Vilniaus Gedimino technikos universitetas

Elektronikos fakultetas

Kompiuterijos ir ryšių technologijų katedra

Informacijos ir sistemų apsauga

Modulis ELKRM17209

Laboratorinio darbo nr 4. ataskaita

Atliko: TETfm-20 grupės magistrantas
Saulius Krasuckas
Tikrino: doc. dr. Eimantas Garšva

VILNIUS, 2021

Darbo Tikslas

✓ Parengti ir išbandyti *Snort 2.9.18* atakų atpažinimo sistemą.

Trumpas atlikto darbo aptarimas

1. Tinklo paruošimas

Išvalau `iptables` nustatymus:

Išsprendžiu aprašo netikslumą.

Tikrinu tinklo nustatymus:

Tinklo nustatymai tvarkingi.

2. Snort instaliavimas

Pereinu į išeities tekstų direktoriją:

Išsprendžiu dar vieną netikslumą.

Parsisiunčiu Snort:

Išarchyvuoju:

Pereinu į išarchyvuotą direktoriją:

Peržiūriu instaliavimo rekomendacijas:

Išsprendžiu ir apeinu daug kompilatoriaus konfigūravimo kliūčių.

Konfigūruoju kompiliatorių:

Sukompiliuoju Snort:

Ir suinstaliuoju:

3. Konfigūracijos ir žurnalo direktorijos

Sukuriu direktorijas:

Pridedu grupę ir vartotoją:

Pakeičiu logų direktorijos teises:

Nukopijuoju standartinius konfigūracinius failus:

4. Pradinis stebėjimas

Stebiu tinklo srautą, įrašau duomenis į failus:

Išsprendžiu nesklandumą su nesusistabdančiu Snort ir netinkamu tinklo sąsajos vardu.

Analizuoju stebėjimo failus:

```
root@ldvm1:~# file snort1
snort1: ASCII text
root@ldvm1:~# cat snort1 | wc -l
138
root@ldvm1:~# less snort1
root@ldvm1:~# cat snort1 | grep -c -- '->'
23
root@ldvm1:~# cat snort1 | grep -- '->'
07/07-07:52:46.822122 192.168.10.14:22 -> 192.168.10.254:40548
07/07-07:52:46.822276 192.168.10.14:22 -> 192.168.10.254:40548
07/07-07:52:46.822451 192.168.10.254:40548 -> 192.168.10.14:22
07/07-07:52:46.822453 192.168.10.254:40548 -> 192.168.10.14:22
07/07-07:52:46.822564 192.168.10.14:22 -> 192.168.10.254:40548
07/07-07:52:46.822686 192.168.10.254:40548 -> 192.168.10.14:22
07/07-07:52:46.822836 192.168.10.14:22 -> 192.168.10.254:40548
07/07-07:52:46.823256 192.168.10.254:40548 -> 192.168.10.14:22
07/07-07:52:47.802795 192.168.10.14:22 -> 192.168.10.254:40548
07/07-07:52:47.803265 192.168.10.254:40548 -> 192.168.10.14:22
07/07-07:52:47.803299 192.168.10.14:22 -> 192.168.10.254:40548
07/07-07:52:47.803619 192.168.10.254:40548 -> 192.168.10.14:22
07/07-07:52:48.826301 192.168.10.14:22 -> 192.168.10.254:40548
07/07-07:52:48.826924 192.168.10.254:40548 -> 192.168.10.14:22
07/07-07:52:49.850174 192.168.10.14:22 -> 192.168.10.254:40548
07/07-07:52:49.850708 192.168.10.254:40548 -> 192.168.10.14:22
07/07-07:52:50.874372 192.168.10.14:22 -> 192.168.10.254:40548
07/07-07:52:50.875024 192.168.10.254:40548 -> 192.168.10.14:22
07/07-07:52:51.899320 192.168.10.14:22 -> 192.168.10.254:40548
07/07-07:52:51.899778 192.168.10.254:40548 -> 192.168.10.14:22
07/07-07:52:52.922172 192.168.10.14:22 -> 192.168.10.254:40548
07/07-07:52:52.922589 192.168.10.254:40548 -> 192.168.10.14:22
07/07-07:52:53.946166 192.168.10.14:22 -> 192.168.10.254:40548
```

- tai tekstinis failas iš 138 eilučių;
- jame aptinku 23 paketus;
- pagal 22/TCP prievadą panašu, kad registruotas tik mano paties SSH srautas;
- atskiras TCP paketas aprašomas tokiu pavidalu:

```
07/07-07:52:46.822453 192.168.10.254:40548 -> 192.168.10.14:22
TCP TTL:64 TOS:0x10 ID:26573 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xCF9BC6E6  Ack: 0x95B0E326  Win: 0x590  TcpLen: 32
TCP Options (3) => NOP NOP TS: 61716058 1184245986
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

5. Paketų rinkimo režimas

Startuoju paketų rinkimo režimu:

Siunčiu užklausas iš fizinio kompiuterio:

Sustabdau paketų rinkimą:

Nuskaitau informaciją apie sustebėtus ICMP paketus: Išsiųstos buvo dvi ICMP užklausos, iš viso surinkti keturi ICMP paketai.

6. Snort konfigūravimas

Susipažįstu su konfigūracijos failo struktūra:

Atkreipiu dėmesį:

- į globalius kintamuosius:
- į naudojamus preprocesorius:
- į išvedimo įskiepius:
- ir į naudojamas taisykles:

Redaguoju failą ir jame įrašau parametrus:

```
[1]+  Stopped                 nano /etc/snort/snort.conf
root@ldvm1:~# cat /etc/snort/snort.conf | awk '/var (RULE_PATH|HOME_NET|EXTERNAL_NET)/'
ipvar HOME_NET 192.168.10.0/24
ipvar EXTERNAL_NET !$HOME_INET
var RULE_PATH /etc/snort/rules
root@ldvm1:~#
```

Naudoju simbolį `#` ir užkomentuoju visas taisykles, išskyrus `local.rules`:

```
root@ldvm1:~# cat /etc/snort/snort.conf | grep '^include .RULE'
include $RULE_PATH/local.rules

root@ldvm1:~# cat /etc/snort/snort.conf | grep -c '^#include .RULE'
104
```

- Iš viso užkomentavau 104 taisykles – daug.

Tikrinu, ar užkomentuotas išvedimas į DB:

```
root@ldvm1:~# cat /etc/snort/snort.conf | grep -n database

root@ldvm1:~# cat /etc/snort/snort.conf | grep -n output
34:#  6) Configure output plugins
515:# Step #6: Configure output plugins
521:# output unified2: filename merged.log, limit 128, nostamp, mpls_event_types,
vlan_event_types
524:# output alert_unified2: filename snort.alert, limit 128, nostamp
525:# output log_unified2: filename snort.log, limit 128, nostamp
528:# output alert_syslog: LOG_AUTH LOG_ALERT
531:# output log_tcpdump: tcpdump.log

root@ldvm1:~# cat /etc/snort/snort.conf | grep -n -w -e log -e mysql
184:# Configure default log directory for snort to log to.  For more information see
snort -h command line options (-l)
201:config event_queue: max_queue 8 log 5 order_events content_length
218:#   pkt-log
225:#   rule-log alert
521:# output unified2: filename merged.log, limit 128, nostamp, mpls_event_types,
vlan_event_types
525:# output log_unified2: filename snort.log, limit 128, nostamp
531:# output log_tcpdump: tcpdump.log
591:#include $RULE_PATH/mysql.rules
628:#include $RULE_PATH/server-mysql.rules
```

- Tokios eilutės net nerandu. Laikau, kad užkomentuota.

7. Taisyklių vieta

Sukuriu direktoriją `/etc/snort/rules`.

Redaguoju failą `local.rules`:

Parašau paprastą taisyklę, kuri praneša apie ICMP paketus, ir failą išsaugau:

```
root@ldvm1:~# cat /etc/snort/rules/local.rules
alert icmp any any -> 192.168.10.14 any (msg: "ICMP test"; sid:10000001;)
root@ldvm1:~#
```

8. ICMP užklausų atpažinimas

Startuoju Snort paslaugą:

Tam išpsrendžiu labai daug kliūčių (žr. Sunkumų skyrelį žemiau).

Išsiunčiu *ping* užklausas iš kaimyno kompiuterio:

```
osboxes@ldvm2:~$ ping -c 2 192.168.10.14
PING 192.168.10.14 (192.168.10.14) 56(84) bytes of data.
64 bytes from 192.168.10.14: icmp_seq=1 ttl=64 time=1.02 ms
64 bytes from 192.168.10.14: icmp_seq=2 ttl=64 time=0.677 ms

--- 192.168.10.14 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1003ms
rtt min/avg/max/mdev = 0.677/0.846/1.016/0.169 ms
```

Stebiu, ar jos buvo atpažintos.

```
osboxes@ldvm1:~$ cat /var/log/snort/alert
[**] [1:10000001:0] ICMP test [**]
[Priority: 0]
07/07-10:00:37.250810 192.168.10.13 -> 192.168.10.14
ICMP TTL:64 TOS:0x0 ID:12730 IpLen:20 DgmLen:84 DF
Type:8  Code:0  ID:1   Seq:1  ECHO

[**] [1:10000001:0] ICMP test [**]
[Priority: 0]
07/07-10:00:38.251703 192.168.10.13 -> 192.168.10.14
ICMP TTL:64 TOS:0x0 ID:12920 IpLen:20 DgmLen:84 DF
Type:8  Code:0  ID:1   Seq:2  ECHO

osboxes@ldvm1:~$ logout
```

Abi išsiųstos ICMP užklausos aptiktos ir atpažintos.

9. *Telnet* paruošimas

Instaliuoju *telnet* serverį:

Redaguoju `local.rules` ir pridedu naują taisyklę:

```
root@ldvm1:~# cat /etc/snort/rules/local.rules
alert icmp any any -> 192.168.10.14 any (msg: "ICMP test"; sid:10000001;)
alert tcp any any -> 192.168.10.14 23 (content: "root"; nocase; msg: "Suspicious
Telnet"; sid: 10000002;)
```

10. *Telnet* tikrinimas

Jungiuosi prie kaimyno kompiuterio per *telnet*:

```
osboxes@ldvm1:~$ telnet kaimynas
Trying 192.168.10.13...
telnet: Unable to connect to remote host: Connection refused
```

- Akivaizdu, kad prisijungti nepavyko: *telnet* paslauga instaliuota ne į jį.

- Jungiuosi priešingai – **iš** kaimyno į savo virtualų kompiuterį:

Visą dieną bandau išspręsti didžiulę kliūtį aptinkant *Telnet* užklausą.

- Pagaliau *telnet* srauto stebėjimas veikia!

```
osboxes@ldvm1:/usr/local/src$ tail -1f /var/log/snort/alert

[**] [1:10000002:0] Suspicious Telnet [**]
[Priority: 0]
07/07-18:53:37.013296 192.168.10.13:38560 -> 192.168.10.14:23
TCP TTL:64 TOS:0x10 ID:56855 IpLen:20 DgmLen:105 DF
***AP*** Seq: 0xFB94525  Ack: 0x47141D77  Win: 0x1F6  TcpLen: 32
TCP Options (3) => NOP NOP TS: 141966812 1508637531
```

Analizuoju atsiradusį įrašą. Jame rodoma:

1. taisyklės identifikatorius `"sid"` (*Snort rule ID*),
2. taisyklės pavadinimas (`"Suspicious Telnet"`),
3. taisyklės prioritetas (`0`),
4. užklausos gavimo data,
5. abu IP adresai,
6. abu TCP portai
7. ir didelė dalis likusios TCP (Layer 4) antraštės.
   - Tačiau tekstą `"root"` renkant ranka, po simbolį, Snort užklausos vis tiek neaptinka. Galimai reikia perkonfigūruoti preprocesorių `ftp_telnet` arba `ftp_telnet_protocol`, kad duomenys būtų imami iš jo tiesiogiai.
     Ar galbūt tiesiog panaudoti kitą sintaksę, skirtą priėjimui prie šio preprocesoriaus apdorotų duomenų tiesiogiai.

Šiam žingsniui išspręsti skyriau beveik 8 val.:

```
11:37:15
19:25:09
```

- Dėl to baigiu šio žingsnio aiškinimąsi ir palieku tai netikslaus 4LD aprašo sąžinei.

Galiausiai lieka neaišku:

- ar taip ir turėjo būti,
- ar `ftp_telnet*` preprocesorius veikia klaidingai,

- ar jam visgi trūko sukonfigūravimo.

11. Bendruomenės taisyklės

Parsisiunčiu bendruomenės taisykles:

Išarchyvuoju taisykles:

Randu dar vieną LD aprašo neatitikimą.

- Peržiūriu taisyklių direktorijos medį:

```
osboxes@ldvm1:/etc/snort$ tree rules
rules
├── community-rules
│   ├── AUTHORS
│   ├── community.rules
│   ├── LICENSE
│   ├── sid-msg.map
│   ├── snort.conf
│   └── VRT-License.txt
├── local.rules
└── local.rules.BACKUP

osboxes@ldvm1:/etc/snort$ ls -lt rules/community-rules
total 2292
-rw-r--r-- 1 1210 root  484378 Jul  7 18:54 sid-msg.map
-rw-r--r-- 1 1210 root 1777148 Jul  7 18:54 community.rules
-rw-r--r-- 1 1210 root   29817 Mar 10 21:04 snort.conf
-rw-r--r-- 1 1210 root   21084 Feb 25 15:49 VRT-License.txt
-rw-r--r-- 1 1210 root    7834 Nov  9  2018 AUTHORS
-rw-r--r-- 1 1210 root   15127 Mar 20  2013 LICENSE
```

Peržiūriu taisyklių failo struktūrą:

```
osboxes@ldvm1:/etc/snort$ ll -h rules/community-rules/community.rules
-rw-r--r-- 1 1210 root 1.7M Jul  7 18:54 rules/community-rules/community.rules

osboxes@ldvm1:/etc/snort$ cat rules/community-rules/community.rules | wc -l
3986
osboxes@ldvm1:/etc/snort$ less -S rules/community-rules/community.rules
```

- Beveik 4000 eilučių. Peržiūriu paskutines:

```
osboxes@ldvm1:/etc/snort$ cat rules/community-rules/community.rules | tail -2
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"INDICATOR-COMPROMISE
Revil Kaseya ransomware log clearing http upload"; flow:to_server,established;
file_data; content:"Server.CreateObject"; content:"KComWExec.execCmd";
fast_pattern:only; metadata:impact_flag red, policy balanced-ips drop, policy
connectivity-ips drop, policy max-detect-ips drop, policy security-ips drop, ruleset
community, service http; reference:url,doublepulsar.com/kaseya-supply-chain-attack-
delivers-mass-ransomware-event-to-us-companies-76e4ec6ec64b;
reference:url,www.huntress.com/blog/rapid-response-kaseya-vsa-mass-msp-ransomware-
incident; classtype:web-application-attack; sid:57879; rev:2;)
```

- Kiekviena taisyklė gana ilga, todėl kerpu ties 80 simb.:

```
osboxes@ldvm1:/etc/snort$ cat rules/community-rules/community.rules | tail | cut -c
1-80
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"MALWARE-BACKDOOR Perl
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"MALWARE-BACKDOOR Perl
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"MALWARE-BACKDOOR Perl
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"MALWARE-BACKDOOR Perl
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"MALWARE-BACKDOOR Perl
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"MALWARE-BACKDOOR Perl
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"OS-WINDOWS Microsoft
# alert tcp any any -> $HOME_NET $HTTP_PORTS (msg:"POLICY-OTHER Active Directory
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"INDICATOR-COMPROMISE
```

- Dalis eilučių užkomentuotos.
- Skaičiuoju tik atkomentuotąsias:

```
osboxes@ldvm1:/etc/snort$ cat rules/community-rules/community.rules | grep -vc ^#
508
```

- Pežiūriu 10 pirmų:

```
osboxes@ldvm1:/etc/snort$ cat rules/community-rules/community.rules | grep -v ^#|
head | cut -c 1-80

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"FILE-IDENTIFY RealNet
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"FILE-IDENTIFY RealNet
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"FILE-IDENTIFY RealNet
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"FILE-IDENTIFY RealNet
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"FILE-IDENTIFY Microso
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"FILE-IDENTIFY Microso
alert tcp $HOME_NET 5880 -> $EXTERNAL_NET any (msg:"MALWARE-BACKDOOR Y3KRAT 1.5
alert tcp $EXTERNAL_NET any -> $HOME_NET 5880 (msg:"MALWARE-BACKDOOR Y3KRAT 1.5
alert tcp $EXTERNAL_NET any -> $HOME_NET 139 (msg:"NETBIOS SMB Trans2 QUERY_FILE
```

- Peržiūriu 10 paskutinių:

```
osboxes@ldvm1:/etc/snort$ cat rules/community-rules/community.rules | grep -v ^#|
tail | cut -c 1-80
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"MALWARE-BACKDOOR Perl
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"MALWARE-BACKDOOR Perl
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"MALWARE-BACKDOOR Perl
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"MALWARE-BACKDOOR Perl
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"MALWARE-BACKDOOR Perl
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"MALWARE-BACKDOOR Perl
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"MALWARE-BACKDOOR Perl
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"OS-WINDOWS Microsoft
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"INDICATOR-COMPROMISE
```

- Peržiūriu pilną pirmąją:

```
osboxes@ldvm1:/etc/snort$ cat rules/community-rules/community.rules | grep -v ^#|
head -2

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"FILE-IDENTIFY
RealNetworks Realplayer .ram playlist file download request";
flow:to_server,established; content:".ra"; fast_pattern:only; http_uri;
pcre:"/\x2eram?([\?\x5c\x2f]|$)/smiU"; flowbits:set,file.realplayer.playlist;
flowbits:noalert; metadata:policy max-detect-ips alert, ruleset community, service
http; reference:url,en.wikipedia.org/wiki/.ram; classtype:misc-activity; sid:2419;
rev:30;)
```

- Direktorijoje randu dar pora failų:

```
osboxes@ldvm1:/etc/snort$ ll rules/community-rules/*.{map,conf}
-rw-r--r-- 1 1210 root 484378 Jul  7 18:54 rules/community-rules/sid-msg.map
-rw-r--r-- 1 1210 root  29817 Mar 10 21:04 rules/community-rules/snort.conf

osboxes@ldvm1:/etc/snort$ file rules/community-rules/*.{map,conf}
rules/community-rules/sid-msg.map: ASCII text, with very long lines
rules/community-rules/snort.conf:  ASCII text, with very long lines
```

- `sig-msg.map` matau sąrašą su `sid` ir `msg` reikšmų poromis iš `*.rules` failo.
- `snort.conf` antraštė teigia, kad šis konfigūracinis failas tinka Sourcefire VRT (https://blog.snort.org/2014/06/sourcefire-vrt-certified-snort-rules.html) (Vulnerability Response Team) taisyklių paketui. Kas tai tokio, nežinau.
  Dar failas sako įgalinąs atsaką (angl. *Active response*, turbūt IPS veikimą).
  Taip pat detalizuoja 9 žingsnius, kuriuos reikėtų įvykdyti pritaikant konfigūraciją sau.
  Panašu, kad tai tiesiog Snort 2.9.9.0 konfigūracijos failas pagal nutylėjimą.

12. Skenavimas įgalinus bendruomenės taisykles

Visų pirma įtraukiu taisykles į konfiguraciją (apraše neradau tokio žingsnio).

Vietoj 2 taisyklių dabar turime 508.

Vykdau skenavimą iš kaimyno kompiuterio:

```
osboxes@ldvm2:~$ sudo nmap -sS -P0 -n -F 192.168.10.14
Starting Nmap 7.80 ( https://nmap.org ) at 2021-07-08 01:36 EEST
Nmap scan report for 192.168.10.14
Host is up (0.0014s latency).
Not shown: 96 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
23/tcp  open  telnet
80/tcp  open  http
443/tcp open  https
MAC Address: 08:00:27:40:2C:F6 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.07 seconds
```

Sprendžiu neaiškumą, kad Snort neaptinka skenavimo.

Pagaliau Snort `alert` logas pasipildė:

```
osboxes@ldvm1:/etc/snort$ tail -1f /var/log/snort/alert
Time: 07/08-09:23:13.918388
event_ref: 0
192.168.10.13 -> 192.168.10.14 (portscan) TCP Portscan
Priority Count: 8
Connection Count: 10
IP Count: 1
Scanner IP Range: 192.168.10.13:192.168.10.13
Port/Proto Count: 10
Port/Proto Range: 25:8888
```

Įrašas atsirado tik vienas. Jame matyti:

- kad vykdomas TCP prievadų skenavimas;
- kad skenuotojas tik vienas;
- kad atlikti 10 TCP prisijungimų (tikėtina, jog skenuota 10 portų, bet nebūtinai) – bendru atveju galimas ir vieno TCP porto skenavimas su keliais prisijungimais);
- skenuotų TCP prievadų yra 10;
- skenuotų TCP prievadų intervalas yra 25 – 8888.

13. MySQL konfigūravimas

Konfigūruoju MySQL vartotoją:

Sukuriu duomenų bazę:

Sprendžiu sunkumą su neveikiančia mysql komanda.

Įeinu į MyQSL komandinį režimą:

Jame sukuriu duomenų bazę:

Kuriu vartotoją su teisėmis:

Nustatau slaptažodį duomenų bazei:

Sprendžiu sunkumą su neveikiančia mysql komanda.

Išeinu iš MySQL komandinio režimo:

14. Snort DB importavimas

Importuoju Snort duomenų bazės schemą:

Vėl klaida. Atlieku analizę. Išsprendimui reikia daug daugiau laiko.

- Turiu vienintelį spėjimą pagal `"src/dynamic-preprocessors/appid/service_plugins/service_mysql.c"` failą: galbūt MySQL palaikymui reikalingas įjungtas OpenAppID palaikymas. O pastarąjį esu išjungęs kompiliatoriaus konfigūravimo fazėje.

Stabdau laboratorinio darbo atlikimą, nes per daug neatitikimų.

Iškilę sunkumai ir pastebėti netikslumai

1. Tinklo paruošimas

```
osboxes@ldvm1:~$ sudo iptables -F
osboxes@ldvm1:~$
```

- Iškart iškilo sunkumas – užstrigo SSH ryšys ir po ilgo laiko SSH klientas atsijungė:

  ```
  osboxes@ldvm1:~$
  osboxes@ldvm1:~$ packet_write_wait: Connection to 192.168.10.14 port 22: Broken pipe
  ```

- Priežasčių supratimui prisijungiau per Serial konsolę ir pasinaudojau `tcpdump` programa:

```
osboxes@ldvm1:~$ sudo tcpdump -ni any
sudo tcpdump -ni any
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked v1), capture size 262144 bytes
22:35:57.299726 IP 192.168.10.14.22 > 192.168.10.254.40526: Flags [P.], seq
4070427175:4070427275, ack 809347258, win 501, options [nop,nop,TS val 1151414038
ecr 28314383], length 100
22:35:57.299901 IP 192.168.10.254.40526 > 192.168.10.14.22: Flags [.], ack 100, win
466, options [nop,nop,TS val 28315249 ecr 1151414038,nop,nop,sack 1 {0:100}], length
0
22:35:58.131852 IP 192.168.10.14.22 > 192.168.10.254.40526: Flags [P.], seq 0:100,
ack 1, win 501, options [nop,nop,TS val 1151414870 ecr 28314383], length 100
22:35:58.134467 IP 192.168.10.254.40526 > 192.168.10.14.22: Flags [.], ack 100, win
466, options [nop,nop,TS val 28316095 ecr 1151414870,nop,nop,sack 1 {0:100}], length
0
22:35:59.795988 IP 192.168.10.14.22 > 192.168.10.254.40526: Flags [P.], seq 0:100,
ack 1, win 501, options [nop,nop,TS val 1151416534 ecr 28314383], length 100
22:35:59.798233 IP 192.168.10.254.40526 > 192.168.10.14.22: Flags [.], ack 100, win
466, options [nop,nop,TS val 28317788 ecr 1151416534,nop,nop,sack 1 {0:100}], length
0
22:36:03.091852 IP 192.168.10.14.22 > 192.168.10.254.40526: Flags [P.], seq 0:100,
ack 1, win 501, options [nop,nop,TS val 1151419830 ecr 28314383], length 100
22:36:03.093223 IP 192.168.10.254.40526 > 192.168.10.14.22: Flags [.], ack 100, win
466, options [nop,nop,TS val 28321139 ecr 1151419830,nop,nop,sack 1 {0:100}], length
0
22:36:09.747774 IP 192.168.10.14.22 > 192.168.10.254.40526: Flags [P.], seq 0:100,
ack 1, win 501, options [nop,nop,TS val 1151426486 ecr 28314383], length 100
22:36:09.748032 IP 192.168.10.254.40526 > 192.168.10.14.22: Flags [.], ack 100, win
466, options [nop,nop,TS val 28327908 ecr 1151426486,nop,nop,sack 1 {0:100}], length
0
22:36:23.059826 IP 192.168.10.14.22 > 192.168.10.254.40526: Flags [P.], seq 0:100,
ack 1, win 501, options [nop,nop,TS val 1151439798 ecr 28314383], length 100
22:36:23.060319 IP 192.168.10.254.40526 > 192.168.10.14.22: Flags [.], ack 100, win
466, options [nop,nop,TS val 28341446 ecr 1151439798,nop,nop,sack 1 {0:100}], length
0
22:36:49.695812 IP 192.168.10.14.22 > 192.168.10.254.40526: Flags [P.], seq 0:100,
ack 1, win 501, options [nop,nop,TS val 1151466434 ecr 28314383], length 100
22:36:49.696170 IP 192.168.10.254.40526 > 192.168.10.14.22: Flags [.], ack 100, win
466, options [nop,nop,TS val 28368534 ecr 1151466434,nop,nop,sack 1 {0:100}], length
0
22:36:54.614139 ARP, Request who-has 192.168.10.14 tell 192.168.10.254, length 46
22:36:54.614163 ARP, Reply 192.168.10.14 is-at 08:00:27:40:2c:f6, length 28
22:36:54.803813 ARP, Request who-has 192.168.10.254 tell 192.168.10.14, length 28
22:36:54.804052 ARP, Reply 192.168.10.254 is-at 0a:00:27:00:00:00, length 46
22:37:42.948130 IP 192.168.10.14.22 > 192.168.10.254.40526: Flags [P.], seq 0:100,
ack 1, win 501, options [nop,nop,TS val 1151519686 ecr 28314383], length 100
22:37:42.948395 IP 192.168.10.254.40526 > 192.168.10.14.22: Flags [.], ack 100, win
466, options [nop,nop,TS val 28422690 ecr 1151519686,nop,nop,sack 1 {0:100}], length
0
22:37:47.870393 ARP, Request who-has 192.168.10.14 tell 192.168.10.254, length 46
22:37:47.870439 ARP, Reply 192.168.10.14 is-at 08:00:27:40:2c:f6, length 28
22:37:48.051718 ARP, Request who-has 192.168.10.254 tell 192.168.10.14, length 28
22:37:48.052034 ARP, Reply 192.168.10.254 is-at 0a:00:27:00:00:00, length 46
```

- Matyti, kad:

    - virtualus kompiuteris fiziniam kompiuteriui siunčia duomenų bloką per TCP;
    - fizinis kompiuteris per TCP siunčia patvirtinimus, kad duomenis gavo;
    - ir veiksmai kartojasi su vis ilgėjančiu intervalu tarp pasikartojimų.
- Peržiūrėjus `iptables` matyti, kad tai įvyksta dėl grandyje `INPUT` pasilikusio `POLICY = DROP` nustatymo:

```
osboxes@ldvm1:~$ sudo iptables --list -n
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  0.0.0.0/0            192.168.10.14        tcp dpt:22
ACCEPT     tcp  --  0.0.0.0/0            192.168.10.14        tcp dpt:443

Chain FORWARD (policy DROP)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

- Tad jei tarpsegmentinį filtrą nustatome scenarijaus pagalba, jį išvalyti reikėtų taip pat:

```
osboxes@ldvm1:~$ sudo /etc/init.d/myfirewall stop
sudo /etc/init.d/myfirewall stop
Stopping firewall (flushing rules)
```

- Tikrinu ryšį:

```
[p@localhost ~]$ ssh osboxes@192.168.10.14
osboxes@192.168.10.14's password:
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.8.0-59-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

154 updates can be installed immediately.
0 of these updates are security updates.
To see these additional updates run: apt list --upgradable

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your
Internet connection or proxy settings

Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Tue Jul  6 22:34:55 2021 from 192.168.10.254
osboxes@ldvm1:~$
```

- Ryšys atsistatė.
- 4LD aprašas šiam žingsniui nevisai korektiškas.

