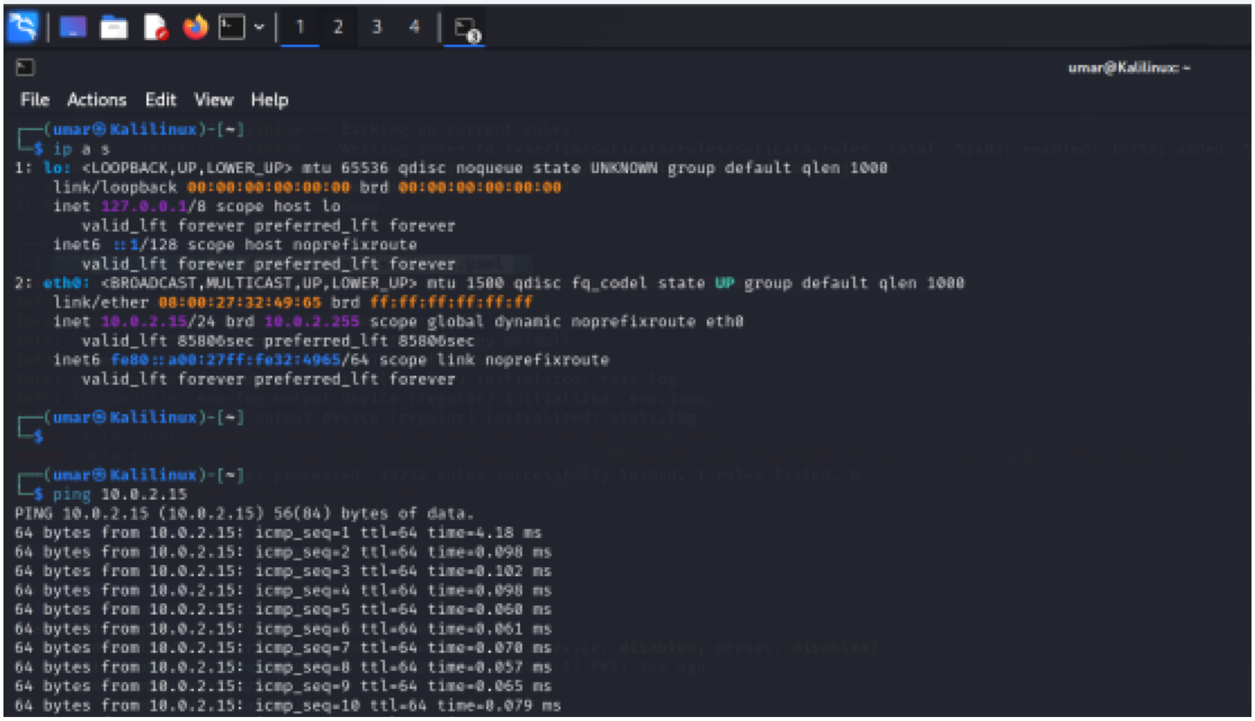
Screenshot of KaliLinux (Snapshot 1)

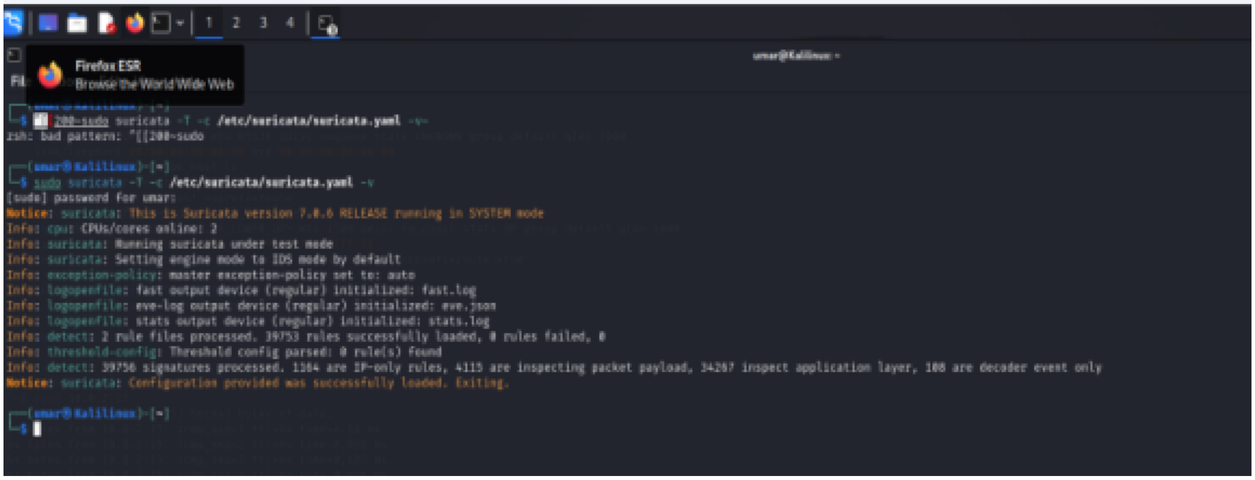


```
┌──(umar㉿Kalilinux)-[~]
└─$ ip a s
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       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 08:00:27:32:49:65 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
       valid_lft 85806sec preferred_lft 85806sec
    inet6 fe80::a00:27ff:fe32:4965/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(umar㉿Kalilinux)-[~]
└─$

┌──(umar㉿Kalilinux)-[~]
└─$ ping 10.0.2.15
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.
