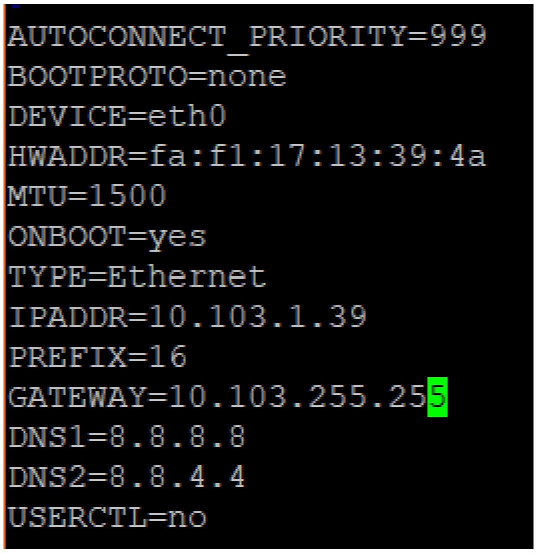
Zadanie 1

Nastavil som si staticku ip adresu v subore /etc/sysconfig/network-scripts/ifcfg-eth0



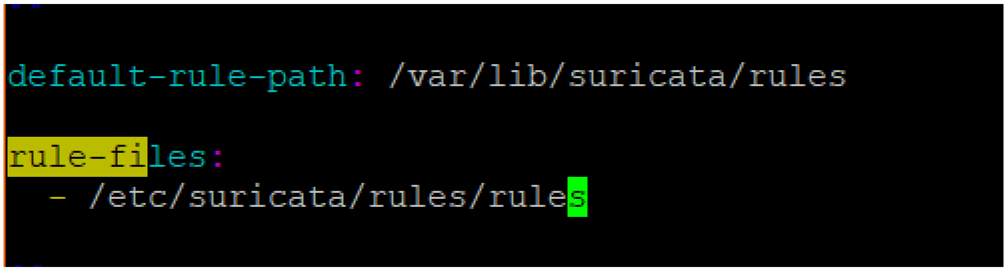
```
AUTOCONNECT_PRIORITY=999
BOOTPROTO=none
DEVICE=eth0
HWADDR=fa:f1:17:13:39:4a
MTU=1500
ONBOOT=yes
TYPE=Ethernet
IPADDR=10.103.1.39
PREFIX=16
GATEWAY=10.103.255.255
DNS1=8.8.8.8
DNS2=8.8.4.4
USERCTL=no
```

Dalej som si stiahol emerging threats cez

wget https://rules.emergingthreats.net/open/suricata-6.0/emerging.rules.tar.gz

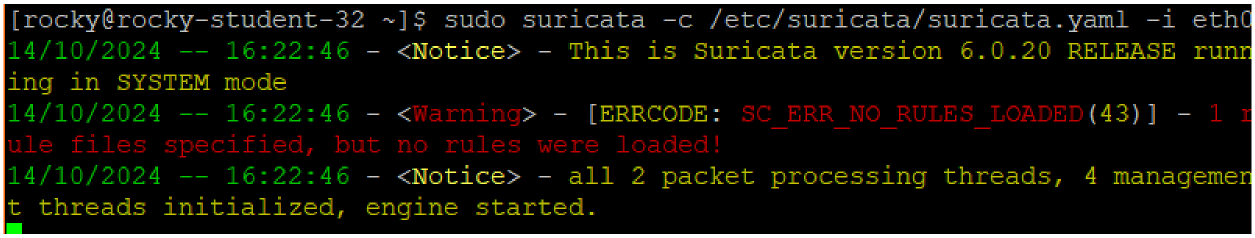
a cez tar rozbalil do /etc/suricata/rules

nasledne som v /etc/suricata/suricata.yaml zmenil rule-files



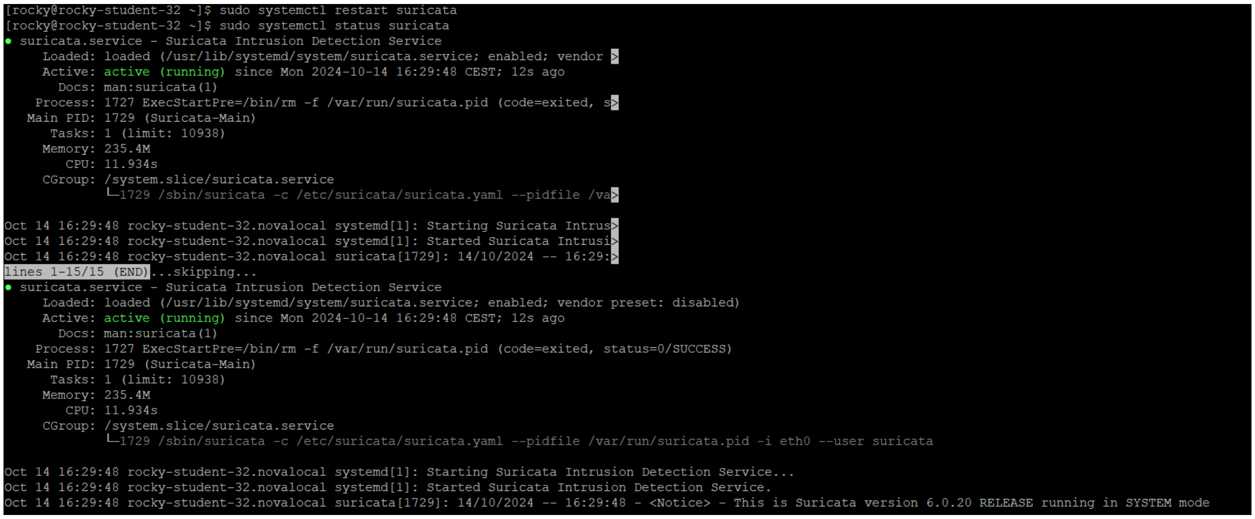
```

default-rule-path: /var/lib/suricata/rules

rule-files:
  - /etc/suricata/rules/rules