2. Snort instaliavimas

```
osboxes@ldvm1:~$ cd /usr/local/src/
osboxes@ldvm1:/usr/local/src$
```

- Siunčiu Snort ir iškart antra kliūtis:

  ```
  osboxes@ldvm1:/usr/local/src$ wget https://www.snort.org/downloads/snort/snort-
  2.9.18.tar.gz
  --2021-07-06 23:11:27--  https://www.snort.org/downloads/snort/snort-2.9.18.tar.gz
  Resolving www.snort.org (www.snort.org)... 104.18.139.9, 104.18.138.9,
  2606:4700::6812:8b09, ...
  Connecting to www.snort.org (www.snort.org)|104.18.139.9|:443... connected.
  HTTP request sent, awaiting response... 302 Found
  Location: https://snort-org-
  site.s3.amazonaws.com/production/release_files/files/000/018/474/original/snort-
  2.9.18.tar.gz?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-
  Credential=AKIAIXACIED2SPMSC7GA%2F20210706%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-
  Date=20210706T201127Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-
  Signature=56f418bb145628cfcf085140ffdcd693b1dbf5deb116d8fac3117c594e7c1a8f
  [following]
  --2021-07-06 23:11:28--  https://snort-org-
  site.s3.amazonaws.com/production/release_files/files/000/018/474/original/snort-
  2.9.18.tar.gz?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-
  Credential=AKIAIXACIED2SPMSC7GA%2F20210706%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-
  Date=20210706T201127Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-
  Signature=56f418bb145628cfcf085140ffdcd693b1dbf5deb116d8fac3117c594e7c1a8f
  Resolving snort-org-site.s3.amazonaws.com (snort-org-site.s3.amazonaws.com)...
  52.217.137.153
  Connecting to snort-org-site.s3.amazonaws.com (snort-org-
  site.s3.amazonaws.com)|52.217.137.153|:443... connected.
  HTTP request sent, awaiting response... 200 OK
  Length: 6909928 (6.6M) [binary/octet-stream]
  snort-2.9.18.tar.gz: Permission denied

  Cannot write to ‘snort-2.9.18.tar.gz’ (Success).`
  ```

- Tikrinu teises:

  ```
  osboxes@ldvm1:/usr/local/src$ ll -d .
  drwxr-xr-x 2 root root 4096 Feb  9 20:47 ./

  osboxes@ldvm1:/usr/local/src$ id
  uid=1000(osboxes) gid=1000(osboxes)
  groups=1000(osboxes),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),120(lpadmin),131(
  lxd),132(sambashare)
  ```

- Ir jas pakeičiu:

```
osboxes@ldvm1:/usr/local/src$ sudo chown osboxes:osboxes .

osboxes@ldvm1:/usr/local/src$ ll -d .
drwxr-xr-x 2 osboxes osboxes 4096 Feb  9 20:47 ./
```

- Konfigūruoju kompiliatorių, iškyla sunkumas:

```
osboxes@ldvm1:/usr/local/src/snort-2.9.18$ ./configure --with-mysql --enable-dynamicplugin
configure: WARNING: unrecognized options: --with-mysql, --enable-dynamicplugin
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for a thread-safe mkdir -p... /usr/bin/mkdir -p
checking for gawk... no
checking for mawk... mawk
  ...
checking for pfring_open in -lpfring... no
checking for pfring_open in -lpcap... no

   ERROR!  Libpcap library/headers (libpcap.a (or .so)/pcap.h)
   not found, go get it from http://www.tcpdump.org
   or use the --with-libpcap-* options, if you have it installed
   in unusual place.  Also check if your libpcap depends on another
   shared library that may be installed in an unusual place
```

- Įdiegiu 2LD metu praleistus ir dabar trūkstančius paketus:

```
osboxes@ldvm1:/usr/local/src/snort-2.9.18$ sudo apt-get install libnet1 libnet1-dev
libpcre3 libpcre3-dev libpcap0.8 libpcap0.8-dev
Reading package lists... Done
Building dependency tree
Reading state information... Done
libpcap0.8 is already the newest version (1.9.1-3).
libpcap0.8 set to manually installed.
libpcre3 is already the newest version (2:8.39-12build1).
libpcre3 set to manually installed.
The following additional packages will be installed:
  libpcre16-3 libpcre32-3 libpcrecpp0v5
The following NEW packages will be installed:
  libnet1 libnet1-dev libpcap0.8-dev libpcre16-3 libpcre3-dev libpcre32-3
libpcrecpp0v5
0 upgraded, 7 newly installed, 0 to remove and 153 not upgraded.
Need to get 1,234 kB of archives.
After this operation, 5,059 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://us.archive.ubuntu.com/ubuntu focal/main amd64 libnet1 amd64 1.1.6+dfsg-
3.1build1 [43.3 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu focal/main amd64 libnet1-dev amd64
1.1.6+dfsg-3.1build1 [101 kB]
Get:3 http://us.archive.ubuntu.com/ubuntu focal/main amd64 libpcap0.8-dev amd64
1.9.1-3 [244 kB]
Get:4 http://us.archive.ubuntu.com/ubuntu focal/main amd64 libpcre16-3 amd64 2:8.39-
12build1 [150 kB]
Get:5 http://us.archive.ubuntu.com/ubuntu focal/main amd64 libpcre32-3 amd64 2:8.39-
12build1 [140 kB]
Get:6 http://us.archive.ubuntu.com/ubuntu focal/main amd64 libpcrecpp0v5 amd64
2:8.39-12build1 [15.5 kB]
Get:7 http://us.archive.ubuntu.com/ubuntu focal/main amd64 libpcre3-dev amd64
2:8.39-12build1 [540 kB]
Fetched 1,234 kB in 4s (345 kB/s)
Selecting previously unselected package libnet1:amd64.
(Reading database ... 197632 files and directories currently installed.)
Preparing to unpack .../0-libnet1_1.1.6+dfsg-3.1build1_amd64.deb ...
Unpacking libnet1:amd64 (1.1.6+dfsg-3.1build1) ...
Selecting previously unselected package libnet1-dev.
Preparing to unpack .../1-libnet1-dev_1.1.6+dfsg-3.1build1_amd64.deb ...
Unpacking libnet1-dev (1.1.6+dfsg-3.1build1) ...
Selecting previously unselected package libpcap0.8-dev:amd64.
Preparing to unpack .../2-libpcap0.8-dev_1.9.1-3_amd64.deb ...
Unpacking libpcap0.8-dev:amd64 (1.9.1-3) ...
Selecting previously unselected package libpcre16-3:amd64.
Preparing to unpack .../3-libpcre16-3_2%3a8.39-12build1_amd64.deb ...
Unpacking libpcre16-3:amd64 (2:8.39-12build1) ...
Selecting previously unselected package libpcre32-3:amd64.
Preparing to unpack .../4-libpcre32-3_2%3a8.39-12build1_amd64.deb ...
Unpacking libpcre32-3:amd64 (2:8.39-12build1) ...
Selecting previously unselected package libpcrecpp0v5:amd64.
Preparing to unpack .../5-libpcrecpp0v5_2%3a8.39-12build1_amd64.deb ...
Unpacking libpcrecpp0v5:amd64 (2:8.39-12build1) ...
Selecting previously unselected package libpcre3-dev:amd64.
Preparing to unpack .../6-libpcre3-dev_2%3a8.39-12build1_amd64.deb ...
Unpacking libpcre3-dev:amd64 (2:8.39-12build1) ...
Setting up libpcrecpp0v5:amd64 (2:8.39-12build1) ...
Setting up libpcre16-3:amd64 (2:8.39-12build1) ...
Setting up libpcap0.8-dev:amd64 (1.9.1-3) ...
Setting up libnet1:amd64 (1.1.6+dfsg-3.1build1) ...
Setting up libpcre32-3:amd64 (2:8.39-12build1) ...
Setting up libpcre3-dev:amd64 (2:8.39-12build1) ...
Setting up libnet1-dev (1.1.6+dfsg-3.1build1) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for libc-bin (2.31-0ubuntu9.2) ...
```

- Taisau, bet dar nesusikonfigūravo:

```
osboxes@ldvm1:/usr/local/src/snort-2.9.18$ ./configure --with-mysql --enable-dynamicplugin
configure: WARNING: unrecognized options: --with-mysql, --enable-dynamicplugin
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for a thread-safe mkdir -p... /usr/bin/mkdir -p
checking for gawk... no
checking for mawk... mawk
  ...
checking for SHA256_Init in -lcrypto... yes
checking for MD5_Init in -lcrypto... yes
checking dnet.h usability... no
checking dnet.h presence... no
checking for dnet.h... no
checking dumbnet.h usability... no
checking dumbnet.h presence... no
checking for dumbnet.h... no

   ERROR!  dnet header not found, go get it from
   http://code.google.com/p/libdnet/ or use the --with-dnet-*
   options, if you have it installed in an unusual place
```

- Trūksta `libdnet`.
- Ieškau ir diegiu `libdnet`:

```
osboxes@ldvm1:/usr/local/src/snort-2.9.18$ apt-cache search libdnet
dnet-common - Base package for Linux DECnet
libdnet - DECnet Libraries
libdnet-dev - DECnet development libraries & Headers
libdumbnet-dev - dumb, portable networking library -- development files
libdumbnet1 - dumb, portable networking library -- shared library
libnet-libdnet-perl - interface to libdumbnet's low-level network functions
libnet-libdnet6-perl - module to add IPv6 support to Net::Libdnet
osboxes@ldvm1:/usr/local/src/snort-2.9.18$ sudo apt-get install libdnet libdnet-dev
Reading package lists... Done
Building dependency tree
Reading state information... Done
Suggested packages:
  dnet-common
The following NEW packages will be installed:
  libdnet libdnet-dev
0 upgraded, 2 newly installed, 0 to remove and 153 not upgraded.
Need to get 357 kB of archives.
After this operation, 996 kB of additional disk space will be used.
Get:1 http://us.archive.ubuntu.com/ubuntu focal/universe amd64 libdnet amd64
2.65build2 [60.1 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu focal/universe amd64 libdnet-dev amd64
2.65build2 [297 kB]
Fetched 357 kB in 1s (248 kB/s)
Selecting previously unselected package libdnet:amd64.
(Reading database ... 197909 files and directories currently installed.)
Preparing to unpack .../libdnet_2.65build2_amd64.deb ...
Unpacking libdnet:amd64 (2.65build2) ...
Selecting previously unselected package libdnet-dev:amd64.
Preparing to unpack .../libdnet-dev_2.65build2_amd64.deb ...
Unpacking libdnet-dev:amd64 (2.65build2) ...
Setting up libdnet:amd64 (2.65build2) ...
Setting up libdnet-dev:amd64 (2.65build2) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for libc-bin (2.31-0ubuntu9.2) ...
```

- Konfigūruoju kompiliatorių, klaida išlieka:

```
osboxes@ldvm1:/usr/local/src/snort-2.9.18$ ./configure --with-mysql --enable-dynamicplugin
configure: WARNING: unrecognized options: --with-mysql, --enable-dynamicplugin
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for a thread-safe mkdir -p... /usr/bin/mkdir -p
checking for gawk... no
checking for mawk... mawk
  ...
checking for SHA256_Init in -lcrypto... yes
checking for MD5_Init in -lcrypto... yes
checking dnet.h usability... no
checking dnet.h presence... no
checking for dnet.h... no
checking dumbnet.h usability... no
checking dumbnet.h presence... no
checking for dumbnet.h... no

   ERROR!  dnet header not found, go get it from
   http://code.google.com/p/libdnet/ or use the --with-dnet-*
   options, if you have it installed in an unusual place
```

- Tikrinu `INSTALL` faile nurodytą įrankį:

```
osboxes@ldvm1:/usr/local/src/snort-2.9.18$ dnet-config

Command 'dnet-config' not found, but can be installed with:

sudo apt install libdumbnet-dev
```

- Išmetu `libdnet` paketus:

```
osboxes@ldvm1:/usr/local/src/snort-2.9.18$ sudo apt-get autoremove libdnet libdnet-dev
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages will be REMOVED:
  libdnet libdnet-dev
0 upgraded, 0 newly installed, 2 to remove and 153 not upgraded.
After this operation, 996 kB disk space will be freed.
Do you want to continue? [Y/n]
(Reading database ... 197958 files and directories currently installed.)
Removing libdnet-dev:amd64 (2.65build2) ...
Removing libdnet:amd64 (2.65build2) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for libc-bin (2.31-0ubuntu9.2) ...
```

- Diegiu `libdumbnet` paketus:

```
osboxes@ldvm1:/usr/local/src/snort-2.9.18$ sudo apt-get install libdumbnet-dev
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libdumbnet1
The following NEW packages will be installed:
  libdumbnet-dev libdumbnet1
0 upgraded, 2 newly installed, 0 to remove and 153 not upgraded.
Need to get 81.8 kB of archives.
After this operation, 329 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://us.archive.ubuntu.com/ubuntu focal/universe amd64 libdumbnet1 amd64
1.12-9build1 [25.4 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu focal/universe amd64 libdumbnet-dev amd64
1.12-9build1 [56.4 kB]
Fetched 81.8 kB in 1s (102 kB/s)
Selecting previously unselected package libdumbnet1:amd64.
(Reading database ... 197909 files and directories currently installed.)
Preparing to unpack .../libdumbnet1_1.12-9build1_amd64.deb ...
Unpacking libdumbnet1:amd64 (1.12-9build1) ...
Selecting previously unselected package libdumbnet-dev.
Preparing to unpack .../libdumbnet-dev_1.12-9build1_amd64.deb ...
Unpacking libdumbnet-dev (1.12-9build1) ...
Setting up libdumbnet1:amd64 (1.12-9build1) ...
Setting up libdumbnet-dev (1.12-9build1) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for libc-bin (2.31-0ubuntu9.2) ...
```

- Konfigūruoju kompiliatorių, nauja klaida:

```
osboxes@ldvm1:/usr/local/src/snort-2.9.18$ ./configure --with-mysql --enable-
dynamicplugin
configure: WARNING: unrecognized options: --with-mysql, --enable-dynamicplugin
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for a thread-safe mkdir -p... /usr/bin/mkdir -p
checking for gawk... no
  ...
checking dumbnet.h presence... yes
checking for dumbnet.h... yes
checking for eth_set in -ldnet... no
checking for eth_set in -ldumbnet... yes
checking for dlsym in -ldl... yes
./configure: line 12576: daq-modules-config: command not found
checking for daq_load_modules in -ldaq_static... no

   ERROR!  daq_static library not found, go get it from
   http://www.snort.org/.
```

- Diegiu `libdaq`:

```
osboxes@ldvm1:/usr/local/src/snort-2.9.18$ daq-modules-config

Command 'daq-modules-config' not found, but can be installed with:

sudo apt install libdaq-dev

osboxes@ldvm1:/usr/local/src/snort-2.9.18$ sudo apt-get install libdaq-dev
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libdaq2
The following NEW packages will be installed:
  libdaq-dev libdaq2
0 upgraded, 2 newly installed, 0 to remove and 153 not upgraded.
Need to get 171 kB of archives.
After this operation, 651 kB of additional disk space will be used.
Do you want to continue? [Y/n]
Get:1 http://us.archive.ubuntu.com/ubuntu focal/universe amd64 libdaq2 amd64 2.0.4-
3build2 [65.2 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu focal/universe amd64 libdaq-dev amd64
2.0.4-3build2 [106 kB]
Fetched 171 kB in 1s (124 kB/s)
Selecting previously unselected package libdaq2.
(Reading database ... 197948 files and directories currently installed.)
Preparing to unpack .../libdaq2_2.0.4-3build2_amd64.deb ...
Unpacking libdaq2 (2.0.4-3build2) ...
Selecting previously unselected package libdaq-dev.
Preparing to unpack .../libdaq-dev_2.0.4-3build2_amd64.deb ...
Unpacking libdaq-dev (2.0.4-3build2) ...
Setting up libdaq2 (2.0.4-3build2) ...
Setting up libdaq-dev (2.0.4-3build2) ...
Processing triggers for libc-bin (2.31-0ubuntu9.2) ...
```

- Konfigūruoju kompiliatorių, dar viena klaida:

```
osboxes@ldvm1:/usr/local/src/snort-2.9.18$ ./configure --with-mysql --enable-
dynamicplugin
configure: WARNING: unrecognized options: --with-mysql, --enable-dynamicplugin
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for a thread-safe mkdir -p... /usr/bin/mkdir -p
checking for gawk... no
  ...
checking for inflate in -lz... yes
checking lzma.h usability... no
checking lzma.h presence... no
checking for lzma.h... no
checking for lzma_stream_decoder in -llzma... no

   ERROR!  flex not found.
   Get it from http://flex.sourceforge.net/
   (You may also try lex instead.)
```

- Diegiu `flex` įrankį:

```
osboxes@ldvm1:/usr/local/src/snort-2.9.18$ flex

Command 'flex' not found, but can be installed with:

sudo apt install flex      # version 2.6.4-6.2, or
sudo apt install flex-old  # version 2.5.4a-10ubuntu2

osboxes@ldvm1:/usr/local/src/snort-2.9.18$ sudo apt-get install flex
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libfl-dev libfl2 libsigsegv2 m4
Suggested packages:
  bison build-essential flex-doc m4-doc
The following NEW packages will be installed:
  flex libfl-dev libfl2 libsigsegv2 m4
0 upgraded, 5 newly installed, 0 to remove and 153 not upgraded.
Need to get 547 kB of archives.
After this operation, 1,530 kB of additional disk space will be used.
Do you want to continue? [Y/n]
Get:1 http://us.archive.ubuntu.com/ubuntu focal/main amd64 libsigsegv2 amd64 2.12-2
[13.9 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu focal/main amd64 m4 amd64 1.4.18-4 [199
kB]
Get:3 http://us.archive.ubuntu.com/ubuntu focal/main amd64 flex amd64 2.6.4-6.2 [317
kB]
Get:4 http://us.archive.ubuntu.com/ubuntu focal/main amd64 libfl2 amd64 2.6.4-6.2
[11.5 kB]
Get:5 http://us.archive.ubuntu.com/ubuntu focal/main amd64 libfl-dev amd64 2.6.4-6.2
[6,316 B]
Fetched 547 kB in 2s (274 kB/s)
Selecting previously unselected package libsigsegv2:amd64.
(Reading database ... 197971 files and directories currently installed.)
Preparing to unpack .../libsigsegv2_2.12-2_amd64.deb ...
Unpacking libsigsegv2:amd64 (2.12-2) ...
Selecting previously unselected package m4.
Preparing to unpack .../archives/m4_1.4.18-4_amd64.deb ...
Unpacking m4 (1.4.18-4) ...
Selecting previously unselected package flex.
Preparing to unpack .../flex_2.6.4-6.2_amd64.deb ...
Unpacking flex (2.6.4-6.2) ...
Selecting previously unselected package libfl2:amd64.
Preparing to unpack .../libfl2_2.6.4-6.2_amd64.deb ...
Unpacking libfl2:amd64 (2.6.4-6.2) ...
Selecting previously unselected package libfl-dev:amd64.
Preparing to unpack .../libfl-dev_2.6.4-6.2_amd64.deb ...
Unpacking libfl-dev:amd64 (2.6.4-6.2) ...
Setting up libsigsegv2:amd64 (2.12-2) ...
Setting up libfl2:amd64 (2.6.4-6.2) ...
Setting up m4 (1.4.18-4) ...
Setting up flex (2.6.4-6.2) ...
Setting up libfl-dev:amd64 (2.6.4-6.2) ...
Processing triggers for libc-bin (2.31-0ubuntu9.2) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for install-info (6.7.0.dfsg.2-5) ...
```

- Vėl konfigūruoju kompiliatorių:

```
osboxes@ldvm1:/usr/local/src/snort-2.9.18$ ./configure --with-mysql --enable-dynamicplugin
configure: WARNING: unrecognized options: --with-mysql, --enable-dynamicplugin
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for a thread-safe mkdir -p... /usr/bin/mkdir -p
checking for gawk... no
  ...
checking for lzma.h... no
checking for lzma_stream_decoder in -llzma... no

   ERROR!  bison not found.
   Get it from http://www.gnu.org/software/bison/
   (You may also try byacc or yacc instead.)
```

- Diegiu `bison`:

```
osboxes@ldvm1:/usr/local/src/snort-2.9.18$ bison

Command 'bison' not found, but can be installed with:

sudo apt install bison    # version 2:3.5.1+dfsg-1, or
sudo apt install bison++  # version 1.21.11-4build1

osboxes@ldvm1:/usr/local/src/snort-2.9.18$ sudo apt-get install bison
Reading package lists... Done
Building dependency tree
Reading state information... Done
Suggested packages:
  bison-doc
The following NEW packages will be installed:
  bison
0 upgraded, 1 newly installed, 0 to remove and 153 not upgraded.
Need to get 657 kB of archives.
After this operation, 2,028 kB of additional disk space will be used.
Get:1 http://us.archive.ubuntu.com/ubuntu focal/main amd64 bison amd64 2:3.5.1+dfsg-1 [657 kB]
Fetched 657 kB in 2s (318 kB/s)
Selecting previously unselected package bison.
(Reading database ... 198128 files and directories currently installed.)
Preparing to unpack .../bison_2%3a3.5.1+dfsg-1_amd64.deb ...
Unpacking bison (2:3.5.1+dfsg-1) ...
Setting up bison (2:3.5.1+dfsg-1) ...
update-alternatives: using /usr/bin/bison.yacc to provide /usr/bin/yacc (yacc) in auto mode
Processing triggers for man-db (2.9.1-1) ...
```

- Vėl konfigūruoju kompiliatorių, dar viena klaida:

```
osboxes@ldvm1:/usr/local/src/snort-2.9.18$ ./configure --with-mysql --enable-
dynamicplugin
configure: WARNING: unrecognized options: --with-mysql, --enable-dynamicplugin
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for a thread-safe mkdir -p... /usr/bin/mkdir -p
  ...
checking for pthread_tryjoin_np... yes
checking for pkg-config... /usr/bin/pkg-config
checking pkg-config is at least version 0.9.0... yes
checking for luajit... no

   ERROR!  LuaJIT library not found. Go get it from http://www.luajit.org/ (or)
   Try compiling without openAppId using '--disable-open-appid'
configure: error: "Fatal!"
```

- Šį sykį mėginu apsieiti be nurodytos bibliotekos (ir OpenAppID palaikymo):

```
osboxes@ldvm1:/usr/local/src/snort-2.9.18$ ./configure --with-mysql --enable-
dynamicplugin --disable-open-appid
configure: WARNING: unrecognized options: --with-mysql, --enable-dynamicplugin
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for a thread-safe mkdir -p... /usr/bin/mkdir -p
checking for gawk... no
  ...
ecking for lzma_stream_decoder in -llzma... no
checking for pthread_tryjoin_np... yes
checking for nghttp2_option_new in -lnghttp2... no

   Libnghttp2 library not found.
   Get it from https://nghttp2.org/

checking for linuxthreads... no
checking for yylex_destroy support... yes
checking for SFLINUX... no
checking for WRLINUX... no
checking that generated files are newer than configure... done
configure: creating ./config.status
config.status: creating snort.pc
config.status: creating Makefile
config.status: creating src/Makefile
config.status: creating src/sfutil/Makefile
config.status: creating src/control/Makefile
config.status: creating src/file-process/Makefile
  ...
config.status: creating tools/file_server/Makefile
config.status: creating src/win32/Makefile
config.status: creating src/reload-adjust/Makefile
config.status: creating config.h
config.status: executing depfiles commands
config.status: executing libtool commands
configure: WARNING: unrecognized options: --with-mysql, --enable-dynamicplugin
```

- Tikrinu dvi minimas opcijas:

```
osboxes@ldvm1:/usr/local/src/snort-2.9.18$ ./configure --help | grep -i mysql
osboxes@ldvm1:/usr/local/src/snort-2.9.18$ ./configure --help | grep -i plugin
osboxes@ldvm1:/usr/local/src/snort-2.9.18$ ./configure --help | grep -i dynam
  --enable-so-with-static-lib  Enable linking of dynamically loaded preprocessors
with a static preprocessor library
  --enable-build-dynamic-examples   Enable building of example dynamically loaded
preprocessor and rule (off by default)
  --disable-dlclose        Only use if you are developing dynamic preprocessors or
shared object rules.  Disable (--disable-dlclose) for testing valgrind leaks in
dynamic libraries so a usable backtrace is reported.  Enabled by default.
```

- Nieko panašaus `./configure` skriptas nesiūlo.
- Turbūt pernelyg pasikeitė kodas versijoje 2.9.18. Mėginu jų nebenaudoti.