64 bytes from 10.0.2.15: icmp_seq=1 ttl=64 time=4.18 ms
64 bytes from 10.0.2.15: icmp_seq=2 ttl=64 time=0.098 ms
64 bytes from 10.0.2.15: icmp_seq=3 ttl=64 time=0.102 ms
64 bytes from 10.0.2.15: icmp_seq=4 ttl=64 time=0.098 ms
64 bytes from 10.0.2.15: icmp_seq=5 ttl=64 time=0.060 ms
64 bytes from 10.0.2.15: icmp_seq=6 ttl=64 time=0.061 ms
64 bytes from 10.0.2.15: icmp_seq=7 ttl=64 time=0.070 ms
64 bytes from 10.0.2.15: icmp_seq=8 ttl=64 time=0.057 ms
64 bytes from 10.0.2.15: icmp_seq=9 ttl=64 time=0.065 ms
64 bytes from 10.0.2.15: icmp_seq=10 ttl=64 time=0.079 ms
```

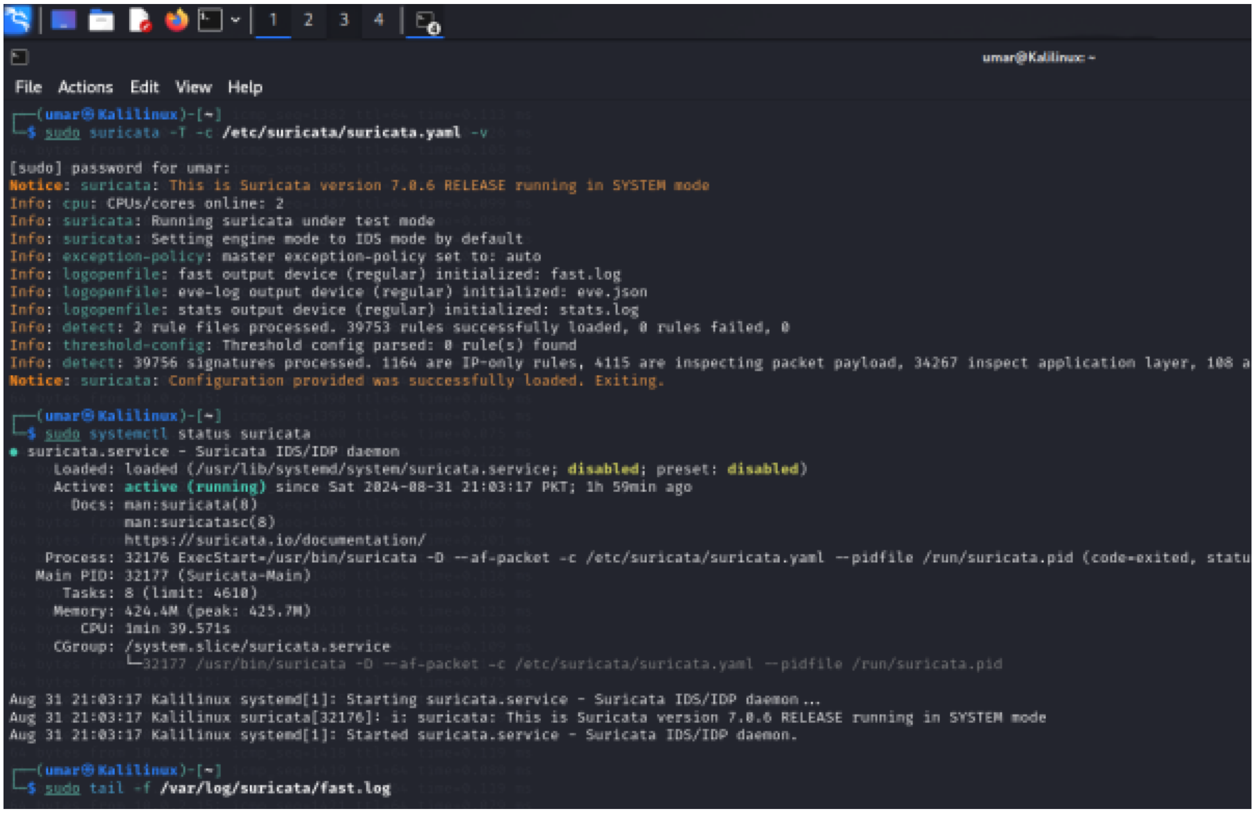
Screenshot of KaliLinux (Snapshot 2)



```
┌──(umar㉿Kalilinux)-[~]
└─$ [[200~sudo suricata -T -c /etc/suricata/suricata.yaml -v~
zsh: bad pattern: ^[[200~sudo

┌──(umar㉿Kalilinux)-[~]
└─$ sudo suricata -T -c /etc/suricata/suricata.yaml -v
[sudo] password for umar:
Notice: suricata: This is Suricata version 7.0.6 RELEASE running in SYSTEM mode
Info: cpu: CPUs/cores online: 2
Info: suricata: Running suricata under test mode
Info: suricata: Setting engine mode to IDS mode by default
Info: exception-policy: master exception-policy set to: auto
Info: logopenfile: fast output device (regular) initialized: fast.log
Info: logopenfile: eve-log output device (regular) initialized: eve.json
Info: logopenfile: stats output device (regular) initialized: stats.log
Info: detect: 2 rule files processed. 39753 rules successfully loaded, 0 rules failed, 0
Info: threshold-config: Threshold config parsed: 0 rule(s) found
Info: detect: 39756 signatures processed. 1364 are IP-only rules, 4115 are inspecting packet payload, 34267 inspect application layer, 108 are decoder event only
Notice: suricata: Configuration provided was successfully loaded. Exiting.

┌──(umar㉿Kalilinux)-[~]
└─$ █
```



```
┌──(umar㉿Kalilinux)-[~]
└─$ sudo suricata -T -c /etc/suricata/suricata.yaml -v

[sudo] password for umar:
Notice: suricata: This is Suricata version 7.0.6 RELEASE running in SYSTEM mode