```

Manualne skusam spustat:



```
[rocky@rocky-student-32 ~]$ sudo suricata -c /etc/suricata/suricata.yaml -i eth0
14/10/2024 -- 16:22:46 - <Notice> - This is Suricata version 6.0.20 RELEASE runn
ing in SYSTEM mode
14/10/2024 -- 16:22:46 - <Warning> - [ERRCODE: SC_ERR_NO_RULES_LOADED(43)] - 1 r
ule files specified, but no rules were loaded!
14/10/2024 -- 16:22:46 - <Notice> - all 2 packet processing threads, 4 managemen
t threads initialized, engine started.
```

Nepodarilo sa nacitat rules, musel som spravit nejake zmeny v yaml subore suricaty (konkretne includnut vsetky emerging threats rules subory po jednom) ale malo by to teraz ist



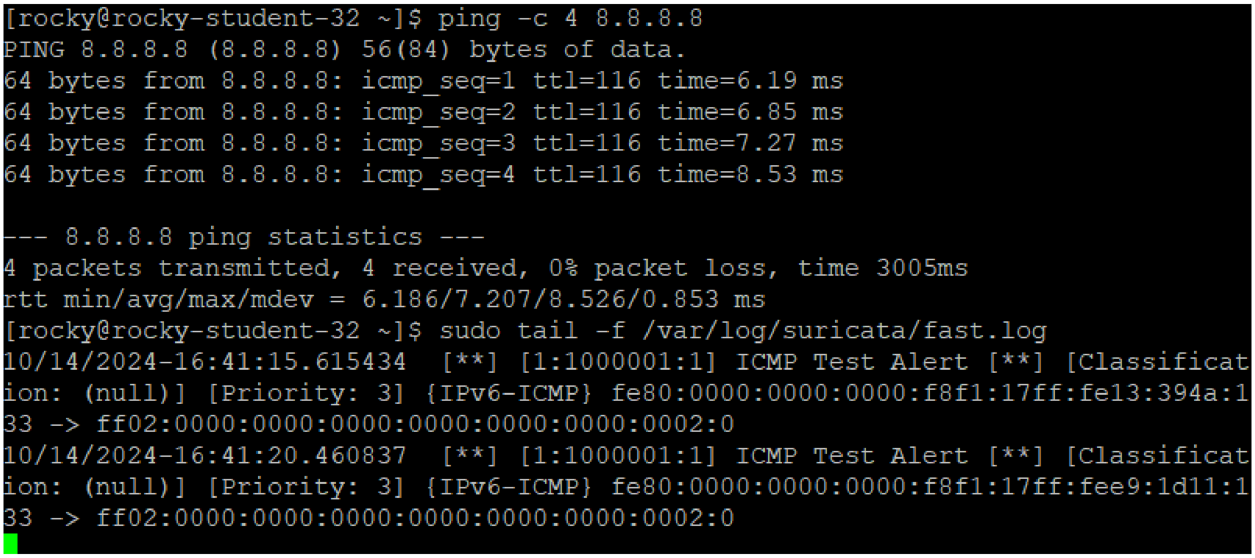
```
[rocky@rocky-student-32 ~]$ sudo systemctl restart suricata
[rocky@rocky-student-32 ~]$ sudo systemctl status suricata
● suricata.service - Suricata Intrusion Detection Service
     Loaded: loaded (/usr/lib/systemd/system/suricata.service; enabled; vendor >
     Active: active (running) since Mon 2024-10-14 16:29:48 CEST; 12s ago
       Docs: man:suricata(1)
    Process: 1727 ExecStartPre=/bin/rm -f /var/run/suricata.pid (code=exited, s>
   Main PID: 1729 (Suricata-Main)
      Tasks: 1 (limit: 10938)
     Memory: 235.4M
        CPU: 11.934s
     CGroup: /system.slice/suricata.service
             └─1729 /sbin/suricata -c /etc/suricata/suricata.yaml --pidfile /va>

Oct 14 16:29:48 rocky-student-32.novalocal systemd[1]: Starting Suricata Intrus>
Oct 14 16:29:48 rocky-student-32.novalocal systemd[1]: Started Suricata Intrusi>
Oct 14 16:29:48 rocky-student-32.novalocal suricata[1729]: 14/10/2024 -- 16:29:>
lines 1-15/15 (END)...skipping...
● suricata.service - Suricata Intrusion Detection Service
     Loaded: loaded (/usr/lib/systemd/system/suricata.service; enabled; vendor preset: disabled)
     Active: active (running) since Mon 2024-10-14 16:29:48 CEST; 12s ago
       Docs: man:suricata(1)
    Process: 1727 ExecStartPre=/bin/rm -f /var/run/suricata.pid (code=exited, status=0/SUCCESS)
   Main PID: 1729 (Suricata-Main)
      Tasks: 1 (limit: 10938)
     Memory: 235.4M
        CPU: 11.934s
     CGroup: /system.slice/suricata.service
             └─1729 /sbin/suricata -c /etc/suricata/suricata.yaml --pidfile /var/run/suricata.pid -i eth0 --user suricata

Oct 14 16:29:48 rocky-student-32.novalocal systemd[1]: Starting Suricata Intrusion Detection Service...
Oct 14 16:29:48 rocky-student-32.novalocal systemd[1]: Started Suricata Intrusion Detection Service.
Oct 14 16:29:48 rocky-student-32.novalocal suricata[1729]: 14/10/2024 -- 16:29:48 - <Notice> - This is Suricata version 6.0.20 RELEASE running in SYSTEM mode
```