3. Konfigūracijos ir žurnalo direktorijos

Sunkumų neaptikta.

4. Pradinis stebėjimas

```
osboxes@ldvm1:/usr/local/src/snort-2.9.18$ sudo -i
root@ldvm1:~# snort -v > snort1
Running in packet dump mode

        --== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to passive.
Acquiring network traffic from "enp0s3".
Decoding Ethernet

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.18 GRE (Build 169)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2021 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.9.1 (with TPACKET_V3)
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.2.11


Commencing packet processing (pid=49740)
```

- Ir susiduriu kliūtim: Snort naudoja ne mano sukonfigūruotąją tinklo sąsają `enp0s8`. Panašu, kad naudoja pirmą sąsają iš eilės, `enp0s3`, per kurią nėra jokio srauto.
- Iškart kita kliūtis – Snort nereaguoja į `Ctrl-C` paspaudimus ir tęsia veikimą:

```
^C
^C^C
```

- Tuomet procesą tik pristabdau paspausdamas `Ctrl-Z` ir terminuoju su komanda `pkill`:

```
^Z
[1]+  Stopped                 snort -v > snort1
root@ldvm1:~#
root@ldvm1:~# pkill -9 snort
root@ldvm1:~#
[1]+  Killed                  snort -v > snort1
```

- Panašu į Snort bugą, kad kol nepagavo nei vieno paketo, programa ignoruoja `Ctrl-C` paspaudimus.
- Paskaitinėju `man snort` ir pakeičiu stebimą tinklo sąsają:

```
root@ldvm1:~# snort -v -i enp0s8 > snort1
Running in packet dump mode

        --== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to passive.
Acquiring network traffic from "enp0s8".
Decoding Ethernet

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.18 GRE (Build 169)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2021 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.9.1 (with TPACKET_V3)
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.2.11

Commencing packet processing (pid=51648)
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
^C*** Caught Int-Signal
===============================================================================
Run time for packet processing was 8.187221 seconds
Snort processed 23 packets.
Snort ran for 0 days 0 hours 0 minutes 8 seconds
   Pkts/sec:            2
===============================================================================
Memory usage summary:
  Total non-mmapped bytes (arena):       786432
  Bytes in mapped regions (hblkhd):      22941696
  Total allocated space (uordblks):      688640
  Total free space (fordblks):           97792
  Topmost releasable block (keepcost):   95696
===============================================================================
Packet I/O Totals:
   Received:           28
   Analyzed:           23 ( 82.143%)
    Dropped:            0 (  0.000%)
   Filtered:            0 (  0.000%)
Outstanding:            5 ( 17.857%)
   Injected:            0
===============================================================================
Breakdown by protocol (includes rebuilt packets):
        Eth:           23 (100.000%)
```

```
       VLAN:            0 (  0.000%)
        IP4:           23 (100.000%)
       Frag:            0 (  0.000%)
       ICMP:            0 (  0.000%)
        UDP:            0 (  0.000%)
        TCP:           23 (100.000%)
        IP6:            0 (  0.000%)
    IP6 Ext:            0 (  0.000%)
   IP6 Opts:            0 (  0.000%)
      Frag6:            0 (  0.000%)
      ICMP6:            0 (  0.000%)
       UDP6:            0 (  0.000%)
       TCP6:            0 (  0.000%)
     Teredo:            0 (  0.000%)
    ICMP-IP:            0 (  0.000%)
    IP4/IP4:            0 (  0.000%)
    IP4/IP6:            0 (  0.000%)
    IP6/IP4:            0 (  0.000%)
    IP6/IP6:            0 (  0.000%)
        GRE:            0 (  0.000%)
    GRE Eth:            0 (  0.000%)
   GRE VLAN:            0 (  0.000%)
    GRE IP4:            0 (  0.000%)
    GRE IP6:            0 (  0.000%)
GRE IP6 Ext:            0 (  0.000%)
   GRE PPTP:            0 (  0.000%)
    GRE ARP:            0 (  0.000%)
    GRE IPX:            0 (  0.000%)
   GRE Loop:            0 (  0.000%)
       MPLS:            0 (  0.000%)
        ARP:            0 (  0.000%)
        IPX:            0 (  0.000%)
   Eth Loop:            0 (  0.000%)
   Eth Disc:            0 (  0.000%)
   IP4 Disc:            0 (  0.000%)
   IP6 Disc:            0 (  0.000%)
   TCP Disc:            0 (  0.000%)
   UDP Disc:            0 (  0.000%)
  ICMP Disc:            0 (  0.000%)
All Discard:            0 (  0.000%)
      Other:            0 (  0.000%)
Bad Chk Sum:           12 ( 52.174%)
    Bad TTL:            0 (  0.000%)
     S5 G 1:            0 (  0.000%)
     S5 G 2:            0 (  0.000%)
      Total:           23
===============================================================================

Memory Statistics for File at:Wed Jul  7 07:52:55 2021

Total buffers allocated:           0
Total buffers freed:               0
Total buffers released:            0
Total file mempool:                0
Total allocated file mempool:      0
Total freed file mempool:          0
Total released file mempool:       0
```

```
Heap Statistics of file:
          Total Statistics:
               Memory in use:              0 bytes
                No of allocs:              0
                 No of frees:              0
===============================================================================
Snort exiting
```

- Sunkumas išspręstas nurodžius aktyvią tinklo sąsają.

5. Paketų rinkimo režimas

Sunkumų neaptikta.

6. Snort konfigūravimas

Sunkumų neaptikta.

7. Taisyklių vieta

Sunkumų neaptikta.

8. ICMP užklausų atpažinimas

```
root@ldvm1:~# /usr/local/bin/snort -u snort -g snort -c /etc/snort/snort.conf
Running in IDS mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/snort.conf"
ERROR: /etc/snort/snort.conf(48) Failed to parse the IP address: !$HOME_INET.
Fatal Error, Quitting..
```

- Gaunu klaidą. Matau perteklinę raidę kintamojo `HOME_INET` varde.
- Pataisau `snort.conf` ir startuoju paslaugą iš naujo.

```
root@ldvm1:~# fg 1
nano /etc/snort/snort.conf


Use "fg" to return to nano.

[1]+  Stopped                 nano /etc/snort/snort.conf

root@ldvm1:~# /usr/local/bin/snort -u snort -g snort -c /etc/snort/snort.conf
Running in IDS mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/snort.conf"
PortVar 'HTTP_PORTS' defined :  [ 80:81 311 383 591 593 901 1220 1414 1741 1830 2301
2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000
8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899
9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555 ]
PortVar 'SHELLCODE_PORTS' defined :  [ 0:79 81:65535 ]
PortVar 'ORACLE_PORTS' defined :  [ 1024:65535 ]
PortVar 'SSH_PORTS' defined :  [ 22 ]
PortVar 'FTP_PORTS' defined :  [ 21 2100 3535 ]
PortVar 'SIP_PORTS' defined :  [ 5060:5061 5600 ]
PortVar 'FILE_DATA_PORTS' defined :  [ 80:81 110 143 311 383 591 593 901 1220 1414
1741 1830 2301 2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510
7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300
8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002
55555 ]
PortVar 'GTP_PORTS' defined :  [ 2123 2152 3386 ]
Detection:
   Search-Method = AC-Full-Q
    Split Any/Any group = enabled
    Search-Method-Optimizations = enabled
    Maximum pattern length = 20
ERROR: /etc/snort/snort.conf(253) Could not stat dynamic module path
"/usr/local/lib/snort_dynamicrules": No such file or directory.

Fatal Error, Quitting..
```

- Tikrinu direktoriją:

```
root@ldvm1:~# ll -d /usr/local/lib/snort*
drwxr-xr-x 4 root root 4096 Jul  7 01:03 /usr/local/lib/snort/
drwxr-xr-x 2 root root 4096 Jul  7 01:03 /usr/local/lib/snort_dynamicengine/
drwxr-xr-x 2 root root 4096 Jul  7 01:03 /usr/local/lib/snort_dynamicpreprocessor/
```

- Susirandu dokumentą ir pagal jį sukuriu trūkstamą direktoriją: snort-centos6x-7x-298x.pdf (https://s3.amazonaws.com/snort-org-site/production/document_files/files/000/000/091/original/snort-centos6x-7x-298x.pdf#page=15)

```
root@ldvm1:~# mkdir /usr/local/lib/snort_dynamicrules
root@ldvm1:~# chown -R snort:snort /usr/local/lib/snort_dynamicrules
root@ldvm1:~# chmod -R 700 /usr/local/lib/snort_dynamicrules
root@ldvm1:~# ll -d /usr/local/lib/snort*
drwxr-xr-x 4 root  root  4096 Jul  7 01:03 /usr/local/lib/snort/
drwxr-xr-x 2 root  root  4096 Jul  7 01:03 /usr/local/lib/snort_dynamicengine/
drwxr-xr-x 2 root  root  4096 Jul  7 01:03 /usr/local/lib/snort_dynamicpreprocessor/
drwx------ 2 snort snort 4096 Jul  7 09:37 /usr/local/lib/snort_dynamicrules/
```

- Startuoju paslaugą iš naujo:

```
root@ldvm1:~# /usr/local/bin/snort -u snort -g snort -c /etc/snort/snort.conf
Running in IDS mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/snort.conf"
PortVar 'HTTP_PORTS' defined :  [ 80:81 311 383 591 593 901 1220 1414 1741 1830 2301
2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000
8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899
9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555 ]
PortVar 'SHELLCODE_PORTS' defined :  [ 0:79 81:65535 ]
PortVar 'ORACLE_PORTS' defined :  [ 1024:65535 ]
PortVar 'SSH_PORTS' defined :  [ 22 ]
PortVar 'FTP_PORTS' defined :  [ 21 2100 3535 ]
PortVar 'SIP_PORTS' defined :  [ 5060:5061 5600 ]
PortVar 'FILE_DATA_PORTS' defined :  [ 80:81 110 143 311 383 591 593 901 1220 1414
1741 1830 2301 2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510
7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300
8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002
55555 ]
PortVar 'GTP_PORTS' defined :  [ 2123 2152 3386 ]
Detection:
   Search-Method = AC-Full-Q
    Split Any/Any group = enabled
    Search-Method-Optimizations = enabled
    Maximum pattern length = 20
Tagged Packet Limit: 256
Loading dynamic engine /usr/local/lib/snort_dynamicengine/libsf_engine.so... done
Loading all dynamic detection libs from /usr/local/lib/snort_dynamicrules...
WARNING: No dynamic libraries found in directory /usr/local/lib/snort_dynamicrules.
  Finished Loading all dynamic detection libs from /usr/local/lib/snort_dynamicrules
Loading all dynamic preprocessor libs from
/usr/local/lib/snort_dynamicpreprocessor/...
  Loading dynamic preprocessor library
/usr/local/lib/snort_dynamicpreprocessor//libsf_dce2_preproc.so... done
  Loading dynamic preprocessor library
/usr/local/lib/snort_dynamicpreprocessor//libsf_dns_preproc.so... done
  Loading dynamic preprocessor library
/usr/local/lib/snort_dynamicpreprocessor//libsf_reputation_preproc.so... done
  Loading dynamic preprocessor library
/usr/local/lib/snort_dynamicpreprocessor//libsf_sip_preproc.so... done
  Loading dynamic preprocessor library
/usr/local/lib/snort_dynamicpreprocessor//libsf_ssh_preproc.so... done
  Loading dynamic preprocessor library
/usr/local/lib/snort_dynamicpreprocessor//libsf_sdf_preproc.so... done
  Loading dynamic preprocessor library
/usr/local/lib/snort_dynamicpreprocessor//libsf_s7commplus_preproc.so... done
  Loading dynamic preprocessor library
/usr/local/lib/snort_dynamicpreprocessor//libsf_dnp3_preproc.so... done
  Loading dynamic preprocessor library
/usr/local/lib/snort_dynamicpreprocessor//libsf_pop_preproc.so... done
  Loading dynamic preprocessor library
/usr/local/lib/snort_dynamicpreprocessor//libsf_imap_preproc.so... done
  Loading dynamic preprocessor library
```

```
/usr/local/lib/snort_dynamicpreprocessor//libsf_modbus_preproc.so... done
  Loading dynamic preprocessor library
/usr/local/lib/snort_dynamicpreprocessor//libsf_gtp_preproc.so... done
  Loading dynamic preprocessor library
/usr/local/lib/snort_dynamicpreprocessor//libsf_ftptelnet_preproc.so... done
  Loading dynamic preprocessor library
/usr/local/lib/snort_dynamicpreprocessor//libsf_ssl_preproc.so... done
  Loading dynamic preprocessor library
/usr/local/lib/snort_dynamicpreprocessor//libsf_smtp_preproc.so... done
  Finished Loading all dynamic preprocessor libs from
/usr/local/lib/snort_dynamicpreprocessor/
Log directory = /var/log/snort
WARNING: ip4 normalizations disabled because not inline.
WARNING: tcp normalizations disabled because not inline.
WARNING: icmp4 normalizations disabled because not inline.
WARNING: ip6 normalizations disabled because not inline.
WARNING: icmp6 normalizations disabled because not inline.
Frag3 global config:
    Max frags: 65536
    Fragment memory cap: 4194304 bytes
Frag3 engine config:
    Bound Address: default
    Target-based policy: WINDOWS
    Fragment timeout: 180 seconds
    Fragment min_ttl:   1
    Fragment Anomalies: Alert
    Overlap Limit:     10
    Min fragment Length:     100
      Max Expected Streams: 768
Stream global config:
    Track TCP sessions: ACTIVE
    Max TCP sessions: 262144
    TCP cache pruning timeout: 30 seconds
    TCP cache nominal timeout: 3600 seconds
    Memcap (for reassembly packet storage): 8388608
    Track UDP sessions: ACTIVE
    Max UDP sessions: 131072
    UDP cache pruning timeout: 30 seconds
    UDP cache nominal timeout: 180 seconds
    Track ICMP sessions: INACTIVE
    Track IP sessions: INACTIVE
    Log info if session memory consumption exceeds 1048576
    Send up to 2 active responses
    Wait at least 5 seconds between responses
    Protocol Aware Flushing: ACTIVE
        Maximum Flush Point: 16000
Stream TCP Policy config:
    Bound Address: default
    Reassembly Policy: WINDOWS
    Timeout: 180 seconds
    Limit on TCP Overlaps: 10
    Maximum number of bytes to queue per session: 1048576
    Maximum number of segs to queue per session: 2621
    Options:
        Require 3-Way Handshake: YES
        3-Way Handshake Timeout: 180
        Detect Anomalies: YES
    Reassembly Ports:
      21 client (Footprint)
      22 client (Footprint)
      23 client (Footprint)
      25 client (Footprint)
      42 client (Footprint)
      53 client (Footprint)
      79 client (Footprint)
      80 client (Footprint) server (Footprint)
      81 client (Footprint) server (Footprint)
      109 client (Footprint)
      110 client (Footprint)
      111 client (Footprint)
      113 client (Footprint)
      119 client (Footprint)
      135 client (Footprint)
      136 client (Footprint)
      137 client (Footprint)
      139 client (Footprint)
      143 client (Footprint)
      161 client (Footprint)
      additional ports configured but not printed.
Stream UDP Policy config:
    Timeout: 180 seconds
HttpInspect Config:
    GLOBAL CONFIG
      Detect Proxy Usage:       NO
      IIS Unicode Map Filename: /etc/snort/unicode.map
      IIS Unicode Map Codepage: 1252
      Memcap used for logging URI and Hostname: 150994944
      Max Gzip Memory: 838860
      Max Gzip Sessions: 1807
      Gzip Compress Depth: 65535
      Gzip Decompress Depth: 65535
      Normalize Random Nulls in Text: NO
    DEFAULT SERVER CONFIG:
      Server profile: All
      Ports (PAF): 80 81 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037
3128 3702 4343 4848 5250 6988 7000 7001 7144 7145 7510 7777 7779 8000 8008 8014 8028
8080 8085 8088 8090 8118 8123 8180 8181 8243 8280 8300 8800 8888 8899 9000 9060 9080
9090 9091 9443 9999 11371 34443 34444 41080 50002 55555
      Server Flow Depth: 0
      Client Flow Depth: 0
      Max Chunk Length: 500000
      Small Chunk Length Evasion: chunk size <= 10, threshold >= 5 times
      Max Header Field Length: 750
      Max Number Header Fields: 100
      Max Number of WhiteSpaces allowed with header folding: 200
      Inspect Pipeline Requests: YES
      URI Discovery Strict Mode: NO
      Allow Proxy Usage: NO
      Disable Alerting: NO
      Oversize Dir Length: 500
      Only inspect URI: NO
      Normalize HTTP Headers: NO
      Inspect HTTP Cookies: YES
      Inspect HTTP Responses: YES
      Extract Gzip from responses: YES
      Decompress response files:
      Unlimited decompression of gzip data from responses: YES
      Normalize Javascripts in HTTP Responses: YES
      Max Number of WhiteSpaces allowed with Javascript Obfuscation in HTTP
responses: 200
      Normalize HTTP Cookies: NO
      Enable XFF and True Client IP: NO
      Log HTTP URI data: NO
      Log HTTP Hostname data: NO
      Extended ASCII code support in URI: NO
      Ascii: YES alert: NO
      Double Decoding: YES alert: NO
      %U Encoding: YES alert: YES
      Bare Byte: YES alert: NO
      UTF 8: YES alert: NO
      IIS Unicode: YES alert: NO
      Multiple Slash: YES alert: NO
      IIS Backslash: YES alert: NO
      Directory Traversal: YES alert: NO
      Web Root Traversal: YES alert: NO
      Apache WhiteSpace: YES alert: NO
      IIS Delimiter: YES alert: NO
      IIS Unicode Map: GLOBAL IIS UNICODE MAP CONFIG
      Non-RFC Compliant Characters: 0x00 0x01 0x02 0x03 0x04 0x05 0x06 0x07
      Whitespace Characters: 0x09 0x0b 0x0c 0x0d
      Legacy mode: NO
rpc_decode arguments:
    Ports to decode RPC on: 111 32770 32771 32772 32773 32774 32775 32776 32777
32778 32779
    alert_fragments: INACTIVE
    alert_large_fragments: INACTIVE
    alert_incomplete: INACTIVE
    alert_multiple_requests: INACTIVE
FTPTelnet Config:
    GLOBAL CONFIG
      Inspection Type: stateful
      Check for Encrypted Traffic: YES alert: NO
      Continue to check encrypted data: YES
    TELNET CONFIG:
      Ports: 23
      Are You There Threshold: 20
      Normalize: YES
      Detect Anomalies: YES
    FTP CONFIG:
      FTP Server: default
        Ports (PAF): 21 2100 3535
        Check for Telnet Cmds: YES alert: YES
        Ignore Telnet Cmd Operations: YES alert: YES
        Ignore open data channels: NO
      FTP Client: default
        Check for Bounce Attacks: YES alert: YES
        Check for Telnet Cmds: YES alert: YES
        Ignore Telnet Cmd Operations: YES alert: YES
        Max Response Length: 256
SMTP Config:
    Ports: 25 465 587 691
    Inspection Type: Stateful
    Normalize: ATRN AUTH BDAT DATA DEBUG EHLO EMAL ESAM ESND ESOM ETRN EVFY EXPN
HELO HELP IDENT MAIL NOOP ONEX QUEU QUIT RCPT RSET SAML SEND STARTTLS SOML TICK TIME
TURN TURNME VERB VRFY X-EXPS XADR XAUTH XCIR XEXCH50 XGEN XLICENSE X-LINK2STATE XQUE
XSTA XTRN XUSR CHUNKING X-ADAT X-DRCP X-ERCP X-EXCH50
    Ignore Data: No
    Ignore TLS Data: No
    Ignore SMTP Alerts: No
    Max Command Line Length: 512
    Max auth Command Line Length: 1000
    Max Specific Command Line Length:
       ATRN:255 AUTH:246 BDAT:255 DATA:246 DEBUG:255
       EHLO:500 EMAL:255 ESAM:255 ESND:255 ESOM:255
       ETRN:246 EVFY:255 EXPN:255 HELO:500 HELP:500
       IDENT:255 MAIL:260 NOOP:255 ONEX:246 QUEU:246
       QUIT:246 RCPT:300 RSET:246 SAML:246 SEND:246
       SIZE:255 STARTTLS:246 SOML:246 TICK:246 TIME:246
       TURN:246 TURNME:246 VERB:246 VRFY:255 X-EXPS:246
       XADR:246 XAUTH:246 XCIR:246 XEXCH50:246 XGEN:246
       XLICENSE:246 X-LINK2STATE:246 XQUE:246 XSTA:246 XTRN:246
       XUSR:246
    Max Header Line Length: 1000
    Max Response Line Length: 512
    X-Link2State Alert: Yes
    Drop on X-Link2State Alert: No
    Alert on commands: None
    Alert on unknown commands: No
    SMTP Memcap: 838860
    MIME Max Mem: 838860
    Base64 Decoding: Enabled
    Base64 Decoding Depth: Unlimited
    Quoted-Printable Decoding: Enabled
    Quoted-Printable Decoding Depth: Unlimited
    Unix-to-Unix Decoding: Enabled
    Unix-to-Unix Decoding Depth: Unlimited
    Non-Encoded MIME attachment Extraction: Enabled
    Non-Encoded MIME attachment Extraction Depth: Unlimited
    Log Attachment filename: Enabled
    Log MAIL FROM Address: Enabled
    Log RCPT TO Addresses: Enabled
    Log Email Headers: Enabled
    Email Hdrs Log Depth: 1464
SSH config:
    Autodetection: ENABLED
    Challenge-Response Overflow Alert: ENABLED
    SSH1 CRC32 Alert: ENABLED
    Server Version String Overflow Alert: ENABLED
    Protocol Mismatch Alert: ENABLED
    Bad Message Direction Alert: DISABLED
    Bad Payload Size Alert: DISABLED
    Unrecognized Version Alert: DISABLED
    Max Encrypted Packets: 20
    Max Server Version String Length: 100
    MaxClientBytes: 19600 (Default)
    Ports:
        22
DCE/RPC 2 Preprocessor Configuration
```

```
  Global Configuration
    DCE/RPC Defragmentation: Enabled
    Memcap: 102400 KB
    Events: co
    SMB Fingerprint policy: Disabled
  Server Default Configuration
    Policy: WinXP
    Detect ports (PAF)
      SMB: 139 445
      TCP: 135
      UDP: 135
      RPC over HTTP server: 593
      RPC over HTTP proxy: None
    Autodetect ports (PAF)
      SMB: None
      TCP: 1025-65535
      UDP: 1025-65535
      RPC over HTTP server: 1025-65535
      RPC over HTTP proxy: None
    Invalid SMB shares: C$ D$ ADMIN$
    Maximum SMB command chaining: 3 commands
    SMB file inspection: Disabled
DNS config:
    DNS Client rdata txt Overflow Alert: ACTIVE
    Obsolete DNS RR Types Alert: INACTIVE
    Experimental DNS RR Types Alert: INACTIVE
    Ports: 53
SSLPP config:
    Encrypted packets: not inspected
    Ports:
      443      465      563      636      989
      992      993      994      995     7801
     7802     7900     7901     7902     7903
     7904     7905     7906     7907     7908
     7909     7910     7911     7912     7913
     7914     7915     7916     7917     7918
     7919     7920
    Server side data is trusted
    Maximum SSL Heartbeat length: 0
Sensitive Data preprocessor config:
    Global Alert Threshold: 25
    Masked Output: DISABLED
SIP config:
    Max number of sessions: 40000
    Max number of dialogs in a session: 4 (Default)
    Status: ENABLED
    Ignore media channel: DISABLED
    Max URI length: 512
    Max Call ID length: 80
    Max Request name length: 20 (Default)
    Max From length: 256 (Default)
    Max To length: 256 (Default)
    Max Via length: 1024 (Default)
    Max Contact length: 512
    Max Content length: 2048
    Ports:
        5060    5061    5600
    Methods:
          invite cancel ack bye register options refer subscribe update join info
message notify benotify do qauth sprack publish service unsubscribe prack
IMAP Config:
    Ports: 143
    IMAP Memcap: 838860
    MIME Max Mem: 838860
    Base64 Decoding: Enabled
    Base64 Decoding Depth: Unlimited
    Quoted-Printable Decoding: Enabled
    Quoted-Printable Decoding Depth: Unlimited
    Unix-to-Unix Decoding: Enabled
    Unix-to-Unix Decoding Depth: Unlimited
    Non-Encoded MIME attachment Extraction: Enabled
    Non-Encoded MIME attachment Extraction Depth: Unlimited
POP Config:
    Ports: 110
    POP Memcap: 838860
    MIME Max Mem: 838860
    Base64 Decoding: Enabled
    Base64 Decoding Depth: Unlimited
    Quoted-Printable Decoding: Enabled
    Quoted-Printable Decoding Depth: Unlimited
    Unix-to-Unix Decoding: Enabled
    Unix-to-Unix Decoding Depth: Unlimited
    Non-Encoded MIME attachment Extraction: Enabled
    Non-Encoded MIME attachment Extraction Depth: Unlimited
Modbus config:
    Ports:
        502
DNP3 config:
    Memcap: 262144
    Check Link-Layer CRCs: ENABLED
    Ports:
        20000
Reputation config:
ERROR: /etc/snort/snort.conf(512) => Unable to open address file
/etc/snort/../rules/white_list.rules, Error: No such file or directory
Fatal Error, Quitting..
```