Info: cpu: CPUs/cores online: 2
Info: suricata: Running suricata under test mode
Info: suricata: Setting engine mode to IDS mode by default
Info: exception-policy: master exception-policy set to: auto
Info: logopenfile: fast output device (regular) initialized: fast.log
Info: logopenfile: eve-log output device (regular) initialized: eve.json
Info: logopenfile: stats output device (regular) initialized: stats.log
Info: detect: 2 rule files processed. 39753 rules successfully loaded, 0 rules failed, 0
Info: threshold-config: Threshold config parsed: 0 rule(s) found
Info: detect: 39756 signatures processed. 1164 are IP-only rules, 4115 are inspecting packet payload, 34267 inspect application layer, 108 a
Notice: suricata: Configuration provided was successfully loaded. Exiting.

┌──(umar㉿Kalilinux)-[~]
└─$ sudo systemctl status suricata
● suricata.service - Suricata IDS/IDP daemon
     Loaded: loaded (/usr/lib/systemd/system/suricata.service; disabled; preset: disabled)
     Active: active (running) since Sat 2024-08-31 21:03:17 PKT; 1h 59min ago
       Docs: man:suricata(8)
             man:suricatasc(8)
             https://suricata.io/documentation/
    Process: 32176 ExecStart=/usr/bin/suricata -D --af-packet -c /etc/suricata/suricata.yaml --pidfile /run/suricata.pid (code=exited, statu
   Main PID: 32177 (Suricata-Main)
      Tasks: 8 (limit: 4610)
     Memory: 424.4M (peak: 425.7M)
        CPU: 1min 39.571s
     CGroup: /system.slice/suricata.service
             └─32177 /usr/bin/suricata -D --af-packet -c /etc/suricata/suricata.yaml --pidfile /run/suricata.pid

Aug 31 21:03:17 Kalilinux systemd[1]: Starting suricata.service - Suricata IDS/IDP daemon...
Aug 31 21:03:17 Kalilinux suricata[32176]: i: suricata: This is Suricata version 7.0.6 RELEASE running in SYSTEM mode
Aug 31 21:03:17 Kalilinux systemd[1]: Started suricata.service - Suricata IDS/IDP daemon.

┌──(umar㉿Kalilinux)-[~]
└─$ sudo tail -f /var/log/suricata/fast.log
```