
Nmap scan report for 172.16.95.135
Host is up (0.000092s latency).
All 1000 scanned ports on 172.16.95.135 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 00:0C:29:01:5C:6E (VMware)

Service detection performed. Please report any incorrect results a
t https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.65 seconds

┌──(oma7ac㉿iseeya-kali)-[~]
└─$ 
```

Figure 1.2: My nmap scan screenshot

Step 3: Traffic Goes to Elasticsearch

The Nmap scan creates network traffic, and Zeek on your Ubuntu machine captures this traffic and sends the logs to Elasticsearch.

Step 4: View Zeek Logs in Elasticsearch

- Open your browser and go to your Elasticsearch dashboard.
- On the left side, click **Dashboards**.
- Search for “Zeek Logs” and select [Logs Zeek] Overview.
- You’ll see a graph called “Number of Sessions Overtime [Logs Zeek]” (like in Figure 1.3).
- This shows the traffic and logs. In my test, I saw spikes at 20:21 (~1000 sessions) beacuse and 20:23 (1,358 sessions), which match my Nmap scans.

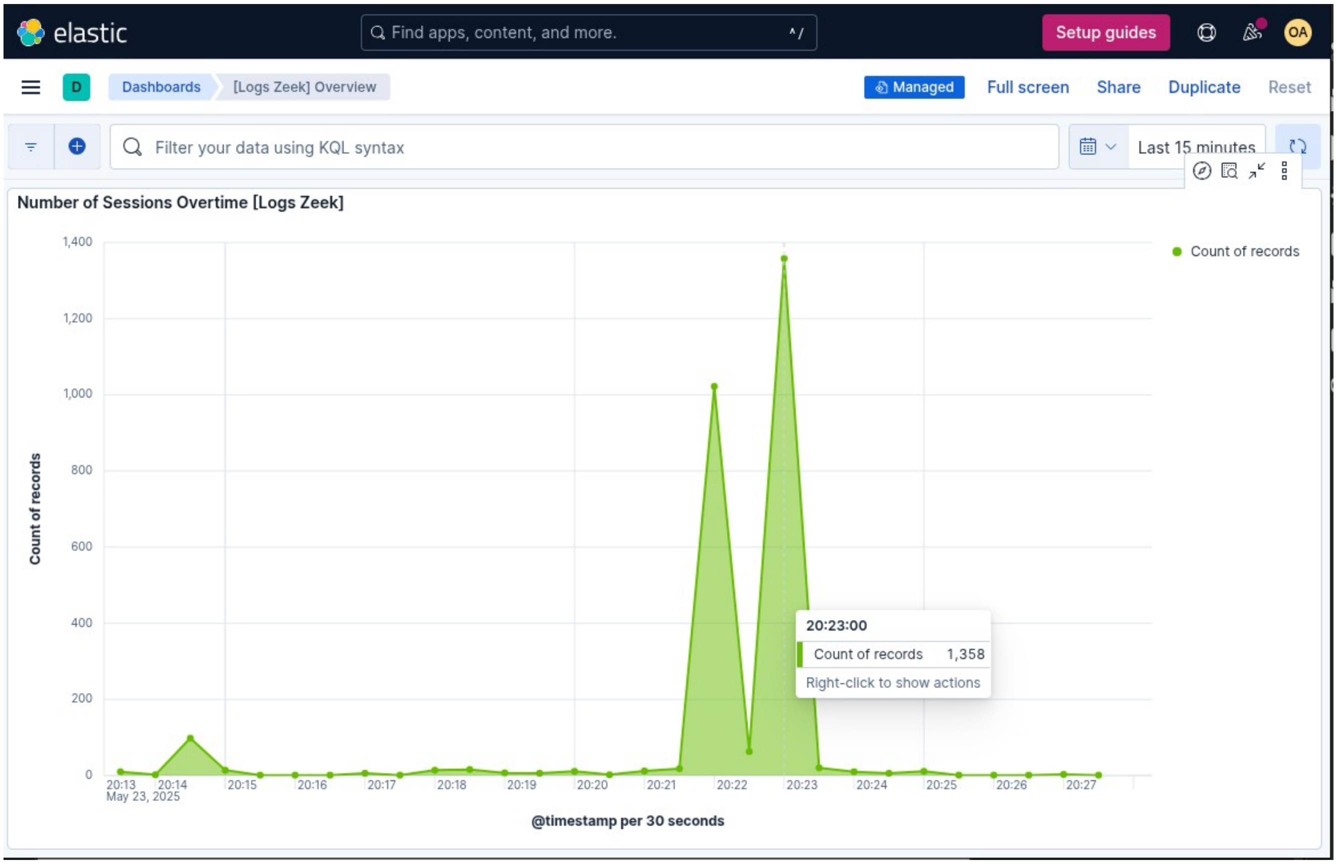


Figure 1.3: Screenshot Of Zeek Dashboard

That’s it! You can now see how Zeek captures traffic and logs it in Elasticsearch.