- Tikrinu nurodytą failą ir jo direktoriją:

```
root@ldvm1:~# grep white_list.rules /etc/snort/snort.conf
   whitelist $WHITE_LIST_PATH/white_list.rules, \

root@ldvm1:~# grep -w WHITE_LIST_PATH /etc/snort/snort.conf
var WHITE_LIST_PATH ../rules
   whitelist $WHITE_LIST_PATH/white_list.rules, \

root@ldvm1:~# find /etc/snort -name white_list.rules
root@ldvm1:~# find / -name white_list.rules
find: ‘/run/user/1000/gvfs’: Permission denied
```

- Tokio failo nėra. Tikrinu jo naudotoją:

```
root@ldvm1:~# grep -C5 WHITE_LIST_PATH/ /etc/snort/snort.conf
# Reputation preprocessor. For more information see README.reputation
preprocessor reputation: \
   memcap 500, \
   priority whitelist, \
   nested_ip inner, \
   whitelist $WHITE_LIST_PATH/white_list.rules, \
   blacklist $BLACK_LIST_PATH/black_list.rules

###################################################
# Step #6: Configure output plugins
# For more information, see Snort Manual, Configuring Snort - Output Modules
```

- Tai preprocesorius `reputation`. Išjungiu jį:

```
root@ldvm1:~# fg
nano /etc/snort/snort.conf


Use "fg" to return to nano.

[1]+  Stopped                 nano /etc/snort/snort.conf

root@ldvm1:~# grep -C5 WHITE_LIST_PATH/ /etc/snort/snort.conf
# 2021-07-07 saukrs: Užkomentuoju, nes neturiu "white_list.rules"
#preprocessor reputation: \
#   memcap 500, \
#   priority whitelist, \
#   nested_ip inner, \
#   whitelist $WHITE_LIST_PATH/white_list.rules, \
#   blacklist $BLACK_LIST_PATH/black_list.rules

###################################################
# Step #6: Configure output plugins
# For more information, see Snort Manual, Configuring Snort - Output Modules
```

- Snort paslauga veikia:

```
root@ldvm1:~# /usr/local/bin/snort -u snort -g snort -c /etc/snort/snort.conf -i
enp0s8
Running in IDS mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/snort.conf"
PortVar 'HTTP_PORTS' defined :  [ 80:81 311 383 591 593 901 1220 1414 1741 1830 2301
2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000
8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899
9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555 ]
PortVar 'SHELLCODE_PORTS' defined :  [ 0:79 81:65535 ]
PortVar 'ORACLE_PORTS' defined :  [ 1024:65535 ]
PortVar 'SSH_PORTS' defined :  [ 22 ]
PortVar 'FTP_PORTS' defined :  [ 21 2100 3535 ]
PortVar 'SIP_PORTS' defined :  [ 5060:5061 5600 ]
PortVar 'FILE_DATA_PORTS' defined :  [ 80:81 110 143 311 383 591 593 901 1220 1414
1741 1830 2301 2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510
7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300
8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002
55555 ]
PortVar 'GTP_PORTS' defined :  [ 2123 2152 3386 ]
Detection:
   Search-Method = AC-Full-Q
    Split Any/Any group = enabled
    Search-Method-Optimizations = enabled
    Maximum pattern length = 20
Tagged Packet Limit: 256
Loading dynamic engine /usr/local/lib/snort_dynamicengine/libsf_engine.so... done
Loading all dynamic detection libs from /usr/local/lib/snort_dynamicrules...
WARNING: No dynamic libraries found in directory /usr/local/lib/snort_dynamicrules.
  Finished Loading all dynamic detection libs from /usr/local/lib/snort_dynamicrules
Loading all dynamic preprocessor libs from
/usr/local/lib/snort_dynamicpreprocessor/...
  Loading dynamic preprocessor library
/usr/local/lib/snort_dynamicpreprocessor//libsf_dce2_preproc.so... done
  Loading dynamic preprocessor library
/usr/local/lib/snort_dynamicpreprocessor//libsf_dns_preproc.so... done
  Loading dynamic preprocessor library
/usr/local/lib/snort_dynamicpreprocessor//libsf_reputation_preproc.so... done
  Loading dynamic preprocessor library
/usr/local/lib/snort_dynamicpreprocessor//libsf_sip_preproc.so... done
  Loading dynamic preprocessor library
/usr/local/lib/snort_dynamicpreprocessor//libsf_ssh_preproc.so... done
  Loading dynamic preprocessor library
/usr/local/lib/snort_dynamicpreprocessor//libsf_sdf_preproc.so... done
  Loading dynamic preprocessor library
/usr/local/lib/snort_dynamicpreprocessor//libsf_s7commplus_preproc.so... done
  Loading dynamic preprocessor library
/usr/local/lib/snort_dynamicpreprocessor//libsf_dnp3_preproc.so... done
  Loading dynamic preprocessor library
/usr/local/lib/snort_dynamicpreprocessor//libsf_pop_preproc.so... done
  Loading dynamic preprocessor library
/usr/local/lib/snort_dynamicpreprocessor//libsf_imap_preproc.so... done
```

```
  Loading dynamic preprocessor library
/usr/local/lib/snort_dynamicpreprocessor//libsf_modbus_preproc.so... done
  Loading dynamic preprocessor library
/usr/local/lib/snort_dynamicpreprocessor//libsf_gtp_preproc.so... done
  Loading dynamic preprocessor library
/usr/local/lib/snort_dynamicpreprocessor//libsf_ftptelnet_preproc.so... done
  Loading dynamic preprocessor library
/usr/local/lib/snort_dynamicpreprocessor//libsf_ssl_preproc.so... done
  Loading dynamic preprocessor library
/usr/local/lib/snort_dynamicpreprocessor//libsf_smtp_preproc.so... done
  Finished Loading all dynamic preprocessor libs from
/usr/local/lib/snort_dynamicpreprocessor/
Log directory = /var/log/snort
WARNING: ip4 normalizations disabled because not inline.
WARNING: tcp normalizations disabled because not inline.
WARNING: icmp4 normalizations disabled because not inline.
WARNING: ip6 normalizations disabled because not inline.
WARNING: icmp6 normalizations disabled because not inline.
Frag3 global config:
    Max frags: 65536
    Fragment memory cap: 4194304 bytes
Frag3 engine config:
    Bound Address: default
    Target-based policy: WINDOWS
    Fragment timeout: 180 seconds
    Fragment min_ttl:   1
    Fragment Anomalies: Alert
    Overlap Limit:     10
    Min fragment Length:     100
      Max Expected Streams: 768
Stream global config:
    Track TCP sessions: ACTIVE
    Max TCP sessions: 262144
    TCP cache pruning timeout: 30 seconds
    TCP cache nominal timeout: 3600 seconds
    Memcap (for reassembly packet storage): 8388608
    Track UDP sessions: ACTIVE
    Max UDP sessions: 131072
    UDP cache pruning timeout: 30 seconds
    UDP cache nominal timeout: 180 seconds
    Track ICMP sessions: INACTIVE
    Track IP sessions: INACTIVE
    Log info if session memory consumption exceeds 1048576
    Send up to 2 active responses
    Wait at least 5 seconds between responses
    Protocol Aware Flushing: ACTIVE
        Maximum Flush Point: 16000
Stream TCP Policy config:
    Bound Address: default
    Reassembly Policy: WINDOWS
    Timeout: 180 seconds
    Limit on TCP Overlaps: 10
    Maximum number of bytes to queue per session: 1048576
    Maximum number of segs to queue per session: 2621
    Options:
        Require 3-Way Handshake: YES
        3-Way Handshake Timeout: 180
        Detect Anomalies: YES
    Reassembly Ports:
      21 client (Footprint)
      22 client (Footprint)
      23 client (Footprint)
      25 client (Footprint)
      42 client (Footprint)
      53 client (Footprint)
      79 client (Footprint)
      80 client (Footprint) server (Footprint)
      81 client (Footprint) server (Footprint)
      109 client (Footprint)
      110 client (Footprint)
      111 client (Footprint)
      113 client (Footprint)
      119 client (Footprint)
      135 client (Footprint)
      136 client (Footprint)
      137 client (Footprint)
      139 client (Footprint)
      143 client (Footprint)
      161 client (Footprint)
      additional ports configured but not printed.
Stream UDP Policy config:
    Timeout: 180 seconds
HttpInspect Config:
    GLOBAL CONFIG
      Detect Proxy Usage:       NO
      IIS Unicode Map Filename: /etc/snort/unicode.map
      IIS Unicode Map Codepage: 1252
      Memcap used for logging URI and Hostname: 150994944
      Max Gzip Memory: 838860
      Max Gzip Sessions: 1807
      Gzip Compress Depth: 65535
      Gzip Decompress Depth: 65535
      Normalize Random Nulls in Text: NO
    DEFAULT SERVER CONFIG:
      Server profile: All
      Ports (PAF): 80 81 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037
3128 3702 4343 4848 5250 6988 7000 7001 7144 7145 7510 7777 7779 8000 8008 8014 8028
8080 8085 8088 8090 8118 8123 8180 8181 8243 8280 8300 8800 8888 8899 9000 9060 9080
9090 9091 9443 9999 11371 34443 34444 41080 50002 55555
      Server Flow Depth: 0
      Client Flow Depth: 0
      Max Chunk Length: 500000
      Small Chunk Length Evasion: chunk size <= 10, threshold >= 5 times
      Max Header Field Length: 750
      Max Number Header Fields: 100
      Max Number of WhiteSpaces allowed with header folding: 200
      Inspect Pipeline Requests: YES
      URI Discovery Strict Mode: NO
      Allow Proxy Usage: NO
      Disable Alerting: NO
      Oversize Dir Length: 500
      Only inspect URI: NO
      Normalize HTTP Headers: NO
      Inspect HTTP Cookies: YES
      Inspect HTTP Responses: YES
      Extract Gzip from responses: YES
      Decompress response files:
      Unlimited decompression of gzip data from responses: YES
      Normalize Javascripts in HTTP Responses: YES
      Max Number of WhiteSpaces allowed with Javascript Obfuscation in HTTP
responses: 200
      Normalize HTTP Cookies: NO
      Enable XFF and True Client IP: NO
      Log HTTP URI data: NO
      Log HTTP Hostname data: NO
      Extended ASCII code support in URI: NO
      Ascii: YES alert: NO
      Double Decoding: YES alert: NO
      %U Encoding: YES alert: YES
      Bare Byte: YES alert: NO
      UTF 8: YES alert: NO
      IIS Unicode: YES alert: NO
      Multiple Slash: YES alert: NO
      IIS Backslash: YES alert: NO
      Directory Traversal: YES alert: NO
      Web Root Traversal: YES alert: NO
      Apache WhiteSpace: YES alert: NO
      IIS Delimiter: YES alert: NO
      IIS Unicode Map: GLOBAL IIS UNICODE MAP CONFIG
      Non-RFC Compliant Characters: 0x00 0x01 0x02 0x03 0x04 0x05 0x06 0x07
      Whitespace Characters: 0x09 0x0b 0x0c 0x0d
      Legacy mode: NO
rpc_decode arguments:
    Ports to decode RPC on: 111 32770 32771 32772 32773 32774 32775 32776 32777
32778 32779
    alert_fragments: INACTIVE
    alert_large_fragments: INACTIVE
    alert_incomplete: INACTIVE
    alert_multiple_requests: INACTIVE
FTPTelnet Config:
    GLOBAL CONFIG
      Inspection Type: stateful
      Check for Encrypted Traffic: YES alert: NO
      Continue to check encrypted data: YES
    TELNET CONFIG:
      Ports: 23
      Are You There Threshold: 20
      Normalize: YES
      Detect Anomalies: YES
    FTP CONFIG:
      FTP Server: default
        Ports (PAF): 21 2100 3535
        Check for Telnet Cmds: YES alert: YES
        Ignore Telnet Cmd Operations: YES alert: YES
        Ignore open data channels: NO
      FTP Client: default
        Check for Bounce Attacks: YES alert: YES
        Check for Telnet Cmds: YES alert: YES
        Ignore Telnet Cmd Operations: YES alert: YES
        Max Response Length: 256
SMTP Config:
    Ports: 25 465 587 691
    Inspection Type: Stateful
    Normalize: ATRN AUTH BDAT DATA DEBUG EHLO EMAL ESAM ESND ESOM ETRN EVFY EXPN
HELO HELP IDENT MAIL NOOP ONEX QUEU QUIT RCPT RSET SAML SEND STARTTLS SOML TICK TIME
TURN TURNME VERB VRFY X-EXPS XADR XAUTH XCIR XEXCH50 XGEN XLICENSE X-LINK2STATE XQUE
XSTA XTRN XUSR CHUNKING X-ADAT X-DRCP X-ERCP X-EXCH50
    Ignore Data: No
    Ignore TLS Data: No
    Ignore SMTP Alerts: No
    Max Command Line Length: 512
    Max auth Command Line Length: 1000
    Max Specific Command Line Length:
       ATRN:255 AUTH:246 BDAT:255 DATA:246 DEBUG:255
       EHLO:500 EMAL:255 ESAM:255 ESND:255 ESOM:255
       ETRN:246 EVFY:255 EXPN:255 HELO:500 HELP:500
       IDENT:255 MAIL:260 NOOP:255 ONEX:246 QUEU:246
       QUIT:246 RCPT:300 RSET:246 SAML:246 SEND:246
       SIZE:255 STARTTLS:246 SOML:246 TICK:246 TIME:246
       TURN:246 TURNME:246 VERB:246 VRFY:255 X-EXPS:246
       XADR:246 XAUTH:246 XCIR:246 XEXCH50:246 XGEN:246
       XLICENSE:246 X-LINK2STATE:246 XQUE:246 XSTA:246 XTRN:246
       XUSR:246
    Max Header Line Length: 1000
    Max Response Line Length: 512
    X-Link2State Alert: Yes
    Drop on X-Link2State Alert: No
    Alert on commands: None
    Alert on unknown commands: No
    SMTP Memcap: 838860
    MIME Max Mem: 838860
    Base64 Decoding: Enabled
    Base64 Decoding Depth: Unlimited
    Quoted-Printable Decoding: Enabled
    Quoted-Printable Decoding Depth: Unlimited
    Unix-to-Unix Decoding: Enabled
    Unix-to-Unix Decoding Depth: Unlimited
    Non-Encoded MIME attachment Extraction: Enabled
    Non-Encoded MIME attachment Extraction Depth: Unlimited
    Log Attachment filename: Enabled
    Log MAIL FROM Address: Enabled
    Log RCPT TO Addresses: Enabled
    Log Email Headers: Enabled
    Email Hdrs Log Depth: 1464
SSH config:
    Autodetection: ENABLED
    Challenge-Response Overflow Alert: ENABLED
    SSH1 CRC32 Alert: ENABLED
    Server Version String Overflow Alert: ENABLED
    Protocol Mismatch Alert: ENABLED
    Bad Message Direction Alert: DISABLED
    Bad Payload Size Alert: DISABLED
    Unrecognized Version Alert: DISABLED
    Max Encrypted Packets: 20
    Max Server Version String Length: 100
    MaxClientBytes: 19600 (Default)
    Ports:
        22
```

```
DCE/RPC 2 Preprocessor Configuration
  Global Configuration
    DCE/RPC Defragmentation: Enabled
    Memcap: 102400 KB
    Events: co
    SMB Fingerprint policy: Disabled
  Server Default Configuration
    Policy: WinXP
    Detect ports (PAF)
      SMB: 139 445
      TCP: 135
      UDP: 135
      RPC over HTTP server: 593
      RPC over HTTP proxy: None
    Autodetect ports (PAF)
      SMB: None
      TCP: 1025-65535
      UDP: 1025-65535
      RPC over HTTP server: 1025-65535
      RPC over HTTP proxy: None
    Invalid SMB shares: C$ D$ ADMIN$
    Maximum SMB command chaining: 3 commands
    SMB file inspection: Disabled
DNS config:
    DNS Client rdata txt Overflow Alert: ACTIVE
    Obsolete DNS RR Types Alert: INACTIVE
    Experimental DNS RR Types Alert: INACTIVE
    Ports: 53
SSLPP config:
    Encrypted packets: not inspected
    Ports:
      443      465      563      636      989
      992      993      994      995     7801
     7802     7900     7901     7902     7903
     7904     7905     7906     7907     7908
     7909     7910     7911     7912     7913
     7914     7915     7916     7917     7918
     7919     7920
    Server side data is trusted
    Maximum SSL Heartbeat length: 0
Sensitive Data preprocessor config:
    Global Alert Threshold: 25
    Masked Output: DISABLED
SIP config:
    Max number of sessions: 40000
    Max number of dialogs in a session: 4 (Default)
    Status: ENABLED
    Ignore media channel: DISABLED
    Max URI length: 512
    Max Call ID length: 80
    Max Request name length: 20 (Default)
    Max From length: 256 (Default)
    Max To length: 256 (Default)
    Max Via length: 1024 (Default)
    Max Contact length: 512
    Max Content length: 2048
    Ports:
        5060    5061    5600
    Methods:
          invite cancel ack bye register options refer subscribe update join info
message notify benotify do qauth sprack publish service unsubscribe prack
IMAP Config:
    Ports: 143
    IMAP Memcap: 838860
    MIME Max Mem: 838860
    Base64 Decoding: Enabled
    Base64 Decoding Depth: Unlimited
    Quoted-Printable Decoding: Enabled
    Quoted-Printable Decoding Depth: Unlimited
    Unix-to-Unix Decoding: Enabled
    Unix-to-Unix Decoding Depth: Unlimited
    Non-Encoded MIME attachment Extraction: Enabled
    Non-Encoded MIME attachment Extraction Depth: Unlimited
POP Config:
    Ports: 110
    POP Memcap: 838860
    MIME Max Mem: 838860
    Base64 Decoding: Enabled
    Base64 Decoding Depth: Unlimited
    Quoted-Printable Decoding: Enabled
    Quoted-Printable Decoding Depth: Unlimited
    Unix-to-Unix Decoding: Enabled
    Unix-to-Unix Decoding Depth: Unlimited
    Non-Encoded MIME attachment Extraction: Enabled
    Non-Encoded MIME attachment Extraction Depth: Unlimited
Modbus config:
    Ports:
        502
DNP3 config:
    Memcap: 262144
    Check Link-Layer CRCs: ENABLED
    Ports:
        20000

+++++++++++++++++++++++++++++++++++++++++++++++++++
Initializing rule chains...
1 Snort rules read
    1 detection rules
    0 decoder rules
    0 preprocessor rules
1 Option Chains linked into 1 Chain Headers
+++++++++++++++++++++++++++++++++++++++++++++++++++

+-------------------[Rule Port Counts]---------------------------------------
|             tcp     udp    icmp      ip
|     src       0       0       0       0
|     dst       0       0       0       0
|     any       0       0       1       0
|      nc       0       0       1       0
|     s+d       0       0       0       0
+----------------------------------------------------------------------------

+-----------------------[detection-filter-config]------------------------------
| memory-cap : 1048576 bytes
```

```
+-----------------------[detection-filter-rules]--------------------------------
| none
--------------------------------------------------------------------------------

+-----------------------[rate-filter-config]------------------------------------
| memory-cap : 1048576 bytes
+-----------------------[rate-filter-rules]-------------------------------------
| none
--------------------------------------------------------------------------------

+-----------------------[event-filter-config]-----------------------------------
| memory-cap : 1048576 bytes
+-----------------------[event-filter-global]-----------------------------------
+-----------------------[event-filter-local]------------------------------------
| none
+-----------------------[suppression]-------------------------------------------
| none
--------------------------------------------------------------------------------
Rule application order: pass->drop->sdrop->reject->alert->log
Verifying Preprocessor Configurations!

[ Port Based Pattern Matching Memory ]
[ Number of patterns truncated to 20 bytes: 0 ]
pcap DAQ configured to passive.
Acquiring network traffic from "enp0s8".
Reload thread starting...
Reload thread started, thread 0x7fe51e0c8700 (52340)
Decoding Ethernet
Set gid to 1001
Set uid to 1001

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.18 GRE (Build 169)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2021 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.9.1 (with TPACKET_V3)
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.2.11

           Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 3.2  <Build 1>
           Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
           Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
           Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
           Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
           Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
           Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
           Preprocessor Object: SF_POP  Version 1.0  <Build 1>
           Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
           Preprocessor Object: SF_S7COMMPLUS  Version 1.0  <Build 1>
           Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
           Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
           Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
           Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
           Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
           Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
Commencing packet processing (pid=52335)
```

9. *Telnet* paruošimas

Sunkumų neaptikta.

10. *Telnet* tikrinimas

- Akivaizdu, kad prisijungti nepavyko: *telnet* paslauga instaliuota ne į jį.
- Jungiuosi priešingai – **iš** kaimyno į savo virtualų kompiuterį:

```
osboxes@ldvm2:~$ telnet 192.168.10.14
Trying 192.168.10.14...
Connected to 192.168.10.14.
Escape character is '^]'.
Ubuntu 20.04.2 LTS
ldvm1 login:
```

- Vedu vartotojo vardą `root`:

```
ldvm1 login: root
Password:

Login incorrect
ldvm1 login:
telnet> Connection closed.
```

- Analizuoju Snort įrašus. Deja, naujų neatsirado, tik senasis ICMP:

```
osboxes@ldvm1:~$ grep 1000000 /var/log/snort/alert
[**] [1:10000001:0] ICMP test [**]
[**] [1:10000001:0] ICMP test [**]
```

- Prisimenu konfigūravimo scenarijaus perspėjimus apie DAQ.
- Kartoju konfigūravimą, ieškau pranešimų apie DAQ:

```
osboxes@ldvm1:/usr/local/src/snort-2.9.18$ ./configure | grep -i daq
checking for daq_load_modules in -ldaq_static... yes
checking for daq_hup_apply... yes
checking for daq_acquire_with_meta... yes
checking for daq_dp_add_dc... yes
checking for daq real addresses... no
checking whether DAQ_PKT_FLAG_DECRYPTED_SSL is declared... no
checking whether DAQ_PKT_FLAG_LOCALLY_ORIGINATED is declared... no
checking whether DAQ_PKT_FLAG_LOCALLY_DESTINED is declared... no
checking for struct _DAQ_DP_key_t.sa.src_ip4... yes
checking for daq address space ID... yes
checking for daq flow ID... yes
checking for daq extended flow modifiers... no
checking for daq query flow... no
checking for daq data channel flags... no
checking for DAQ_VERDICT_RETRY... yes
checking for daq packet trace... no
DAQ version doesn't support packet trace.
checking for daq verdict reason... no
DAQ version doesn't support tracing verdict reason.
```

