**Zadanie 1**

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

A screenshot of a computer program

Description automatically generated

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

A black background with white text

Description automatically generated

Manualne skusam spustat: A screen shot of a computer

Description automatically generated

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 istA computer screen shot of text

Description automatically generated

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:

A computer screen with white text

Description automatically generated

**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.



Úloha 2

To iste aj tu



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;)