Pridal som aj custom rule do /etc/suricata/rules/local.rules:

alert icmp any any -> any any (msg:"ICMP Test Alert"; sid:1000001; rev:1;)

(sid je unique id pravidla a malo by byt zevraj and 1 milion, rev je verzia)

a vyskusal som ho nasledovne:



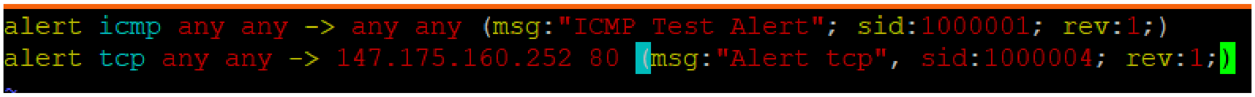
```
[rocky@rocky-student-32 ~]$ ping -c 4 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=116 time=6.19 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=116 time=6.85 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=116 time=7.27 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=116 time=8.53 ms

--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 6.186/7.207/8.526/0.853 ms
[rocky@rocky-student-32 ~]$ sudo tail -f /var/log/suricata/fast.log
10/14/2024-16:41:15.615434  [**] [1:1000001:1] ICMP Test Alert [**] [Classificat
ion: (null)] [Priority: 3] {IPv6-ICMP} fe80:0000:0000:0000:f8f1:17ff:fe13:394a:1
33 -> ff02:0000:0000:0000:0000:0000:0000:0002:0
10/14/2024-16:41:20.460837  [**] [1:1000001:1] ICMP Test Alert [**] [Classificat
ion: (null)] [Priority: 3] {IPv6-ICMP} fe80:0000:0000:0000:f8f1:17ff:fee9:1d11:1
33 -> ff02:0000:0000:0000:0000:0000:0000:0002:0
```

Zadanie 2

Úloha 1

Pridal som pravidlo ale nemam ho ako otestovat kedze nemam kamaratov :(

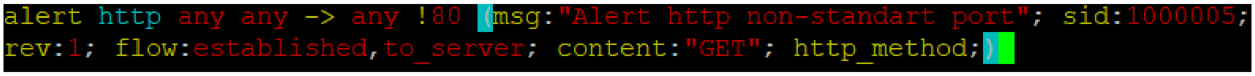
Dal som tam moju ip pocitaca ale to nebude fungovat.



```
alert icmp any any -> any any (msg:"ICMP Test Alert"; sid:1000001; rev:1;)
alert tcp any any -> 147.175.160.252 80 (msg:"Alert tcp", sid:1000004; rev:1;)
~
```

Úloha 2

To iste aj tu



```
alert http any any -> any !80 (msg:"Alert http non-standart port"; sid:1000005;
rev:1; flow:established,to_server; content:"GET"; http_method;)
```

Keby to mám ako otestovať, samozrejme by som si restartol suricatu s novým pravidlom a skusil napr cez curl nejaku komunikaciu na nestandartnom porte.

Monitorovanie odchádzajúcej komunikacie je dolezita napr. Kvoli detekcii kompromizovanych strojov, alebo prevencia datovych unikov.

Úloha 3

Kedze som si minule cvicenie nesetupol shell, taktiez nemam kamaratov tak neviem ako spravit tuto ulohu

Pravidlo by vyzeralo asi nejak takto:

drop tcp any any -> any any (msg:"Dropping shadow"; content:"/etc/shadow"; sid:1000006; rev:1;)