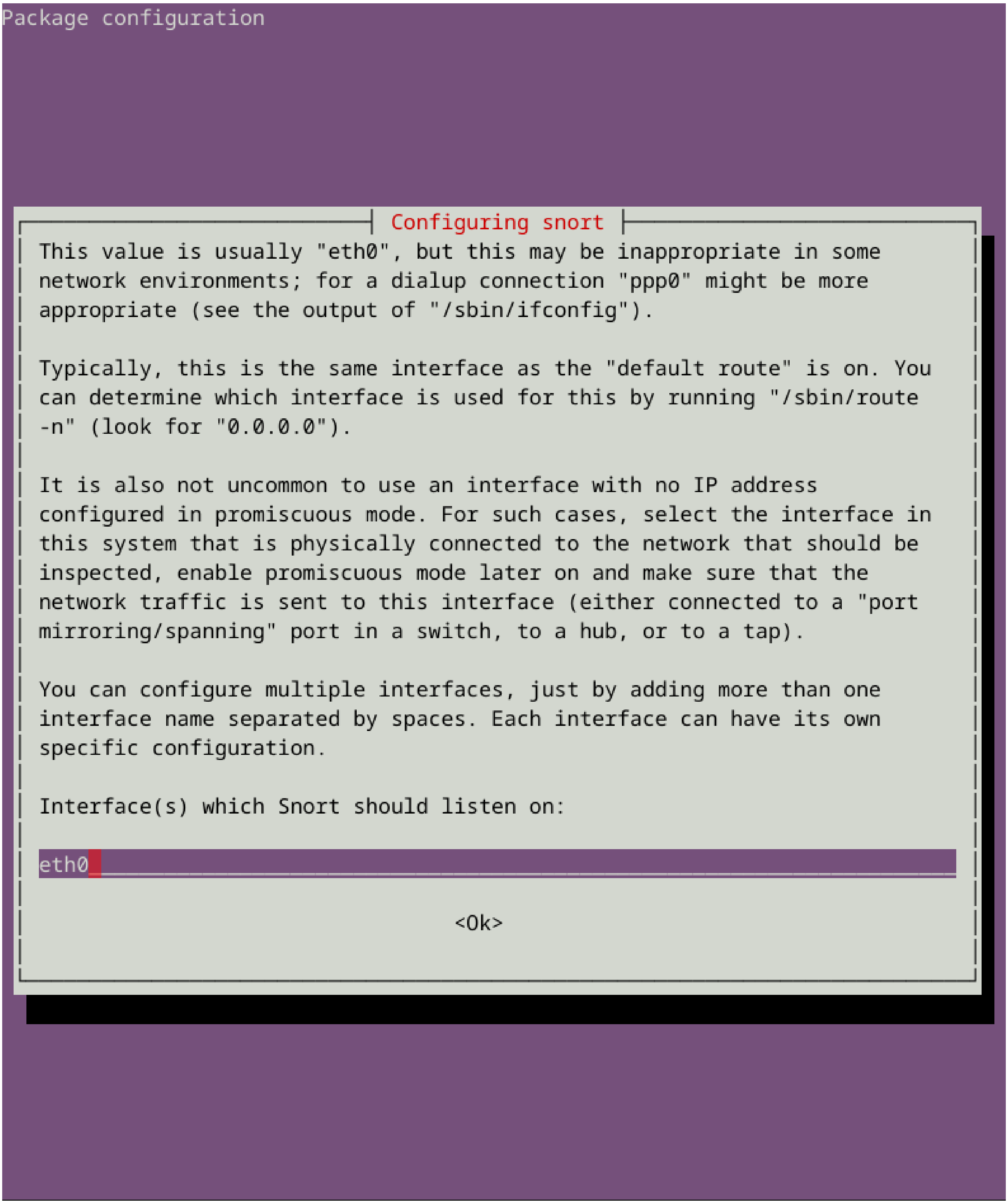
- Kyla įtarimas, kad nauja Snort versija nėra pilnai suderinama su sena DAQ biblioteka.
- Pasižymiu Snort versiją, stabdau ją ir darau `make uninstall`:

```
osboxes@ldvm1:/usr/local/src/snort-2.9.18$ snort -V 2>&1 | tee ~/debug/12.snort-iš-
src.txt

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.18 GRE (Build 169)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2021 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.9.1 (with TPACKET_V3)
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.2.11

osboxes@ldvm1:/usr/local/src/snort-2.9.18$ sudo make uninstall
[sudo] password for osboxes:
Making uninstall in src
make[1]: Entering directory '/usr/local/src/snort-2.9.18/src'
Making uninstall in sfutil
make[2]: Entering directory '/usr/local/src/snort-2.9.18/src/sfutil'
make[2]: Nothing to be done for 'uninstall'.
make[2]: Leaving directory '/usr/local/src/snort-2.9.18/src/sfutil'
  ...
make[2]: Leaving directory '/usr/local/src/snort-2.9.18/tools/u2boat'
Making uninstall in u2spewfoo
make[2]: Entering directory '/usr/local/src/snort-2.9.18/tools/u2spewfoo'
 ( cd '/usr/local/bin' && rm -f u2spewfoo )
make[2]: Leaving directory '/usr/local/src/snort-2.9.18/tools/u2spewfoo'
make[2]: Entering directory '/usr/local/src/snort-2.9.18/tools'
make[2]: Leaving directory '/usr/local/src/snort-2.9.18/tools'
make[1]: Leaving directory '/usr/local/src/snort-2.9.18/tools'
make[1]: Entering directory '/usr/local/src/snort-2.9.18'
 ( cd '/usr/local/share/man/man8' && rm -f snort.8 )
 ( cd '/usr/local/lib/pkgconfig' && rm -f snort.pc )
make[1]: Leaving directory '/usr/local/src/snort-2.9.18'
```

- Instaliuoju paketinę Snort versiją:

```
osboxes@ldvm1:/usr/local/src/snort-2.9.18$ sudo apt-get install snort
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  oinkmaster snort-common snort-common-libraries snort-rules-default
Suggested packages:
  snort-doc
The following NEW packages will be installed:
  oinkmaster snort snort-common snort-common-libraries snort-rules-default
0 upgraded, 5 newly installed, 0 to remove and 154 not upgraded.
Need to get 0 B/1,333 kB of archives.
After this operation, 7,051 kB of additional disk space will be used.
Do you want to continue? [Y/n]
```

- Nurodau `enp0s8` tinklo sąsają.



```
Package configuration

                         ┤ Configuring snort ├
 This value is usually "eth0", but this may be inappropriate in some
 network environments; for a dialup connection "ppp0" might be more
 appropriate (see the output of "/sbin/ifconfig").

 Typically, this is the same interface as the "default route" is on. You
 can determine which interface is used for this by running "/sbin/route
 -n" (look for "0.0.0.0").

 It is also not uncommon to use an interface with no IP address
 configured in promiscuous mode. For such cases, select the interface in
 this system that is physically connected to the network that should be
 inspected, enable promiscuous mode later on and make sure that the
 network traffic is sent to this interface (either connected to a "port
 mirroring/spanning" port in a switch, to a hub, or to a tap).

 You can configure multiple interfaces, just by adding more than one
 interface name separated by spaces. Each interface can have its own
 specific configuration.

 Interface(s) which Snort should listen on:

 eth0

                                  <Ok>
```

```
----8><----------------------------------------------------------------------
Package configuration


 ┌────────────────────────────┤ Configuring snort ├───────────────────────────┐
 │ This value is usually "eth0", but this may be inappropriate in some        │
 │ network environments; for a dialup connection "ppp0" might be more         │
 │ appropriate (see the output of "/sbin/ifconfig").                          │
 │                                                                            │
 │ Typically, this is the same interface as the "default route" is on. You    │
 │ can determine which interface is used for this by running "/sbin/route     │
 │ -n" (look for "0.0.0.0").                                                  │
 │                                                                            │
 │ It is also not uncommon to use an interface with no IP address             │
 │ configured in promiscuous mode. For such cases, select the interface in    │
 │ this system that is physically connected to the network that should be     │
 │ inspected, enable promiscuous mode later on and make sure that the         │
 │ network traffic is sent to this interface (either connected to a "port     │
 │ mirroring/spanning" port in a switch, to a hub, or to a tap).              │
 │                                                                            │
 │ You can configure multiple interfaces, just by adding more than one        │
 │ interface name separated by spaces. Each interface can have its own        │
 │ specific configuration.                                                    │
 │                                                                            │
 │ Interface(s) which Snort should listen on:                                 │
 │                                                                            │
 │ eth0______________________________________________________________________ │
 │                                                                            │
 │                                 <Ok>                                       │
 │                                                                            │
 └────────────────────────────────────────────────────────────────────────────┘


----8><----------------------------------------------------------------------
```

- Praleidžiu LAN potinklio konfigūravimą (spaudžiu `Esc`):

  https://user-images.githubusercontent.com/74717106/124731359-d32cbb80-df1a-11eb-8e70-5b7b41236e40.png

```
----8><-------------------------------------------------------------------------
Package configuration


 ┌────────────────────────────┤ Configuring snort ├────────────────────────────┐
 │ Please use the CIDR form - for example, 192.168.1.0/24 for a block of       │
 │ 256 addresses or 192.168.1.42/32 for just one. Multiple values should be    │
 │ comma-separated (without spaces).                                           │
 │                                                                             │
 │ Please note that if Snort is configured to use multiple interfaces, it      │
 │ will use this value as the HOME_NET definition for all of them.             │
 │                                                                             │
 │ Address range for the local network:                                        │
 │                                                                             │
 │ 192.168.0.0/16___________________________________________________________   │
 │                                                                             │
 │                                  <Ok>                                       │
 │                                                                             │
 └─────────────────────────────────────────────────────────────────────────────┘


----8><-------------------------------------------------------------------------
```

- Tęsiu paketinį instaliavimą:

```
Selecting previously unselected package snort-common-libraries.
(Reading database ... 198337 files and directories currently installed.)
Preparing to unpack .../snort-common-libraries_2.9.7.0-5build1_amd64.deb ...
Unpacking snort-common-libraries (2.9.7.0-5build1) ...
Selecting previously unselected package snort-rules-default.
Preparing to unpack .../snort-rules-default_2.9.7.0-5build1_all.deb ...
Unpacking snort-rules-default (2.9.7.0-5build1) ...
Selecting previously unselected package snort-common.
Preparing to unpack .../snort-common_2.9.7.0-5build1_all.deb ...
Unpacking snort-common (2.9.7.0-5build1) ...
Selecting previously unselected package snort.
Preparing to unpack .../snort_2.9.7.0-5build1_amd64.deb ...
Unpacking snort (2.9.7.0-5build1) ...
Selecting previously unselected package oinkmaster.
Preparing to unpack .../oinkmaster_2.0-4_all.deb ...
Unpacking oinkmaster (2.0-4) ...
Setting up oinkmaster (2.0-4) ...
Setting up snort-common (2.9.7.0-5build1) ...
Setting up snort-rules-default (2.9.7.0-5build1) ...
Setting up snort-common-libraries (2.9.7.0-5build1) ...
Setting up snort (2.9.7.0-5build1) ...
```

- Patvirtinu, kad Snort stebės tinklo sąsają `enp0s8` :

```
----8><----------------------------------------------------------------------
Package configuration


 ┌───────────────────────────┤ Configuring snort ├──────────────────────────┐
 │ This value is usually "eth0", but this may be inappropriate in some      │
 │ network environments; for a dialup connection "ppp0" might be more       │
 │ appropriate (see the output of "/sbin/ifconfig").                        │
 │                                                                          │
 │ Typically, this is the same interface as the "default route" is on. You  │
 │ can determine which interface is used for this by running "/sbin/route   │
 │ -n" (look for "0.0.0.0").                                                │
 │                                                                          │
 │ It is also not uncommon to use an interface with no IP address           │
 │ configured in promiscuous mode. For such cases, select the interface in  │
 │ this system that is physically connected to the network that should be   │
 │ inspected, enable promiscuous mode later on and make sure that the       │
 │ network traffic is sent to this interface (either connected to a "port   │
 │ mirroring/spanning" port in a switch, to a hub, or to a tap).            │
 │                                                                          │
 │ You can configure multiple interfaces, just by adding more than one      │
 │ interface name separated by spaces. Each interface can have its own      │
 │ specific configuration.                                                  │
 │                                                                          │
 │ Interface(s) which Snort should listen on:                               │
 │                                                                          │
 │ enp0s8__________________________________________________________________ │
 │                                                                          │
 │                                 <Ok>                                     │
 │                                                                          │
 └──────────────────────────────────────────────────────────────────────────┘

----8><----------------------------------------------------------------------
```

- Paketinis diegimas baigėsi:

```
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for systemd (245.4-4ubuntu3.7) ...
```

- Tikrinu. Pasileido automatinė Snort *systemd* paslauga:

```
osboxes@ldvm1:/usr/local/src/snort-2.9.18$ systemctl status snort
● snort.service - LSB: Lightweight network intrusion detection system
     Loaded: loaded (/etc/init.d/snort; generated)
     Active: active (running) since Wed 2021-07-07 12:24:04 EEST; 56s ago
       Docs: man:systemd-sysv-generator(8)
      Tasks: 2 (limit: 1105)
     Memory: 142.2M
     CGroup: /system.slice/snort.service
             └─66919 /usr/sbin/snort -m 027 -D -d -l /var/log/snort -u snort -g
snort -c /etc/snort/snort.conf -S HOME_NET=[192.168.0.0/16] -i enp0s8

Jul 07 12:24:04 ldvm1 snort[66919]:            Preprocessor Object: SF_IMAP  Version
1.0  <Build 1>
Jul 07 12:24:04 ldvm1 snort[66919]:            Preprocessor Object: SF_POP  Version
1.0  <Build 1>
Jul 07 12:24:04 ldvm1 snort[66919]:            Preprocessor Object: SF_DNP3  Version
1.1  <Build 1>
Jul 07 12:24:04 ldvm1 snort[66919]:            Preprocessor Object: SF_SDF  Version
1.1  <Build 1>
Jul 07 12:24:04 ldvm1 snort[66919]:            Preprocessor Object: SF_SSH  Version
1.1  <Build 3>
Jul 07 12:24:04 ldvm1 snort[66919]:            Preprocessor Object: SF_SIP  Version
1.1  <Build 1>
Jul 07 12:24:04 ldvm1 snort[66919]:            Preprocessor Object: SF_REPUTATION
Version 1.1  <Build 1>
Jul 07 12:24:04 ldvm1 snort[66919]:            Preprocessor Object: SF_DNS  Version
1.1  <Build 4>
Jul 07 12:24:04 ldvm1 snort[66919]:            Preprocessor Object: SF_DCERPC2
Version 1.0  <Build 3>
Jul 07 12:24:04 ldvm1 snort[66919]: Commencing packet processing (pid=66919)
```

- Sustabdau Snort automatinę *systemd* paslaugą ir ją uždraudžiu:

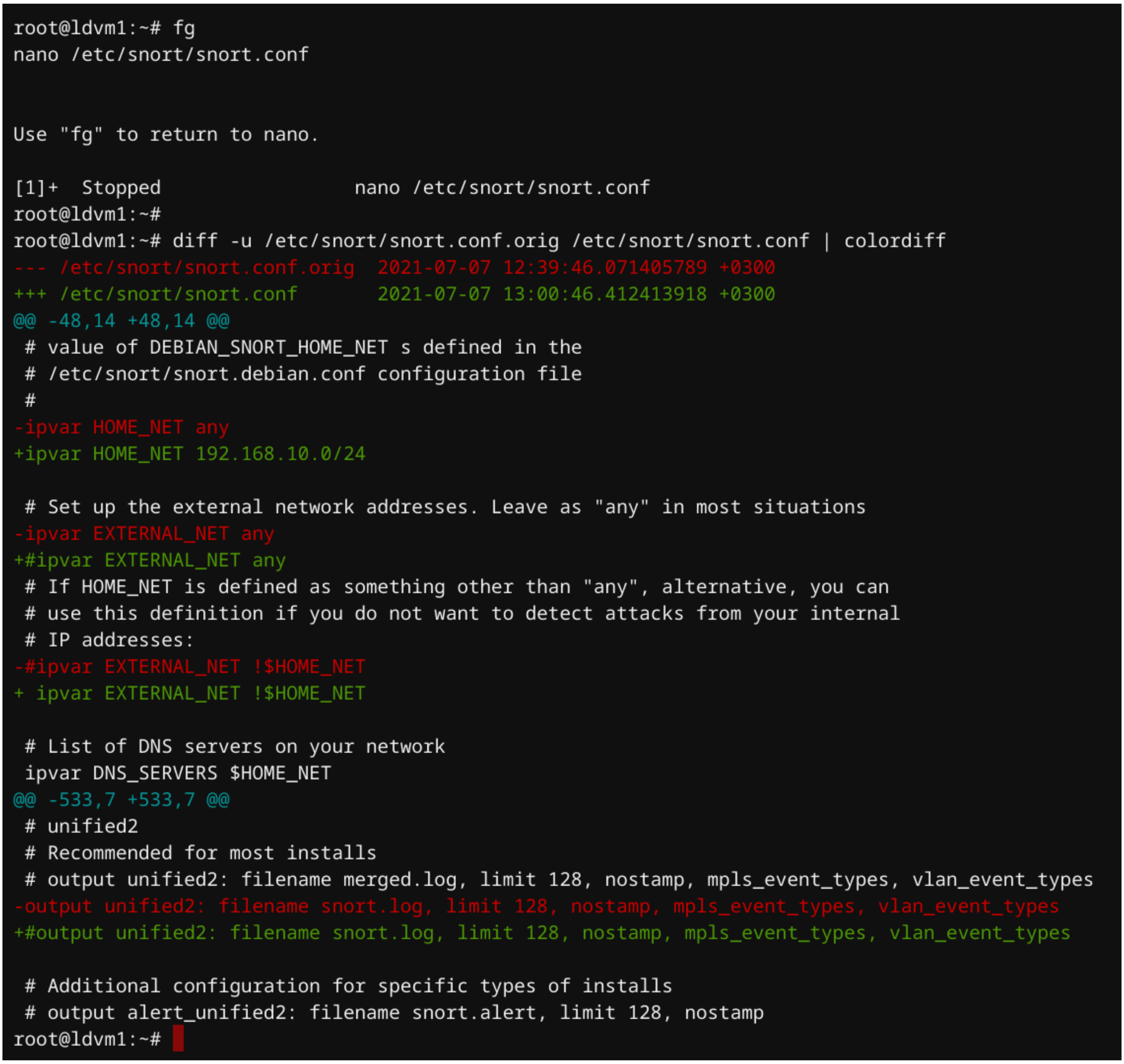
```
osboxes@ldvm1:/usr/local/src/snort-2.9.18$ sudo systemctl stop snort

osboxes@ldvm1:/usr/local/src/snort-2.9.18$ sudo systemctl disable snort
snort.service is not a native service, redirecting to systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install disable snort

osboxes@ldvm1:/usr/local/src/snort-2.9.18$ systemctl status snort
● snort.service - LSB: Lightweight network intrusion detection system
     Loaded: loaded (/etc/init.d/snort; generated)
     Active: inactive (dead)
       Docs: man:systemd-sysv-generator(8)

Jul 07 12:27:13 ldvm1 snort[66919]:
===============================================================================
Jul 07 12:27:13 ldvm1 snort[66919]:
===============================================================================
Jul 07 12:27:13 ldvm1 snort[66919]: SIP Preprocessor Statistics
Jul 07 12:27:13 ldvm1 snort[66919]:   Total sessions: 0
Jul 07 12:27:13 ldvm1 snort[66919]:
===============================================================================
Jul 07 12:27:13 ldvm1 snort[66919]: Could not remove pid file
/var/run//snort_enp0s8.pid: Permission denied
Jul 07 12:27:13 ldvm1 snort[66919]: Snort exiting
Jul 07 12:27:13 ldvm1 snort[67661]:    ...done.
Jul 07 12:27:13 ldvm1 systemd[1]: snort.service: Succeeded.
Jul 07 12:27:13 ldvm1 systemd[1]: Stopped LSB: Lightweight network intrusion
detection system.
```

- Palyginu Snort versijų skirtumą:

```
osboxes@ldvm1:/usr/local/src/snort-2.9.18$ snort -V 2>&1 | tee ~/debug/13.snort-iš-pkg.txt

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.7.0 GRE (Build 149)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.9.1 (with TPACKET_V3)
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.2.11

osboxes@ldvm1:/usr/local/src/snort-2.9.18$ diff -u ~/debug/{12,13}*.txt
--- "/home/osboxes/debug/12.snort-i\305\241-src.txt"    2021-07-07 12:10:10.174286960 +0300
+++ "/home/osboxes/debug/13.snort-i\305\241-pkg.txt"    2021-07-07 12:30:59.455117888 +0300
@@ -1,8 +1,8 @@

    ,,_     -*> Snort! <*-
-  o"  )~   Version 2.9.18 GRE (Build 169)
+  o"  )~   Version 2.9.7.0 GRE (Build 149)
    ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
-           Copyright (C) 2014-2021 Cisco and/or its affiliates. All rights reserved.
+           Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
            Copyright (C) 1998-2013 Sourcefire, Inc., et al.
            Using libpcap version 1.9.1 (with TPACKET_V3)
            Using PCRE version: 8.39 2016-06-14
```

- Vėl sukonfigūruoju `snort.conf` ir palyginu su paketine konfigūracija:

```
root@ldvm1:~# nano /etc/snort/snort.conf


Use "fg" to return to nano.

[1]+  Stopped                 nano /etc/snort/snort.conf

root@ldvm1:~# diff -u /etc/snort/snort.conf.orig /etc/snort/snort.conf | colordiff
--- /etc/snort/snort.conf.orig  2021-07-07 12:39:46.071405789 +0300
+++ /etc/snort/snort.conf       2021-07-07 13:00:46.412413918 +0300
@@ -48,14 +48,14 @@
 # value of DEBIAN_SNORT_HOME_NET s defined in the
 # /etc/snort/snort.debian.conf configuration file
 #
-ipvar HOME_NET any
+ipvar HOME_NET 192.168.10.0/24

 # Set up the external network addresses. Leave as "any" in most situations
-ipvar EXTERNAL_NET any
+#ipvar EXTERNAL_NET any
 # If HOME_NET is defined as something other than "any", alternative, you can
 # use this definition if you do not want to detect attacks from your internal
 # IP addresses:
-#ipvar EXTERNAL_NET !$HOME_NET
+ ipvar EXTERNAL_NET !$HOME_NET

 # List of DNS servers on your network
 ipvar DNS_SERVERS $HOME_NET
@@ -533,7 +533,7 @@
 # unified2
 # Recommended for most installs
 # output unified2: filename merged.log, limit 128, nostamp, mpls_event_types,
vlan_event_types
-output unified2: filename snort.log, limit 128, nostamp, mpls_event_types,
vlan_event_types
+#output unified2: filename snort.log, limit 128, nostamp, mpls_event_types,
vlan_event_types

 # Additional configuration for specific types of installs
 # output alert_unified2: filename snort.alert, limit 128, nostamp
```



```
root@ldvm1:~# fg
nano /etc/snort/snort.conf


Use "fg" to return to nano.

[1]+  Stopped                 nano /etc/snort/snort.conf
root@ldvm1:~#
root@ldvm1:~# diff -u /etc/snort/snort.conf.orig /etc/snort/snort.conf | colordiff
--- /etc/snort/snort.conf.orig  2021-07-07 12:39:46.071405789 +0300
+++ /etc/snort/snort.conf       2021-07-07 13:00:46.412413918 +0300
@@ -48,14 +48,14 @@
 # value of DEBIAN_SNORT_HOME_NET s defined in the
 # /etc/snort/snort.debian.conf configuration file
 #
-ipvar HOME_NET any
+ipvar HOME_NET 192.168.10.0/24

 # Set up the external network addresses. Leave as "any" in most situations
-ipvar EXTERNAL_NET any
+#ipvar EXTERNAL_NET any
 # If HOME_NET is defined as something other than "any", alternative, you can
 # use this definition if you do not want to detect attacks from your internal
 # IP addresses:
-#ipvar EXTERNAL_NET !$HOME_NET
+ ipvar EXTERNAL_NET !$HOME_NET

 # List of DNS servers on your network
 ipvar DNS_SERVERS $HOME_NET
@@ -533,7 +533,7 @@
 # unified2
 # Recommended for most installs
 # output unified2: filename merged.log, limit 128, nostamp, mpls_event_types, vlan_event_types
-output unified2: filename snort.log, limit 128, nostamp, mpls_event_types, vlan_event_types
+#output unified2: filename snort.log, limit 128, nostamp, mpls_event_types, vlan_event_types

 # Additional configuration for specific types of installs
 # output alert_unified2: filename snort.alert, limit 128, nostamp
root@ldvm1:~#
```

- Galiausiai startuoju senesnę Snort paslaugą (v2.9.7):

```
root@ldvm1:~# snort -u snort -g snort -c /etc/snort/snort.conf -i enp0s8
Running in IDS mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/snort.conf"
PortVar 'HTTP_PORTS' defined :  [ 80:81 311 383 591 593 901 1220 1414 1741 1830 2301
2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000
8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899
9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555 ]
PortVar 'SHELLCODE_PORTS' defined :  [ 0:79 81:65535 ]
PortVar 'ORACLE_PORTS' defined :  [ 1024:65535 ]
PortVar 'SSH_PORTS' defined :  [ 22 ]
PortVar 'FTP_PORTS' defined :  [ 21 2100 3535 ]
PortVar 'SIP_PORTS' defined :  [ 5060:5061 5600 ]
PortVar 'FILE_DATA_PORTS' defined :  [ 80:81 110 143 311 383 591 593 901 1220 1414
1741 1830 2301 2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510
7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300
8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002
55555 ]
PortVar 'GTP_PORTS' defined :  [ 2123 2152 3386 ]
Detection:
   Search-Method = AC-Full-Q
    Split Any/Any group = enabled
    Search-Method-Optimizations = enabled
    Maximum pattern length = 20
Tagged Packet Limit: 256
Loading dynamic engine /usr/lib/snort_dynamicengine/libsf_engine.so... done
Loading all dynamic detection libs from /usr/lib/snort_dynamicrules...
WARNING: No dynamic libraries found in directory /usr/lib/snort_dynamicrules.
  Finished Loading all dynamic detection libs from /usr/lib/snort_dynamicrules
Loading all dynamic preprocessor libs from /usr/lib/snort_dynamicpreprocessor/...
  Loading dynamic preprocessor library
/usr/lib/snort_dynamicpreprocessor//libsf_dce2_preproc.so... done
  Loading dynamic preprocessor library
/usr/lib/snort_dynamicpreprocessor//libsf_dns_preproc.so... done
  Loading dynamic preprocessor library
/usr/lib/snort_dynamicpreprocessor//libsf_reputation_preproc.so... done
  Loading dynamic preprocessor library
/usr/lib/snort_dynamicpreprocessor//libsf_sip_preproc.so... done
  Loading dynamic preprocessor library
/usr/lib/snort_dynamicpreprocessor//libsf_ssh_preproc.so... done
  Loading dynamic preprocessor library
/usr/lib/snort_dynamicpreprocessor//libsf_sdf_preproc.so... done
  Loading dynamic preprocessor library
/usr/lib/snort_dynamicpreprocessor//libsf_dnp3_preproc.so... done
  Loading dynamic preprocessor library
/usr/lib/snort_dynamicpreprocessor//libsf_pop_preproc.so... done
  Loading dynamic preprocessor library
/usr/lib/snort_dynamicpreprocessor//libsf_imap_preproc.so... done
  Loading dynamic preprocessor library
/usr/lib/snort_dynamicpreprocessor//libsf_modbus_preproc.so... done
  Loading dynamic preprocessor library
/usr/lib/snort_dynamicpreprocessor//libsf_gtp_preproc.so... done
```

```
  Loading dynamic preprocessor library
/usr/lib/snort_dynamicpreprocessor//libsf_ftptelnet_preproc.so... done
  Loading dynamic preprocessor library
/usr/lib/snort_dynamicpreprocessor//libsf_ssl_preproc.so... done
  Loading dynamic preprocessor library
/usr/lib/snort_dynamicpreprocessor//libsf_smtp_preproc.so... done
  Finished Loading all dynamic preprocessor libs from
/usr/lib/snort_dynamicpreprocessor/
Log directory = /var/log/snort
WARNING: ip4 normalizations disabled because not inline.
WARNING: tcp normalizations disabled because not inline.
WARNING: icmp4 normalizations disabled because not inline.
WARNING: ip6 normalizations disabled because not inline.
WARNING: icmp6 normalizations disabled because not inline.
Frag3 global config:
    Max frags: 65536
    Fragment memory cap: 4194304 bytes
Frag3 engine config:
    Bound Address: default
    Target-based policy: WINDOWS
    Fragment timeout: 180 seconds
    Fragment min_ttl:   1
    Fragment Anomalies: Alert
    Overlap Limit:     10
    Min fragment Length:     100
      Max Expected Streams: 768
Stream global config:
    Track TCP sessions: ACTIVE
    Max TCP sessions: 262144
    TCP cache pruning timeout: 30 seconds
    TCP cache nominal timeout: 3600 seconds
    Memcap (for reassembly packet storage): 8388608
    Track UDP sessions: ACTIVE
    Max UDP sessions: 131072
    UDP cache pruning timeout: 30 seconds
    UDP cache nominal timeout: 180 seconds
    Track ICMP sessions: INACTIVE
    Track IP sessions: INACTIVE
    Log info if session memory consumption exceeds 1048576
    Send up to 2 active responses
    Wait at least 5 seconds between responses
    Protocol Aware Flushing: ACTIVE
        Maximum Flush Point: 16000
Stream TCP Policy config:
    Bound Address: default
    Reassembly Policy: WINDOWS
    Timeout: 180 seconds
    Limit on TCP Overlaps: 10
    Maximum number of bytes to queue per session: 1048576
    Maximum number of segs to queue per session: 2621
    Options:
        Require 3-Way Handshake: YES
        3-Way Handshake Timeout: 180
        Detect Anomalies: YES
    Reassembly Ports:
      21 client (Footprint)
      22 client (Footprint)
      23 client (Footprint)
      25 client (Footprint)
      42 client (Footprint)
      53 client (Footprint)
      79 client (Footprint)
      80 client (Footprint) server (Footprint)
      81 client (Footprint) server (Footprint)
      109 client (Footprint)
      110 client (Footprint)
      111 client (Footprint)
      113 client (Footprint)
      119 client (Footprint)
      135 client (Footprint)
      136 client (Footprint)
      137 client (Footprint)
      139 client (Footprint)
      143 client (Footprint)
      161 client (Footprint)
      additional ports configured but not printed.
Stream UDP Policy config:
    Timeout: 180 seconds
HttpInspect Config:
    GLOBAL CONFIG
      Detect Proxy Usage:       NO
      IIS Unicode Map Filename: /etc/snort/unicode.map
      IIS Unicode Map Codepage: 1252
      Memcap used for logging URI and Hostname: 150994944
      Max Gzip Memory: 104857600
      Max Gzip Sessions: 201649
      Gzip Compress Depth: 65535
      Gzip Decompress Depth: 65535
    DEFAULT SERVER CONFIG:
      Server profile: All
      Ports (PAF): 80 81 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037
3128 3702 4343 4848 5250 6988 7000 7001 7144 7145 7510 7777 7779 8000 8008 8014 8028
8080 8085 8088 8090 8118 8123 8180 8181 8243 8280 8300 8800 8888 8899 9000 9060 9080
9090 9091 9443 9999 11371 34443 34444 41080 50002 55555
      Server Flow Depth: 0
      Client Flow Depth: 0
      Max Chunk Length: 500000
      Small Chunk Length Evasion: chunk size <= 10, threshold >= 5 times
      Max Header Field Length: 750
      Max Number Header Fields: 100
      Max Number of WhiteSpaces allowed with header folding: 200
      Inspect Pipeline Requests: YES
      URI Discovery Strict Mode: NO
      Allow Proxy Usage: NO
      Disable Alerting: NO
      Oversize Dir Length: 500
      Only inspect URI: NO
      Normalize HTTP Headers: NO
      Inspect HTTP Cookies: YES
      Inspect HTTP Responses: YES
      Extract Gzip from responses: YES
      Decompress response files:
      Unlimited decompression of gzip data from responses: YES
      Normalize Javascripts in HTTP Responses: YES
      Max Number of WhiteSpaces allowed with Javascript Obfuscation in HTTP
responses: 200
      Normalize HTTP Cookies: NO
      Enable XFF and True Client IP: NO
      Log HTTP URI data: NO
      Log HTTP Hostname data: NO
      Extended ASCII code support in URI: NO
      Ascii: YES alert: NO
      Double Decoding: YES alert: NO
      %U Encoding: YES alert: YES
      Bare Byte: YES alert: NO
      UTF 8: YES alert: NO
      IIS Unicode: YES alert: NO
      Multiple Slash: YES alert: NO
      IIS Backslash: YES alert: NO
      Directory Traversal: YES alert: NO
      Web Root Traversal: YES alert: NO
      Apache WhiteSpace: YES alert: NO
      IIS Delimiter: YES alert: NO
      IIS Unicode Map: GLOBAL IIS UNICODE MAP CONFIG
      Non-RFC Compliant Characters: 0x00 0x01 0x02 0x03 0x04 0x05 0x06 0x07
      Whitespace Characters: 0x09 0x0b 0x0c 0x0d
rpc_decode arguments:
    Ports to decode RPC on: 111 32770 32771 32772 32773 32774 32775 32776 32777
32778 32779
    alert_fragments: INACTIVE
    alert_large_fragments: INACTIVE
    alert_incomplete: INACTIVE
    alert_multiple_requests: INACTIVE
FTPTelnet Config:
    GLOBAL CONFIG
      Inspection Type: stateful
      Check for Encrypted Traffic: YES alert: NO
      Continue to check encrypted data: YES
    TELNET CONFIG:
      Ports: 23
      Are You There Threshold: 20
      Normalize: YES
      Detect Anomalies: YES
    FTP CONFIG:
      FTP Server: default
        Ports (PAF): 21 2100 3535
        Check for Telnet Cmds: YES alert: YES
        Ignore Telnet Cmd Operations: YES alert: YES
        Ignore open data channels: NO
      FTP Client: default
        Check for Bounce Attacks: YES alert: YES
        Check for Telnet Cmds: YES alert: YES
        Ignore Telnet Cmd Operations: YES alert: YES
        Max Response Length: 256
SMTP Config:
    Ports: 25 465 587 691
    Inspection Type: Stateful
    Normalize: ATRN AUTH BDAT DATA DEBUG EHLO EMAL ESAM ESND ESOM ETRN EVFY EXPN
HELO HELP IDENT MAIL NOOP ONEX QUEU QUIT RCPT RSET SAML SEND STARTTLS SOML TICK TIME
TURN TURNME VERB VRFY X-EXPS XADR XAUTH XCIR XEXCH50 XGEN XLICENSE X-LINK2STATE XQUE
XSTA XTRN XUSR CHUNKING X-ADAT X-DRCP X-ERCP X-EXCH50
```

```
    Ignore Data: No
    Ignore TLS Data: No
    Ignore SMTP Alerts: No
    Max Command Line Length: 512
    Max Specific Command Line Length:
       ATRN:255 AUTH:246 BDAT:255 DATA:246 DEBUG:255
       EHLO:500 EMAL:255 ESAM:255 ESND:255 ESOM:255
       ETRN:246 EVFY:255 EXPN:255 HELO:500 HELP:500
       IDENT:255 MAIL:260 NOOP:255 ONEX:246 QUEU:246
       QUIT:246 RCPT:300 RSET:246 SAML:246 SEND:246
       SIZE:255 STARTTLS:246 SOML:246 TICK:246 TIME:246
       TURN:246 TURNME:246 VERB:246 VRFY:255 X-EXPS:246
       XADR:246 XAUTH:246 XCIR:246 XEXCH50:246 XGEN:246
       XLICENSE:246 X-LINK2STATE:246 XQUE:246 XSTA:246 XTRN:246
       XUSR:246
    Max Header Line Length: 1000
    Max Response Line Length: 512
    X-Link2State Alert: Yes
    Drop on X-Link2State Alert: No
    Alert on commands: None
    Alert on unknown commands: No
    SMTP Memcap: 838860
    MIME Max Mem: 838860
    Base64 Decoding: Enabled
    Base64 Decoding Depth: Unlimited
    Quoted-Printable Decoding: Enabled
    Quoted-Printable Decoding Depth: Unlimited
    Unix-to-Unix Decoding: Enabled
    Unix-to-Unix Decoding Depth: Unlimited
    Non-Encoded MIME attachment Extraction: Enabled
    Non-Encoded MIME attachment Extraction Depth: Unlimited
    Log Attachment filename: Enabled
    Log MAIL FROM Address: Enabled
    Log RCPT TO Addresses: Enabled
    Log Email Headers: Enabled
    Email Hdrs Log Depth: 1464
SSH config:
    Autodetection: ENABLED
    Challenge-Response Overflow Alert: ENABLED
    SSH1 CRC32 Alert: ENABLED
    Server Version String Overflow Alert: ENABLED
    Protocol Mismatch Alert: ENABLED
    Bad Message Direction Alert: DISABLED
    Bad Payload Size Alert: DISABLED
    Unrecognized Version Alert: DISABLED
    Max Encrypted Packets: 20
    Max Server Version String Length: 100
    MaxClientBytes: 19600 (Default)
    Ports:
        22
DCE/RPC 2 Preprocessor Configuration
  Global Configuration
    DCE/RPC Defragmentation: Enabled
    Memcap: 102400 KB
    Events: co
    SMB Fingerprint policy: Disabled
  Server Default Configuration
```

```
    Policy: WinXP
    Detect ports (PAF)
      SMB: 139 445
      TCP: 135
      UDP: 135
      RPC over HTTP server: 593
      RPC over HTTP proxy: None
    Autodetect ports (PAF)
      SMB: None
      TCP: 1025-65535
      UDP: 1025-65535
      RPC over HTTP server: 1025-65535
      RPC over HTTP proxy: None
    Invalid SMB shares: C$ D$ ADMIN$
    Maximum SMB command chaining: 3 commands
    SMB file inspection: Disabled
DNS config:
    DNS Client rdata txt Overflow Alert: ACTIVE
    Obsolete DNS RR Types Alert: INACTIVE
    Experimental DNS RR Types Alert: INACTIVE
    Ports: 53
SSLPP config:
    Encrypted packets: not inspected
    Ports:
      443      465      563      636      989
      992      993      994      995     7801
     7802     7900     7901     7902     7903
     7904     7905     7906     7907     7908
     7909     7910     7911     7912     7913
     7914     7915     7916     7917     7918
     7919     7920
    Server side data is trusted
    Maximum SSL Heartbeat length: 0
Sensitive Data preprocessor config:
    Global Alert Threshold: 25
    Masked Output: DISABLED
SIP config:
    Max number of sessions: 40000
    Max number of dialogs in a session: 4 (Default)
    Status: ENABLED
    Ignore media channel: DISABLED
    Max URI length: 512
    Max Call ID length: 80
    Max Request name length: 20 (Default)
    Max From length: 256 (Default)
    Max To length: 256 (Default)
    Max Via length: 1024 (Default)
    Max Contact length: 512
    Max Content length: 2048
    Ports:
        5060    5061    5600
    Methods:
          invite cancel ack bye register options refer subscribe update join info
message notify benotify do qauth sprack publish service unsubscribe prack
IMAP Config:
    Ports: 143
    IMAP Memcap: 838860
    MIME Max Mem: 838860
    Base64 Decoding: Enabled
    Base64 Decoding Depth: Unlimited
    Quoted-Printable Decoding: Enabled
    Quoted-Printable Decoding Depth: Unlimited
    Unix-to-Unix Decoding: Enabled
    Unix-to-Unix Decoding Depth: Unlimited
    Non-Encoded MIME attachment Extraction: Enabled
    Non-Encoded MIME attachment Extraction Depth: Unlimited
POP Config:
    Ports: 110
    POP Memcap: 838860
    MIME Max Mem: 838860
    Base64 Decoding: Enabled
    Base64 Decoding Depth: Unlimited
    Quoted-Printable Decoding: Enabled
    Quoted-Printable Decoding Depth: Unlimited
    Unix-to-Unix Decoding: Enabled
    Unix-to-Unix Decoding Depth: Unlimited
    Non-Encoded MIME attachment Extraction: Enabled
    Non-Encoded MIME attachment Extraction Depth: Unlimited
Modbus config:
    Ports:
        502
DNP3 config:
    Memcap: 262144
    Check Link-Layer CRCs: ENABLED
    Ports:
        20000

+++++++++++++++++++++++++++++++++++++++++++++++++++
Initializing rule chains...
WARNING: /etc/snort/rules/chat.rules(33) threshold (in rule) is deprecated; use
detection_filter instead.

WARNING: /etc/snort/rules/telnet.rules(35) GID 1 SID 719 in rule duplicates previous
rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-sql-injection.rules(6) GID 1 SID 100000106 in
rule duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-sql-injection.rules(7) GID 1 SID 100000107 in
rule duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-sql-injection.rules(8) GID 1 SID 100000108 in
rule duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-sql-injection.rules(9) GID 1 SID 100000109 in
rule duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-sql-injection.rules(11) GID 1 SID 100000192 in
rule duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-sql-injection.rules(12) GID 1 SID 100000193 in
rule duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-sql-injection.rules(13) GID 1 SID 100000194 in
```

```
rule duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-sql-injection.rules(14) GID 1 SID 100000690 in
rule duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-sql-injection.rules(15) GID 1 SID 100000691 in
rule duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-client.rules(6) GID 1 SID 100000118 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-client.rules(7) GID 1 SID 100000119 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-client.rules(9) GID 1 SID 100000228 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-client.rules(14) GID 1 SID 100000284 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-client.rules(16) GID 1 SID 100000447 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-client.rules(18) GID 1 SID 100000692 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-client.rules(20) GID 1 SID 100000693 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-client.rules(23) GID 1 SID 100000864 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-iis.rules(7) GID 1 SID 100000138 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-iis.rules(8) GID 1 SID 100000139 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-iis.rules(9) GID 1 SID 100000173 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-iis.rules(10) GID 1 SID 100000174 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(6) GID 1 SID 100000121 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(7) GID 1 SID 100000122 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(8) GID 1 SID 100000129 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(9) GID 1 SID 100000130 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(10) GID 1 SID 100000131 in rule
```

```
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(12) GID 1 SID 100000132 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(13) GID 1 SID 100000133 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(14) GID 1 SID 100000140 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(15) GID 1 SID 100000141 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(16) GID 1 SID 100000142 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(17) GID 1 SID 100000143 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(18) GID 1 SID 100000144 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(19) GID 1 SID 100000145 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(20) GID 1 SID 100000146 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(22) GID 1 SID 100000148 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(23) GID 1 SID 100000149 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(24) GID 1 SID 100000150 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(25) GID 1 SID 100000177 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(26) GID 1 SID 100000178 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(27) GID 1 SID 100000179 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(28) GID 1 SID 100000184 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(29) GID 1 SID 100000185 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(30) GID 1 SID 100000200 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(31) GID 1 SID 100000209 in rule
```

```
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(33) GID 1 SID 100000216 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(34) GID 1 SID 100000217 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(35) GID 1 SID 100000225 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(38) GID 1 SID 100000237 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(39) GID 1 SID 100000302 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(40) GID 1 SID 100000303 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(42) GID 1 SID 100000313 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(43) GID 1 SID 100000314 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(49) GID 1 SID 100000317 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(50) GID 1 SID 100000318 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(51) GID 1 SID 100000319 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(52) GID 1 SID 100000320 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(53) GID 1 SID 100000321 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(54) GID 1 SID 100000322 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(55) GID 1 SID 100000323 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(56) GID 1 SID 100000324 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(57) GID 1 SID 100000325 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(58) GID 1 SID 100000326 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(59) GID 1 SID 100000327 in rule
```

```
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(60) GID 1 SID 100000328 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(61) GID 1 SID 100000329 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(62) GID 1 SID 100000330 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(63) GID 1 SID 100000331 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(64) GID 1 SID 100000332 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(65) GID 1 SID 100000333 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(66) GID 1 SID 100000334 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(67) GID 1 SID 100000335 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(68) GID 1 SID 100000336 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(69) GID 1 SID 100000337 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(70) GID 1 SID 100000338 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(71) GID 1 SID 100000339 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(72) GID 1 SID 100000340 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(73) GID 1 SID 100000341 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(74) GID 1 SID 100000342 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(75) GID 1 SID 100000343 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(76) GID 1 SID 100000344 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(77) GID 1 SID 100000345 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(78) GID 1 SID 100000346 in rule
```

```
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(79) GID 1 SID 100000347 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(80) GID 1 SID 100000348 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(81) GID 1 SID 100000349 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(82) GID 1 SID 100000350 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(83) GID 1 SID 100000351 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(84) GID 1 SID 100000352 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(85) GID 1 SID 100000353 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(86) GID 1 SID 100000354 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(87) GID 1 SID 100000355 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(88) GID 1 SID 100000356 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(89) GID 1 SID 100000357 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(90) GID 1 SID 100000358 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(91) GID 1 SID 100000359 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(92) GID 1 SID 100000360 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(93) GID 1 SID 100000361 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(94) GID 1 SID 100000362 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(95) GID 1 SID 100000363 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(96) GID 1 SID 100000364 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(97) GID 1 SID 100000365 in rule
```

```
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(98) GID 1 SID 100000366 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(99) GID 1 SID 100000367 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(100) GID 1 SID 100000368 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(101) GID 1 SID 100000369 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(102) GID 1 SID 100000370 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(103) GID 1 SID 100000371 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(104) GID 1 SID 100000372 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(105) GID 1 SID 100000373 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(106) GID 1 SID 100000374 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(107) GID 1 SID 100000375 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(108) GID 1 SID 100000376 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(109) GID 1 SID 100000377 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(110) GID 1 SID 100000378 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(111) GID 1 SID 100000379 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(112) GID 1 SID 100000380 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(113) GID 1 SID 100000382 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(114) GID 1 SID 100000383 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(115) GID 1 SID 100000384 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(116) GID 1 SID 100000385 in rule
```

```
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(117) GID 1 SID 100000386 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(119) GID 1 SID 100000387 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(120) GID 1 SID 100000388 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(121) GID 1 SID 100000389 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(122) GID 1 SID 100000390 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(123) GID 1 SID 100000391 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(124) GID 1 SID 100000392 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(125) GID 1 SID 100000393 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(126) GID 1 SID 100000394 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(127) GID 1 SID 100000395 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(128) GID 1 SID 100000396 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(129) GID 1 SID 100000397 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(130) GID 1 SID 100000398 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(131) GID 1 SID 100000399 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(132) GID 1 SID 100000400 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(133) GID 1 SID 100000401 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(134) GID 1 SID 100000402 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(135) GID 1 SID 100000403 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(136) GID 1 SID 100000404 in rule
```

```
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(137) GID 1 SID 100000405 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(138) GID 1 SID 100000406 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(139) GID 1 SID 100000407 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(140) GID 1 SID 100000408 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(141) GID 1 SID 100000409 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(142) GID 1 SID 100000410 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(143) GID 1 SID 100000411 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(144) GID 1 SID 100000412 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(145) GID 1 SID 100000413 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(146) GID 1 SID 100000414 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(147) GID 1 SID 100000415 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(148) GID 1 SID 100000416 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(149) GID 1 SID 100000417 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(150) GID 1 SID 100000418 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(151) GID 1 SID 100000419 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(152) GID 1 SID 100000420 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(153) GID 1 SID 100000421 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(154) GID 1 SID 100000422 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(155) GID 1 SID 100000423 in rule
```

```
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(156) GID 1 SID 100000424 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(157) GID 1 SID 100000425 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(158) GID 1 SID 100000426 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(161) GID 1 SID 100000427 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(162) GID 1 SID 100000428 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(163) GID 1 SID 100000429 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(166) GID 1 SID 100000430 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(167) GID 1 SID 100000431 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(168) GID 1 SID 100000432 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(169) GID 1 SID 100000433 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(170) GID 1 SID 100000434 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(171) GID 1 SID 100000435 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(172) GID 1 SID 100000436 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(173) GID 1 SID 100000437 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(174) GID 1 SID 100000438 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(175) GID 1 SID 100000439 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(176) GID 1 SID 100000440 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(177) GID 1 SID 100000441 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(178) GID 1 SID 100000442 in rule
```

```
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(179) GID 1 SID 100000443 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(180) GID 1 SID 100000444 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(181) GID 1 SID 100000448 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(182) GID 1 SID 100000449 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(183) GID 1 SID 100000450 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(184) GID 1 SID 100000451 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(185) GID 1 SID 100000452 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(186) GID 1 SID 100000453 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(187) GID 1 SID 100000454 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(188) GID 1 SID 100000455 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(189) GID 1 SID 100000456 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(190) GID 1 SID 100000457 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(191) GID 1 SID 100000458 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(192) GID 1 SID 100000459 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(193) GID 1 SID 100000460 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(194) GID 1 SID 100000461 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(195) GID 1 SID 100000462 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(196) GID 1 SID 100000694 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(197) GID 1 SID 100000695 in rule
```

```
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(198) GID 1 SID 100000696 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(199) GID 1 SID 100000697 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(200) GID 1 SID 100000698 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(201) GID 1 SID 100000699 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(202) GID 1 SID 100000700 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(203) GID 1 SID 100000701 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(204) GID 1 SID 100000702 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(207) GID 1 SID 100000890 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(208) GID 1 SID 100000891 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(211) GID 1 SID 100000895 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(212) GID 1 SID 100000896 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(213) GID 1 SID 100000897 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(214) GID 1 SID 100000898 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-misc.rules(215) GID 1 SID 100000899 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(6) GID 1 SID 100000151 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(7) GID 1 SID 100000186 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(8) GID 1 SID 100000187 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(9) GID 1 SID 100000188 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(10) GID 1 SID 100000195 in rule
```

```
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(11) GID 1 SID 100000201 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(12) GID 1 SID 100000202 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(13) GID 1 SID 100000203 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(14) GID 1 SID 100000204 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(15) GID 1 SID 100000205 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(16) GID 1 SID 100000206 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(17) GID 1 SID 100000211 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(18) GID 1 SID 100000212 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(19) GID 1 SID 100000213 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(20) GID 1 SID 100000214 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(21) GID 1 SID 100000218 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(22) GID 1 SID 100000220 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(23) GID 1 SID 100000221 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(24) GID 1 SID 100000285 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(25) GID 1 SID 100000286 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(26) GID 1 SID 100000287 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(27) GID 1 SID 100000288 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(28) GID 1 SID 100000289 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(29) GID 1 SID 100000290 in rule
```

```
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(30) GID 1 SID 100000291 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(31) GID 1 SID 100000292 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(32) GID 1 SID 100000293 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(33) GID 1 SID 100000294 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(34) GID 1 SID 100000295 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(35) GID 1 SID 100000296 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(36) GID 1 SID 100000297 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(37) GID 1 SID 100000298 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(38) GID 1 SID 100000299 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(39) GID 1 SID 100000300 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(40) GID 1 SID 100000304 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(41) GID 1 SID 100000305 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(42) GID 1 SID 100000306 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(43) GID 1 SID 100000307 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(44) GID 1 SID 100000308 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(45) GID 1 SID 100000309 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(46) GID 1 SID 100000445 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(48) GID 1 SID 100000463 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(49) GID 1 SID 100000464 in rule
```

```
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(50) GID 1 SID 100000465 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(51) GID 1 SID 100000466 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(52) GID 1 SID 100000467 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(53) GID 1 SID 100000468 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(54) GID 1 SID 100000469 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(55) GID 1 SID 100000470 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(56) GID 1 SID 100000471 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(57) GID 1 SID 100000472 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(58) GID 1 SID 100000473 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(59) GID 1 SID 100000474 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(60) GID 1 SID 100000475 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(61) GID 1 SID 100000476 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(62) GID 1 SID 100000477 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(63) GID 1 SID 100000478 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(64) GID 1 SID 100000479 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(65) GID 1 SID 100000480 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(66) GID 1 SID 100000481 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(67) GID 1 SID 100000482 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(68) GID 1 SID 100000483 in rule
```

```
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(69) GID 1 SID 100000484 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(70) GID 1 SID 100000485 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(71) GID 1 SID 100000486 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(72) GID 1 SID 100000487 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(73) GID 1 SID 100000488 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(74) GID 1 SID 100000489 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(75) GID 1 SID 100000490 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(76) GID 1 SID 100000491 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(77) GID 1 SID 100000492 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(78) GID 1 SID 100000493 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(79) GID 1 SID 100000494 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(80) GID 1 SID 100000495 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(81) GID 1 SID 100000496 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(82) GID 1 SID 100000497 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(83) GID 1 SID 100000498 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(84) GID 1 SID 100000499 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(85) GID 1 SID 100000500 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(86) GID 1 SID 100000501 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(87) GID 1 SID 100000502 in rule
```

```
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(88) GID 1 SID 100000503 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(89) GID 1 SID 100000504 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(90) GID 1 SID 100000505 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(91) GID 1 SID 100000506 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(92) GID 1 SID 100000507 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(93) GID 1 SID 100000508 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(94) GID 1 SID 100000509 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(95) GID 1 SID 100000510 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(96) GID 1 SID 100000511 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(97) GID 1 SID 100000512 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(98) GID 1 SID 100000513 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(99) GID 1 SID 100000514 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(100) GID 1 SID 100000515 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(101) GID 1 SID 100000516 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(102) GID 1 SID 100000517 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(103) GID 1 SID 100000518 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(104) GID 1 SID 100000519 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(105) GID 1 SID 100000520 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(106) GID 1 SID 100000521 in rule
```

```
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(107) GID 1 SID 100000522 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(108) GID 1 SID 100000523 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(109) GID 1 SID 100000524 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(110) GID 1 SID 100000525 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(111) GID 1 SID 100000526 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(112) GID 1 SID 100000527 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(113) GID 1 SID 100000528 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(114) GID 1 SID 100000529 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(115) GID 1 SID 100000530 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(116) GID 1 SID 100000531 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(117) GID 1 SID 100000532 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(118) GID 1 SID 100000533 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(119) GID 1 SID 100000534 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(120) GID 1 SID 100000535 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(121) GID 1 SID 100000536 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(122) GID 1 SID 100000537 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(123) GID 1 SID 100000538 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(124) GID 1 SID 100000539 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(125) GID 1 SID 100000540 in rule
```

```
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(126) GID 1 SID 100000541 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(127) GID 1 SID 100000542 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(128) GID 1 SID 100000543 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(129) GID 1 SID 100000544 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(130) GID 1 SID 100000545 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(131) GID 1 SID 100000546 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(132) GID 1 SID 100000547 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(133) GID 1 SID 100000548 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(134) GID 1 SID 100000549 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(135) GID 1 SID 100000550 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(136) GID 1 SID 100000551 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(137) GID 1 SID 100000552 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(138) GID 1 SID 100000553 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(139) GID 1 SID 100000554 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(140) GID 1 SID 100000555 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(141) GID 1 SID 100000556 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(142) GID 1 SID 100000557 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(143) GID 1 SID 100000558 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(144) GID 1 SID 100000559 in rule
```

```
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(145) GID 1 SID 100000560 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(146) GID 1 SID 100000561 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(147) GID 1 SID 100000562 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(148) GID 1 SID 100000563 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(149) GID 1 SID 100000564 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(150) GID 1 SID 100000565 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(151) GID 1 SID 100000566 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(152) GID 1 SID 100000567 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(153) GID 1 SID 100000568 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(154) GID 1 SID 100000569 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(155) GID 1 SID 100000570 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(156) GID 1 SID 100000571 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(157) GID 1 SID 100000572 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(158) GID 1 SID 100000573 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(159) GID 1 SID 100000574 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(160) GID 1 SID 100000575 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(161) GID 1 SID 100000576 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(162) GID 1 SID 100000577 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(163) GID 1 SID 100000578 in rule
```

```
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(164) GID 1 SID 100000579 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(165) GID 1 SID 100000580 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(166) GID 1 SID 100000581 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(167) GID 1 SID 100000582 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(168) GID 1 SID 100000583 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(169) GID 1 SID 100000584 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(170) GID 1 SID 100000585 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(171) GID 1 SID 100000586 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(172) GID 1 SID 100000587 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(173) GID 1 SID 100000588 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(174) GID 1 SID 100000589 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(175) GID 1 SID 100000590 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(176) GID 1 SID 100000591 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(177) GID 1 SID 100000592 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(178) GID 1 SID 100000593 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(179) GID 1 SID 100000594 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(180) GID 1 SID 100000595 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(181) GID 1 SID 100000596 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(182) GID 1 SID 100000597 in rule
```

```
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(183) GID 1 SID 100000598 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(184) GID 1 SID 100000599 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(185) GID 1 SID 100000600 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(186) GID 1 SID 100000601 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(187) GID 1 SID 100000602 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(188) GID 1 SID 100000603 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(189) GID 1 SID 100000604 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(190) GID 1 SID 100000605 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(191) GID 1 SID 100000606 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(192) GID 1 SID 100000607 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(193) GID 1 SID 100000608 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(194) GID 1 SID 100000609 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(195) GID 1 SID 100000610 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(196) GID 1 SID 100000611 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(197) GID 1 SID 100000612 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(198) GID 1 SID 100000613 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(199) GID 1 SID 100000614 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(200) GID 1 SID 100000615 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(201) GID 1 SID 100000616 in rule
```

```
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(202) GID 1 SID 100000617 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(203) GID 1 SID 100000618 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(204) GID 1 SID 100000619 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(205) GID 1 SID 100000620 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(206) GID 1 SID 100000621 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(207) GID 1 SID 100000622 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(208) GID 1 SID 100000623 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(209) GID 1 SID 100000624 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(210) GID 1 SID 100000625 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(211) GID 1 SID 100000626 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(212) GID 1 SID 100000627 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(213) GID 1 SID 100000628 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(214) GID 1 SID 100000629 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(215) GID 1 SID 100000630 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(216) GID 1 SID 100000631 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(217) GID 1 SID 100000632 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(218) GID 1 SID 100000633 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(219) GID 1 SID 100000634 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(220) GID 1 SID 100000635 in rule
```

```
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(221) GID 1 SID 100000636 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(222) GID 1 SID 100000637 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(223) GID 1 SID 100000638 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(224) GID 1 SID 100000639 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(225) GID 1 SID 100000640 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(226) GID 1 SID 100000641 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(227) GID 1 SID 100000642 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(228) GID 1 SID 100000643 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(229) GID 1 SID 100000644 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(230) GID 1 SID 100000645 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(231) GID 1 SID 100000646 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(232) GID 1 SID 100000647 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(233) GID 1 SID 100000648 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(234) GID 1 SID 100000649 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(235) GID 1 SID 100000650 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(236) GID 1 SID 100000651 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(237) GID 1 SID 100000652 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(238) GID 1 SID 100000653 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(239) GID 1 SID 100000654 in rule
```

```
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(240) GID 1 SID 100000655 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(241) GID 1 SID 100000656 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(242) GID 1 SID 100000657 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(243) GID 1 SID 100000658 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(244) GID 1 SID 100000659 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(245) GID 1 SID 100000660 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(246) GID 1 SID 100000661 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(247) GID 1 SID 100000662 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(248) GID 1 SID 100000663 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(249) GID 1 SID 100000664 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(250) GID 1 SID 100000665 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(251) GID 1 SID 100000666 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(252) GID 1 SID 100000667 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(253) GID 1 SID 100000668 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(254) GID 1 SID 100000669 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(255) GID 1 SID 100000670 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(256) GID 1 SID 100000671 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(257) GID 1 SID 100000672 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(258) GID 1 SID 100000673 in rule
```

```
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(259) GID 1 SID 100000674 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(260) GID 1 SID 100000675 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(261) GID 1 SID 100000676 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(262) GID 1 SID 100000677 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(263) GID 1 SID 100000678 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(264) GID 1 SID 100000679 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(265) GID 1 SID 100000680 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(266) GID 1 SID 100000681 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(267) GID 1 SID 100000682 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(268) GID 1 SID 100000683 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(270) GID 1 SID 100000703 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(271) GID 1 SID 100000704 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(272) GID 1 SID 100000705 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(273) GID 1 SID 100000706 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(274) GID 1 SID 100000707 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(275) GID 1 SID 100000708 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(276) GID 1 SID 100000709 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(277) GID 1 SID 100000710 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(278) GID 1 SID 100000711 in rule
```

```
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(279) GID 1 SID 100000712 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(280) GID 1 SID 100000713 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(281) GID 1 SID 100000714 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(282) GID 1 SID 100000715 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(283) GID 1 SID 100000716 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(284) GID 1 SID 100000717 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(285) GID 1 SID 100000718 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(286) GID 1 SID 100000719 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(287) GID 1 SID 100000720 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(288) GID 1 SID 100000721 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(289) GID 1 SID 100000722 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(290) GID 1 SID 100000723 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(291) GID 1 SID 100000724 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(292) GID 1 SID 100000725 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(293) GID 1 SID 100000726 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(294) GID 1 SID 100000727 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(295) GID 1 SID 100000728 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(296) GID 1 SID 100000729 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(297) GID 1 SID 100000730 in rule
```

```
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(298) GID 1 SID 100000731 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(299) GID 1 SID 100000732 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(300) GID 1 SID 100000733 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(301) GID 1 SID 100000734 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(302) GID 1 SID 100000735 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(303) GID 1 SID 100000736 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(304) GID 1 SID 100000737 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(305) GID 1 SID 100000738 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(306) GID 1 SID 100000739 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(307) GID 1 SID 100000740 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(308) GID 1 SID 100000741 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(309) GID 1 SID 100000742 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(310) GID 1 SID 100000743 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(311) GID 1 SID 100000744 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(312) GID 1 SID 100000745 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(313) GID 1 SID 100000746 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(314) GID 1 SID 100000747 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(315) GID 1 SID 100000748 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(316) GID 1 SID 100000749 in rule
```

```
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(317) GID 1 SID 100000750 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(318) GID 1 SID 100000751 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(319) GID 1 SID 100000752 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(320) GID 1 SID 100000753 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(321) GID 1 SID 100000754 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(322) GID 1 SID 100000755 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(323) GID 1 SID 100000756 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(324) GID 1 SID 100000757 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(325) GID 1 SID 100000758 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(326) GID 1 SID 100000759 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(327) GID 1 SID 100000760 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(328) GID 1 SID 100000761 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(329) GID 1 SID 100000762 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(330) GID 1 SID 100000763 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(331) GID 1 SID 100000764 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(332) GID 1 SID 100000765 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(333) GID 1 SID 100000766 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(334) GID 1 SID 100000767 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(335) GID 1 SID 100000768 in rule
```

```
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(336) GID 1 SID 100000769 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(337) GID 1 SID 100000770 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(338) GID 1 SID 100000771 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(339) GID 1 SID 100000772 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(340) GID 1 SID 100000773 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(341) GID 1 SID 100000774 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(342) GID 1 SID 100000775 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(343) GID 1 SID 100000776 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(344) GID 1 SID 100000777 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(345) GID 1 SID 100000778 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(346) GID 1 SID 100000779 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(347) GID 1 SID 100000780 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(348) GID 1 SID 100000781 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(349) GID 1 SID 100000782 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(350) GID 1 SID 100000783 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(351) GID 1 SID 100000784 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(352) GID 1 SID 100000785 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(353) GID 1 SID 100000786 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(354) GID 1 SID 100000787 in rule
```

```
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(355) GID 1 SID 100000788 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(356) GID 1 SID 100000789 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(357) GID 1 SID 100000790 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(358) GID 1 SID 100000791 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(359) GID 1 SID 100000792 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(360) GID 1 SID 100000793 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(361) GID 1 SID 100000794 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(362) GID 1 SID 100000795 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(363) GID 1 SID 100000796 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(364) GID 1 SID 100000797 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(365) GID 1 SID 100000798 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(366) GID 1 SID 100000799 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(367) GID 1 SID 100000800 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(368) GID 1 SID 100000801 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(369) GID 1 SID 100000802 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(370) GID 1 SID 100000803 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(371) GID 1 SID 100000804 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(372) GID 1 SID 100000805 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(373) GID 1 SID 100000806 in rule
```

```
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(374) GID 1 SID 100000807 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(375) GID 1 SID 100000808 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(376) GID 1 SID 100000809 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(377) GID 1 SID 100000810 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(378) GID 1 SID 100000811 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(379) GID 1 SID 100000812 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(380) GID 1 SID 100000813 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(381) GID 1 SID 100000814 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(382) GID 1 SID 100000815 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(383) GID 1 SID 100000816 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(384) GID 1 SID 100000817 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(385) GID 1 SID 100000818 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(386) GID 1 SID 100000820 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(387) GID 1 SID 100000821 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(388) GID 1 SID 100000822 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(389) GID 1 SID 100000823 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(390) GID 1 SID 100000824 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(391) GID 1 SID 100000825 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(392) GID 1 SID 100000826 in rule
```

```
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(393) GID 1 SID 100000827 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(394) GID 1 SID 100000828 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(395) GID 1 SID 100000829 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(396) GID 1 SID 100000830 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(397) GID 1 SID 100000831 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(398) GID 1 SID 100000832 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(399) GID 1 SID 100000833 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(400) GID 1 SID 100000834 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(401) GID 1 SID 100000835 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(402) GID 1 SID 100000836 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(403) GID 1 SID 100000837 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(404) GID 1 SID 100000838 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(405) GID 1 SID 100000839 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(406) GID 1 SID 100000840 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(407) GID 1 SID 100000841 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(408) GID 1 SID 100000842 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(409) GID 1 SID 100000843 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(410) GID 1 SID 100000844 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(411) GID 1 SID 100000845 in rule
```

```
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(412) GID 1 SID 100000846 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(413) GID 1 SID 100000847 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(414) GID 1 SID 100000849 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(415) GID 1 SID 100000850 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(416) GID 1 SID 100000851 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(417) GID 1 SID 100000852 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(418) GID 1 SID 100000853 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(419) GID 1 SID 100000854 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(420) GID 1 SID 100000855 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(421) GID 1 SID 100000856 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(422) GID 1 SID 100000857 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(423) GID 1 SID 100000858 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(424) GID 1 SID 100000859 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(425) GID 1 SID 100000860 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(426) GID 1 SID 100000861 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(427) GID 1 SID 100000862 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(428) GID 1 SID 100000863 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(431) GID 1 SID 100000865 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(432) GID 1 SID 100000866 in rule
```

```
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(433) GID 1 SID 100000867 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(434) GID 1 SID 100000868 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(435) GID 1 SID 100000869 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(436) GID 1 SID 100000870 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(437) GID 1 SID 100000871 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(438) GID 1 SID 100000872 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(439) GID 1 SID 100000873 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(441) GID 1 SID 100000882 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(443) GID 1 SID 100000883 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(444) GID 1 SID 100000884 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(445) GID 1 SID 100000885 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(446) GID 1 SID 100000886 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(447) GID 1 SID 100000887 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(448) GID 1 SID 100000888 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(449) GID 1 SID 100000889 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(450) GID 1 SID 100000906 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(451) GID 1 SID 100000907 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(452) GID 1 SID 100000908 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(453) GID 1 SID 100000909 in rule
```

```
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(454) GID 1 SID 100000910 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(455) GID 1 SID 100000911 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(456) GID 1 SID 100000912 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(457) GID 1 SID 100000913 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(458) GID 1 SID 100000914 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(459) GID 1 SID 100000915 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(460) GID 1 SID 100000916 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(461) GID 1 SID 100000917 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(462) GID 1 SID 100000918 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(463) GID 1 SID 100000919 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(464) GID 1 SID 100000920 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(465) GID 1 SID 100000921 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(466) GID 1 SID 100000922 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(467) GID 1 SID 100000925 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(468) GID 1 SID 100000926 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(469) GID 1 SID 100000929 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(470) GID 1 SID 100000930 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(471) GID 1 SID 100000931 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(472) GID 1 SID 100000932 in rule
```

```
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(473) GID 1 SID 100000933 in rule
duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/community-web-php.rules(474) GID 1 SID 100000934 in rule
duplicates previous rule. Ignoring old rule.

4154 Snort rules read
    3479 detection rules
    0 decoder rules
    0 preprocessor rules
3479 Option Chains linked into 295 Chain Headers
0 Dynamic rules
+++++++++++++++++++++++++++++++++++++++++++++++++++

+-------------------[Rule Port Counts]---------------------------------------
|             tcp     udp    icmp      ip
|     src     152      18       0       0
|     dst    3308     126       0       0
|     any     383      48     146      22
|      nc      27       8      95      20
|     s+d      12       5       0       0
+----------------------------------------------------------------------------

+-----------------------[detection-filter-config]------------------------------
| memory-cap : 1048576 bytes
+-----------------------[detection-filter-rules]-------------------------------
| none
-------------------------------------------------------------------------------

+-----------------------[rate-filter-config]-----------------------------------
| memory-cap : 1048576 bytes
+-----------------------[rate-filter-rules]------------------------------------
| none
-------------------------------------------------------------------------------

+-----------------------[event-filter-config]----------------------------------
| memory-cap : 1048576 bytes
+-----------------------[event-filter-global]----------------------------------
| none
+-----------------------[event-filter-local]-----------------------------------
| gen-id=1      sig-id=2494       type=Both      tracking=dst count=20  seconds=60
| gen-id=1      sig-id=2924       type=Threshold tracking=dst count=10  seconds=60
| gen-id=1      sig-id=2923       type=Threshold tracking=dst count=10  seconds=60
| gen-id=1      sig-id=2495       type=Both      tracking=dst count=20  seconds=60
| gen-id=1      sig-id=3273       type=Threshold tracking=src count=5   seconds=2
| gen-id=1      sig-id=1991       type=Limit     tracking=src count=1   seconds=60
| gen-id=1      sig-id=3152       type=Threshold tracking=src count=5   seconds=2
| gen-id=1      sig-id=2275       type=Threshold tracking=dst count=5   seconds=60
| gen-id=1      sig-id=2496       type=Both      tracking=dst count=20  seconds=60
| gen-id=1      sig-id=2523       type=Both      tracking=dst count=10  seconds=10
+-----------------------[suppression]------------------------------------------
| none
-------------------------------------------------------------------------------
Rule application order: activation->dynamic->pass->drop->sdrop->reject->alert->log
Verifying Preprocessor Configurations!
```

```
WARNING: flowbits key 'ms_sql_seen_dns' is checked but not ever set.
WARNING: flowbits key 'smb.tree.create.llsrpc' is set but not ever checked.
33 out of 1024 flowbits in use.

[ Port Based Pattern Matching Memory ]
+- [ Aho-Corasick Summary ] -------------------------------------
| Storage Format    : Full-Q
| Finite Automaton  : DFA
| Alphabet Size     : 256 Chars
| Sizeof State      : Variable (1,2,4 bytes)
| Instances         : 215
|     1 byte states : 204
|     2 byte states : 11
|     4 byte states : 0
| Characters        : 64997
| States            : 32149
| Transitions       : 874108
| State Density     : 10.6%
| Patterns          : 5057
| Match States      : 3857
| Memory (MB)       : 17.00
|   Patterns        : 0.51
|   Match Lists     : 1.02
|   DFA
|     1 byte states : 1.02
|     2 byte states : 14.06
|     4 byte states : 0.00
+----------------------------------------------------------------
[ Number of patterns truncated to 20 bytes: 1039 ]
pcap DAQ configured to passive.
Acquiring network traffic from "enp0s8".
Reload thread starting...
Reload thread started, thread 0x7f90bc307700 (67862)
Decoding Ethernet
Set gid to 136
Set uid to 129

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.7.0 GRE (Build 149)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.9.1 (with TPACKET_V3)
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.2.11

           Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 2.4  <Build 1>
           Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
           Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
           Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
           Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
           Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
           Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
           Preprocessor Object: SF_POP  Version 1.0  <Build 1>
           Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
           Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
           Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
           Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
           Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
           Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
           Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
Commencing packet processing (pid=67857)
```

- Kartoju ICMP užklausą:

```
osboxes@ldvm2:~$
osboxes@ldvm2:~$ ping -c1 192.168.10.14
PING 192.168.10.14 (192.168.10.14) 56(84) bytes of data.
64 bytes from 192.168.10.14: icmp_seq=1 ttl=64 time=0.557 ms

--- 192.168.10.14 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.557/0.557/0.557/0.000 ms
```

- Kartoju *telnet* užklausą:

```
osboxes@ldvm2:~$ telnet 192.168.10.14
Trying 192.168.10.14...
Connected to 192.168.10.14.
Escape character is '^]'.
Ubuntu 20.04.2 LTS
ldvm1 login: root
Password:

Login incorrect
ldvm1 login:
telnet> Connection closed.
```

- Deja, Snort neaptiko naujos *telnet* užklausos, tik naują ICMP:

```
osboxes@ldvm1:/usr/local/src/snort-2.9.18$ grep 1000000 /var/log/snort/alert
[**] [1:10000001:0] ICMP test [**]
[**] [1:10000001:0] ICMP test [**]
[**] [1:10000001:0] ICMP test [**]
```

- Išdalinu taisyklę į kelias taisykles po vieną raidę:

```
alert tcp any any -> any 23 (content: "r"; nocase; msg: "Telnet su raide <r>"; sid:
10000003;)
alert tcp any any -> any 23 (content: "o"; nocase; msg: "Telnet su raide <o>"; sid:
10000004;)
alert tcp any any -> any 23 (content: "t"; nocase; msg: "Telnet su raide <t>"; sid:
10000005;)
```

- Nurodau Snort atsinaujinti konfigūraciją:

```
osboxes@ldvm1:/usr/local/src/snort-2.9.18$ sudo pkill -SIGHUP snort
```

```
  ...
Rule application order: activation->dynamic->pass->drop->sdrop->reject->alert->log
      Max Expected Streams: 768
Verifying Preprocessor Configurations!
WARNING: flowbits key 'smb.tree.create.llsrpc' is set but not ever checked.
WARNING: flowbits key 'ms_sql_seen_dns' is checked but not ever set.
33 out of 1024 flowbits in use.

[ Port Based Pattern Matching Memory ]
+- [ Aho-Corasick Summary ] -------------------------------------
| Storage Format    : Full-Q
| Finite Automaton  : DFA
| Alphabet Size     : 256 Chars
| Sizeof State      : Variable (1,2,4 bytes)
| Instances         : 215
|     1 byte states : 204
|     2 byte states : 11
|     4 byte states : 0
| Characters        : 64987
| States            : 32138
| Transitions       : 872093
| State Density     : 10.6%
| Patterns          : 5057
| Match States      : 3865
| Memory (MB)       : 17.00
|   Patterns        : 0.51
|   Match Lists     : 1.02
|   DFA
|     1 byte states : 4.07
|     2 byte states : 56.22
|     4 byte states : 0.00
+----------------------------------------------------------------
[ Number of patterns truncated to 20 bytes: 1039 ]
Session Reload: Reference Count Non-zero for old configuration.

        --== Reload Complete ==--
```

- Kartoju *telnet* užklausą, šitaip Snortas užklausas aptinka:

```
osboxes@ldvm1:/usr/local/src/snort-2.9.18$ grep 1000000 /var/log/snort/alert
[**] [1:10000001:0] ICMP test [**]
[**] [1:10000001:0] ICMP test [**]
[**] [1:10000001:0] ICMP test [**]
[**] [1:10000003:0] Telnet su raide <r> [**]
[**] [1:10000004:0] Telnet su raide <o> [**]
[**] [1:10000004:0] Telnet su raide <o> [**]
[**] [1:10000005:0] Telnet su raide <t> [**]
```

- Paskutinis įrašas toks:

```
[**] [1:10000005:0] Telnet su raide <t> [**]
[Priority: 0]
07/07-14:51:47.052408 192.168.10.13:38348 -> 192.168.10.14:23
TCP TTL:64 TOS:0x10 ID:24141 IpLen:20 DgmLen:53 DF
***AP*** Seq: 0x461679D9  Ack: 0xB290FFC2  Win: 0x1F6  TcpLen: 32
TCP Options (3) => NOP NOP TS: 127699005 1494370432
```

- Leidžiu `tcpdump` paketų gaudyklę ir kartoju *telnet* užklausą:

```
osboxes@ldvm1:/usr/local/src/snort-2.9.18$ sudo tcpdump -tni enp0s8 -X -q dst host
192.168.10.14 and tcp port 23
```

- Su kiekvienu klavišo paspaudimu virtualus kompiuteris gauna po du paketus:
  - simboliui `"r"`:

```
IP 192.168.10.13.38356 > 192.168.10.14.23: tcp 1
        0x0000:  4510 0035 5bdf 4000 4006 4968 c0a8 0a0d  E..5[.@.@.Ih....
        0x0010:  c0a8 0a0e 95d4 0017 5080 9674 e054 41d4  ........P..t.TA.
        0x0020:  8018 01f6 1865 0000 0101 080a 07a3 51cd  .....e........Q.
        0x0030:  5919 035a 72                             Y..Zr
IP 192.168.10.13.38356 > 192.168.10.14.23: tcp 0
        0x0000:  4510 0034 5be0 4000 4006 4968 c0a8 0a0d  E..4[.@.@.Ih....
        0x0010:  c0a8 0a0e 95d4 0017 5080 9675 e054 41d5  ........P..u.TA.
        0x0020:  8010 01f6 74ce 0000 0101 080a 07a3 51cf  ....t.........Q.
        0x0030:  5919 18f6                                Y...
```

  - simboliui `"o"`:

```
IP 192.168.10.13.38356 > 192.168.10.14.23: tcp 1
        0x0000:  4510 0035 5be1 4000 4006 4966 c0a8 0a0d  E..5[.@.@.If....
        0x0010:  c0a8 0a0e 95d4 0017 5080 9675 e054 41d5  ........P..u.TA.
        0x0020:  8018 01f6 f6c9 0000 0101 080a 07a3 60ca  ..............`.
        0x0030:  5919 18f6 6f                             Y...o
IP 192.168.10.13.38356 > 192.168.10.14.23: tcp 0
        0x0000:  4510 0034 5be2 4000 4006 4966 c0a8 0a0d  E..4[.@.@.If....
        0x0010:  c0a8 0a0e 95d4 0017 5080 9676 e054 41d6  ........P..v.TA.
        0x0020:  8010 01f6 56d2 0000 0101 080a 07a3 60cb  ....V.........`.
        0x0030:  5919 27f4                                Y.'.
```

- Matyti, kad perduodami simboliai yra paketų poros pirmojo paketo gale.
- Surandu būdą perduoti `"root"` vartotojo vardą iškart, iš komandinės eilutės:

```
osboxes@ldvm2:~$ telnet -l root 192.168.10.14
Trying 192.168.10.14...
Connected to 192.168.10.14.
Escape character is '^]'.
Password:

Login incorrect
ldvm1 login:
telnet> Connection closed.
```

- Deja, Snort šios *telnet* užklausos neaptiko:

```
osboxes@ldvm1:/usr/local/src/snort-2.9.18$ grep 1000000 /var/log/snort/alert
[**] [1:10000001:0] ICMP test [**]
[**] [1:10000001:0] ICMP test [**]
[**] [1:10000001:0] ICMP test [**]
[**] [1:10000003:0] Telnet su raide <r> [**]
[**] [1:10000004:0] Telnet su raide <o> [**]
[**] [1:10000004:0] Telnet su raide <o> [**]
[**] [1:10000005:0] Telnet su raide <t> [**]
```

- Tikrinu su `tcpdump`:

```
osboxes@ldvm1:/usr/local/src/snort-2.9.18$ sudo tcpdump -tni enp0s8 -X -q dst host
192.168.10.14 and tcp port 23 | grep -A1 -e ^IP -e USER -e oot
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp0s8, link-type EN10MB (Ethernet), capture size 262144 bytes

IP 192.168.10.13.38376 > 192.168.10.14.23: tcp 0
        0x0000:  4510 003c 9df2 4000 4006 074e c0a8 0a0d  E..<..@.@..N....
  ...
IP 192.168.10.13.38380 > 192.168.10.14.23: tcp 53
        0x0000:  4510 0069 9dfa 4000 4006 0719 c0a8 0a0d  E..i..@.@.......
--
        0x0040:  3430 30ff f0ff fa27 0000 5553 4552 0172  400....'..USER.r
        0x0050:  6f6f 74ff f0ff fa18 0078 7465 726d 2d32  oot......xterm-2
        0x0060:  3536 636f 6c6f 72ff f0                   56color..
IP 192.168.10.13.38380 > 192.168.10.14.23: tcp 0
        0x0000:  4510 0034 9dfb 4000 4006 074d c0a8 0a0d  E..4..@.@..M....
  ...
```

- Matyti, kad dabar visi 4 simboliai `"root"` atkeliauja kartu.
  Tačiau Snort jų vis tiek neaptinka.
- Kilo mintis, kad Ubuntu DAQ biblioteka pagal nutylėjimą galbūt ne tik per sena, bet turi ir defektų.
- Tikrinu turimą `libdaq` versiją:

```
osboxes@ldvm1:/usr/local/src/snort-2.9.18$ dpkg --list | grep daq | cut -c 1-80
ii  libdaq-dev                                 2.0.4-3build2
ii  libdaq2                                    2.0.4-3build2

osboxes@ldvm1:/usr/local/src/snort-2.9.18$ dpkg --list libdaq2 libdaq-dev
Desired=Unknown/Install/Remove/Purge/Hold
| Status=Not/Inst/Conf-files/Unpacked/halF-conf/Half-inst/trig-aWait/Trig-pend
|/ Err?=(none)/Reinst-required (Status,Err: uppercase=bad)
||/ Name           Version       Architecture Description
+++-==============-=============-============-=================================>
ii  libdaq-dev     2.0.4-3build2 amd64        Data Acquisition library for pack>
ii  libdaq2        2.0.4-3build2 amd64        Data Acquisition library for pack>
```

- `snort.org` siūlo naujesnę `libdaq` versiją: https://www.snort.org/downloads/snort/daq-2.0.7.tar.gz
- Parsisiunčiu `libdaq`:

```
osboxes@ldvm1:/usr/local/src/snort-2.9.18$ cd ..
osboxes@ldvm1:/usr/local/src$
osboxes@ldvm1:/usr/local/src$ wget https://www.snort.org/downloads/snort/daq-
2.0.7.tar.gz
--2021-07-07 15:41:19--  https://www.snort.org/downloads/snort/daq-2.0.7.tar.gz
Resolving www.snort.org (www.snort.org)... 104.18.138.9, 104.18.139.9,
2606:4700::6812:8a09, ...
Connecting to www.snort.org (www.snort.org)|104.18.138.9|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://snort-org-
site.s3.amazonaws.com/production/release_files/files/000/018/470/original/daq-
2.0.7.tar.gz?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-
Credential=AKIAIXACIED2SPMSC7GA%2F20210707%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-
Date=20210707T124119Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-
Signature=20b5a0a6ff60da192509cbf10c3be60e2a2393ee8a3d61be526f3d70f335f153
[following]
--2021-07-07 15:41:19--  https://snort-org-
site.s3.amazonaws.com/production/release_files/files/000/018/470/original/daq-
2.0.7.tar.gz?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-
Credential=AKIAIXACIED2SPMSC7GA%2F20210707%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-
Date=20210707T124119Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-
Signature=20b5a0a6ff60da192509cbf10c3be60e2a2393ee8a3d61be526f3d70f335f153
Resolving snort-org-site.s3.amazonaws.com (snort-org-site.s3.amazonaws.com)...
52.216.251.172
Connecting to snort-org-site.s3.amazonaws.com (snort-org-
site.s3.amazonaws.com)|52.216.251.172|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 515154 (503K) [binary/octet-stream]
Saving to: ‘daq-2.0.7.tar.gz.2’

daq-2.0.7.tar.gz.2  100%[===================>] 503.08K   398KB/s    in 1.3s

2021-07-07 15:41:21 (398 KB/s) - ‘daq-2.0.7.tar.gz.2’ saved [515154/515154]
```

- Atnaujinu `libdaq` pagal Snort_2.9.9.x_on_Ubuntu_14-16.pdf (https://s3.amazonaws.com/snort-org-site/production/document_files/files/000/000/122/original/Snort_2.9.9.x_on_Ubuntu_14-16.pdf) .
    - Išarchyvuoju:

      ```
      osboxes@ldvm1:/usr/local/src$ tar xvzf daq-2.0.7.tar.gz
      daq-2.0.7/
      daq-2.0.7/config.h.in
      daq-2.0.7/config.guess
      daq-2.0.7/api/
      daq-2.0.7/api/daq.h
      daq-2.0.7/api/Makefile.am
        ...
      daq-2.0.7/sfbpf/sf-redefines.h
      daq-2.0.7/README
      daq-2.0.7/configure.ac
      daq-2.0.7/Makefile.in
      daq-2.0.7/ChangeLog
      daq-2.0.7/depcomp
      ```

    - Konfigūruoju kompiliatorių:

      ```
      osboxes@ldvm1:/usr/local/src$ cd daq-2.0.7/

      osboxes@ldvm1:/usr/local/src/daq-2.0.7$ ./configure
      checking for a BSD-compatible install... /usr/bin/install -c
      checking whether build environment is sane... yes
      checking for a thread-safe mkdir -p... /usr/bin/mkdir -p
      checking for gawk... no
        ...
      checking for strtoul... yes
      checking that generated files are newer than configure... done
      configure: creating ./config.status
      config.status: creating Makefile
      config.status: creating api/Makefile
      config.status: creating os-daq-modules/Makefile
      config.status: creating os-daq-modules/daq-modules-config
      config.status: creating sfbpf/Makefile
      config.status: creating config.h
      config.status: executing depfiles commands
      config.status: executing libtool commands

      Build AFPacket DAQ module.. : yes
      Build Dump DAQ module...... : yes
      Build IPFW DAQ module...... : yes
      Build IPQ DAQ module....... : no
      Build NFQ DAQ module....... : no
      Build PCAP DAQ module...... : yes
      Build netmap DAQ module.... : no
      ```

- Kompiliuoju:

```
osboxes@ldvm1:/usr/local/src/daq-2.0.7$ make
make  all-recursive
make[1]: Entering directory '/usr/local/src/daq-2.0.7'
Making all in api
make[2]: Entering directory '/usr/local/src/daq-2.0.7/api'
/bin/bash ../libtool  --tag=CC   --mode=compile gcc -DHAVE_CONFIG_H -I. -I..   -
I/usr/include  -g -O2 -fvisibility=hidden -Wall -Wwrite-strings -Wsign-compare -
Wcast-align -Wextra -Wformat -Wformat-security -Wno-unused-parameter -fno-strict-
aliasing -fdiagnostics-show-option -pedantic -std=c99 -D_GNU_SOURCE -MT
daq_base.lo -MD -MP -MF .deps/daq_base.Tpo -c -o daq_base.lo daq_base.c
libtool: compile:  gcc -DHAVE_CONFIG_H -I. -I.. -I/usr/include -g -O2 -
fvisibility=hidden -Wall -Wwrite-strings -Wsign-compare -Wcast-align -Wextra -
Wformat -Wformat-security -Wno-unused-parameter -fno-strict-aliasing -
fdiagnostics-show-option -pedantic -std=c99 -D_GNU_SOURCE -MT daq_base.lo -MD -MP
-MF .deps/daq_base.Tpo -c daq_base.c  -fPIC -DPIC -o .libs/daq_base.o
  ...
/bin/bash ../libtool  --tag=CC   --mode=link gcc -DBUILDING_SO -g -O2 -
fvisibility=hidden -Wall -Wwrite-strings -Wsign-compare -Wcast-align -Wextra -
Wformat -Wformat-security -Wno-unused-parameter -fno-strict-aliasing -
fdiagnostics-show-option -pedantic -std=c99 -D_GNU_SOURCE -module -export-dynamic
-avoid-version -shared   -o daq_ipfw.la -rpath /usr/local/lib/daq daq_ipfw_la-
daq_ipfw.lo ../sfbpf/libsfbpf.la
libtool: link: gcc -shared  -fPIC -DPIC  .libs/daq_ipfw_la-daq_ipfw.o   -Wl,-
rpath -Wl,/usr/local/src/daq-2.0.7/sfbpf/.libs ../sfbpf/.libs/libsfbpf.so  -g -O2
-Wl,-soname -Wl,daq_ipfw.so -o .libs/daq_ipfw.so
libtool: link: ( cd ".libs" && rm -f "daq_ipfw.la" && ln -s "../daq_ipfw.la"
"daq_ipfw.la" )
make[2]: Leaving directory '/usr/local/src/daq-2.0.7/os-daq-modules'
make[2]: Entering directory '/usr/local/src/daq-2.0.7'
make[2]: Leaving directory '/usr/local/src/daq-2.0.7'
make[1]: Leaving directory '/usr/local/src/daq-2.0.7'
```

- Išinstaliuoju `libdaq` ir `snort` versijas pagal nutylėjimą:

```
osboxes@ldvm1:/usr/local/src/snort-2.9.18$ sudo apt-get autoremove libdaq2 libdaq-dev --purge
Reading package lists... Done
Building dependency tree
Reading state information... Done
Package 'libdaq-dev' is not installed, so not removed
The following packages will be REMOVED:
  libdaq2* oinkmaster* snort* snort-common* snort-common-libraries* snort-rules-default*
0 upgraded, 0 newly installed, 6 to remove and 154 not upgraded.
After this operation, 7,246 kB disk space will be freed.
Do you want to continue? [Y/n] y
(Reading database ... 198477 files and directories currently installed.)
Removing snort (2.9.7.0-5build1) ...
Stopping snort (via systemctl): snort.service.
Removing libdaq2 (2.0.4-3build2) ...
Removing oinkmaster (2.0-4) ...
Removing snort-common (2.9.7.0-5build1) ...
Removing snort-common-libraries (2.9.7.0-5build1) ...
Removing snort-rules-default (2.9.7.0-5build1) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for libc-bin (2.31-0ubuntu9.2) ...
(Reading database ... 198321 files and directories currently installed.)
Purging configuration files for oinkmaster (2.0-4) ...
Purging configuration files for snort (2.9.7.0-5build1) ...
Purging configuration files for snort-common (2.9.7.0-5build1) ...
Purging configuration files for snort-rules-default (2.9.7.0-5build1) ...
dpkg: warning: while removing snort-rules-default, directory '/etc/snort/rules' not empty so not removed
Processing triggers for systemd (245.4-4ubuntu3.7) ...
```

- Instaliuoju naują `libdaq`:

```
osboxes@ldvm1:/usr/local/src/daq-2.0.7$ sudo make install
Making install in api
make[1]: Entering directory '/usr/local/src/daq-2.0.7/api'
make[2]: Entering directory '/usr/local/src/daq-2.0.7/api'
 /usr/bin/mkdir -p '/usr/local/lib'
  /bin/bash ../libtool   --mode=install /usr/bin/install -c   libdaq.la
libdaq_static.la '/usr/local/lib'
  libtool: install: /usr/bin/install -c .libs/libdaq.so.2.0.4
/usr/local/lib/libdaq.so.2.0.4
  libtool: install: (cd /usr/local/lib && { ln -s -f libdaq.so.2.0.4 libdaq.so.2
|| { rm -f libdaq.so.2 && ln -s libdaq.so.2.0.4 libdaq.so.2; }; })
  libtool: install: (cd /usr/local/lib && { ln -s -f libdaq.so.2.0.4 libdaq.so ||
{ rm -f libdaq.so && ln -s libdaq.so.2.0.4 libdaq.so; }; })
  libtool: install: /usr/bin/install -c .libs/libdaq.lai /usr/local/lib/libdaq.la
  ...
libtool: finish:
PATH="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin:/sbi
n" ldconfig -n /usr/local/lib/daq
----------------------------------------------------------------------
Libraries have been installed in:
   /usr/local/lib/daq

If you ever happen to want to link against installed libraries
in a given directory, LIBDIR, you must either use libtool, and
specify the full pathname of the library, or use the '-LLIBDIR'
flag during linking and do at least one of the following:
   - add LIBDIR to the 'LD_LIBRARY_PATH' environment variable
     during execution
   - add LIBDIR to the 'LD_RUN_PATH' environment variable
     during linking
   - use the '-Wl,-rpath -Wl,LIBDIR' linker flag
   - have your system administrator add LIBDIR to '/etc/ld.so.conf'

See any operating system documentation about shared libraries for
more information, such as the ld(1) and ld.so(8) manual pages.
----------------------------------------------------------------------
make[2]: Nothing to be done for 'install-data-am'.
make[2]: Leaving directory '/usr/local/src/daq-2.0.7/os-daq-modules'
make[1]: Leaving directory '/usr/local/src/daq-2.0.7/os-daq-modules'
make[1]: Entering directory '/usr/local/src/daq-2.0.7'
make[2]: Entering directory '/usr/local/src/daq-2.0.7'
make[2]: Nothing to be done for 'install-exec-am'.
make[2]: Nothing to be done for 'install-data-am'.
make[2]: Leaving directory '/usr/local/src/daq-2.0.7'
make[1]: Leaving directory '/usr/local/src/daq-2.0.7'
```

- Iš naujo susikompiliuoju Snort:

```
osboxes@ldvm1:/usr/local/src/snort-2.9.18$ make clean
Making clean in src
make[1]: Entering directory '/usr/local/src/snort-2.9.18/src'
Making clean in sfutil
make[2]: Entering directory '/usr/local/src/snort-2.9.18/src/sfutil'
rm -rf .libs _libs
test -z "libsfutil.a" || rm -f libsfutil.a
rm -f *.o
rm -f *.lo
  ...
rm -rf .libs _libs
rm -f *.lo
make[2]: Leaving directory '/usr/local/src/snort-2.9.18/tools'
make[1]: Leaving directory '/usr/local/src/snort-2.9.18/tools'
make[1]: Entering directory '/usr/local/src/snort-2.9.18'
rm -rf .libs _libs
rm -f *.lo
make[1]: Leaving directory '/usr/local/src/snort-2.9.18'
```

```
osboxes@ldvm1:/usr/local/src/snort-2.9.18$ ./configure --disable-open-appid 2>&1 |
tee configure-v2.log
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for a thread-safe mkdir -p... /usr/bin/mkdir -p
checking for gawk... no
  ...
checking for separate IP versions on pinhole endpoints... no
checking for DAQ_VERDICT_RETRY... yes
checking for daq packet trace... no
DAQ version doesn't support packet trace.
checking for daq verdict reason... no
DAQ version doesn't support tracing verdict reason.
checking for sparc... no
checking for visibility support... yes
checking zlib.h usability... yes
checking zlib.h presence... yes
checking for zlib.h... yes
checking for inflate in -lz... yes
checking lzma.h usability... no
checking lzma.h presence... no
checking for lzma.h... no
checking for lzma_stream_decoder in -llzma... no
checking for pthread_tryjoin_np... yes
checking for nghttp2_option_new in -lnghttp2... no

   Libnghttp2 library not found.
   Get it from https://nghttp2.org/

checking for linuxthreads... no
checking for yylex_destroy support... yes
checking for SFLINUX... no
checking for WRLINUX... no
checking that generated files are newer than configure... done
configure: creating ./config.status
config.status: creating snort.pc
config.status: creating Makefile
config.status: creating src/Makefile
config.status: creating src/sfutil/Makefile
config.status: creating src/control/Makefile
  ...
config.status: creating tools/file_server/Makefile
config.status: creating src/win32/Makefile
config.status: creating src/reload-adjust/Makefile
config.status: creating config.h
config.status: config.h is unchanged
config.status: executing depfiles commands
config.status: executing libtool commands
```

```
osboxes@ldvm1:/usr/local/src/snort-2.9.18$ time make
make  all-recursive
make[1]: Entering directory '/usr/local/src/snort-2.9.18'
Making all in src
make[2]: Entering directory '/usr/local/src/snort-2.9.18/src'
Making all in sfutil
make[3]: Entering directory '/usr/local/src/snort-2.9.18/src/sfutil'
gcc -DHAVE_CONFIG_H -I. -I../.. -I../.. -I../../src -I../../src/sfutil -
I/usr/include/pcap -I../../src/output-plugins -I../../src/detection-plugins -
I../../src/dynamic-plugins -I../../src/preprocessors -
I../../src/preprocessors/portscan -I../../src/preprocessors/HttpInspect/include -
I../../src/preprocessors/Session -I../../src/preprocessors/Stream6 -
I../../src/target-based -I../../src/control -I../../src/file-process -
I../../src/file-process/libs -I../../src/side-channel -I../../src/side-
channel/plugins -I../../src/reload-adjust  -DGRE -DMPLS -DPPM_MGR -DNDEBUG -
DENABLE_REACT -DENABLE_RESPOND -DENABLE_RESPONSE3 -DSF_WCHAR -DTARGET_BASED -
DPERF_PROFILING -DSNORT_RELOAD -DNO_NON_ETHER_DECODER -DNORMALIZER -DACTIVE_RESPONSE
-g -O2 -DSF_VISIBILITY -fvisibility=hidden -Wall -c sfghash.c
  ...
gcc -DHAVE_CONFIG_H -I. -I../.. -I../.. -I../../src -I../../src/sfutil -
I/usr/include/pcap -I../../src/output-plugins -I../../src/detection-plugins -
I../../src/dynamic-plugins -I../../src/preprocessors -
I../../src/preprocessors/portscan -I../../src/preprocessors/HttpInspect/include -
I../../src/preprocessors/Session -I../../src/preprocessors/Stream6 -
I../../src/target-based -I../../src/control -I../../src/file-process -
I../../src/file-process/libs -I../../src/side-channel -I../../src/side-
channel/plugins -I../../src/reload-adjust -I/usr/include/pcap  -DGRE -DMPLS -
DPPM_MGR -DNDEBUG -DENABLE_REACT -DENABLE_RESPOND -DENABLE_RESPONSE3 -DSF_WCHAR -
DTARGET_BASED -DPERF_PROFILING -DSNORT_RELOAD -DNO_NON_ETHER_DECODER -DNORMALIZER -
DACTIVE_RESPONSE -g -O2 -DSF_VISIBILITY -fvisibility=hidden -Wall  -g -O2 -
DSF_VISIBILITY -fvisibility=hidden -Wall -MT u2spewfoo-u2spewfoo.o -MD -MP -MF
.deps/u2spewfoo-u2spewfoo.Tpo -c -o u2spewfoo-u2spewfoo.o `test -f 'u2spewfoo.c' ||
echo './'`u2spewfoo.c
mv -f .deps/u2spewfoo-u2spewfoo.Tpo .deps/u2spewfoo-u2spewfoo.Po
/bin/bash ../../libtool  --tag=CC   --mode=link gcc -g -O2 -DSF_VISIBILITY -
fvisibility=hidden -Wall  -g -O2 -DSF_VISIBILITY -fvisibility=hidden -Wall  -lpcre -
ldumbnet -o u2spewfoo u2spewfoo-u2spewfoo.o  -lz -ldaq_static -ldumbnet -lpcre -
lpcap -lnsl -lm -lm  -lcrypto -ldl -L/usr/local/lib -ldaq_static_modules  -lsfbpf -
lpcap -lsfbpf -lpcap -lz -lpthread -lpthread -lpthread
libtool: link: gcc -g -O2 -DSF_VISIBILITY -fvisibility=hidden -Wall -g -O2 -
DSF_VISIBILITY -fvisibility=hidden -Wall -o u2spewfoo u2spewfoo-u2spewfoo.o
/usr/local/lib/libdaq_static.a /usr/lib/x86_64-linux-gnu/libdumbnet.so -lpcre -lnsl
-lm -lcrypto -ldl -L/usr/local/lib /usr/local/lib/libdaq_static_modules.a
/usr/local/lib/libsfbpf.so -lpcap -lz -lpthread
make[3]: Leaving directory '/usr/local/src/snort-2.9.18/tools/u2spewfoo'
make[3]: Entering directory '/usr/local/src/snort-2.9.18/tools'
make[3]: Nothing to be done for 'all-am'.
make[3]: Leaving directory '/usr/local/src/snort-2.9.18/tools'
make[2]: Leaving directory '/usr/local/src/snort-2.9.18/tools'
make[2]: Entering directory '/usr/local/src/snort-2.9.18'
make[2]: Leaving directory '/usr/local/src/snort-2.9.18'
make[1]: Leaving directory '/usr/local/src/snort-2.9.18'

real    3m9.933s
user    2m30.969s
sys     0m27.158s
```

- Deja, perspėjimai apie DAQ versiją išliko:

```
DAQ version doesn't support packet trace.
checking for daq verdict reason... no
DAQ version doesn't support tracing verdict reason.
```

- Vėl instaliuoju naują Snort:

```
osboxes@ldvm1:/usr/local/src/snort-2.9.18$ sudo make install
Making install in src
make[1]: Entering directory '/usr/local/src/snort-2.9.18/src'
Making install in sfutil
make[2]: Entering directory '/usr/local/src/snort-2.9.18/src/sfutil'
make[3]: Entering directory '/usr/local/src/snort-2.9.18/src/sfutil'
  ...
make[3]: Leaving directory '/usr/local/src/snort-2.9.18/tools'
make[2]: Leaving directory '/usr/local/src/snort-2.9.18/tools'
make[1]: Leaving directory '/usr/local/src/snort-2.9.18/tools'
make[1]: Entering directory '/usr/local/src/snort-2.9.18'
make[2]: Entering directory '/usr/local/src/snort-2.9.18'
make[2]: Nothing to be done for 'install-exec-am'.
 /usr/bin/mkdir -p '/usr/local/share/man/man8'
 /usr/bin/install -c -m 644 snort.8 '/usr/local/share/man/man8'
 /usr/bin/mkdir -p '/usr/local/lib/pkgconfig'
 /usr/bin/install -c -m 644 snort.pc '/usr/local/lib/pkgconfig'
make[2]: Leaving directory '/usr/local/src/snort-2.9.18'
make[1]: Leaving directory '/usr/local/src/snort-2.9.18'
```

- Snort trūksta naujos bibliotekos:

```
osboxes@ldvm1:/usr/local/src/snort-2.9.18$ snort -V
snort: error while loading shared libraries: libsfbpf.so.0: cannot open shared
object file: No such file or directory
```

- Atnaujinu bibliotekų sąrašus:

```
osboxes@ldvm1:/usr/local/src/snort-2.9.18$ sudo find / -name libsfbpf.so.0
find: ‘/run/user/1000/gvfs’: Permission denied
/usr/local/lib/libsfbpf.so.0
/usr/local/src/daq-2.0.7/sfbpf/.libs/libsfbpf.so.0

osboxes@ldvm1:/usr/local/src/snort-2.9.18$ sudo ldconfig
```

- Vėl veikia Snort 2.9.18:

```
osboxes@ldvm1:/usr/local/src/snort-2.9.18$ snort -V

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.18 GRE (Build 169)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2021 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.9.1 (with TPACKET_V3)
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.2.11
```

- Vėl įkeliu naujo Snort konfigūracinius failus:

```
osboxes@ldvm1:/usr/local/src/snort-2.9.18$ sudo groupadd snort
osboxes@ldvm1:/usr/local/src/snort-2.9.18$ sudo useradd -g snort snort
osboxes@ldvm1:/usr/local/src/snort-2.9.18$ sudo mkdir /var/log/snort
osboxes@ldvm1:/usr/local/src/snort-2.9.18$ sudo chown snort:snort /var/log/snort
osboxes@ldvm1:/usr/local/src/snort-2.9.18$ sudo cp -v /usr/local/src/snort-
2.9.18/etc/*.* /etc/snort/
'/usr/local/src/snort-2.9.18/etc/attribute_table.dtd' ->
'/etc/snort/attribute_table.dtd'
'/usr/local/src/snort-2.9.18/etc/classification.config' ->
'/etc/snort/classification.config'
'/usr/local/src/snort-2.9.18/etc/file_magic.conf' -> '/etc/snort/file_magic.conf'
'/usr/local/src/snort-2.9.18/etc/gen-msg.map' -> '/etc/snort/gen-msg.map'
'/usr/local/src/snort-2.9.18/etc/Makefile.am' -> '/etc/snort/Makefile.am'
'/usr/local/src/snort-2.9.18/etc/Makefile.in' -> '/etc/snort/Makefile.in'
'/usr/local/src/snort-2.9.18/etc/reference.config' -> '/etc/snort/reference.config'
'/usr/local/src/snort-2.9.18/etc/snort.conf' -> '/etc/snort/snort.conf'
'/usr/local/src/snort-2.9.18/etc/threshold.conf' -> '/etc/snort/threshold.conf'
'/usr/local/src/snort-2.9.18/etc/unicode.map' -> '/etc/snort/unicode.map'
```

- Grąžinu savo pradinę konfigūraciją:

```
osboxes@ldvm1:/usr/local/src/snort-2.9.18$ sudo -i
root@ldvm1:~#
root@ldvm1:~# cat ~osboxes/debug/snort.conf.diff | patch /etc/snort/snort.conf
patching file /etc/snort/snort.conf

root@ldvm1:~# nano /etc/snort/rules/local.rules


Use "fg" to return to nano.

[1]+  Stopped                 nano /etc/snort/rules/local.rules

root@ldvm1:~# cat /etc/snort/rules/local.rules
 alert icmp any any -> 192.168.10.14 any (msg: "ICMP test"; sid:10000001;)
 alert tcp any any -> any 23 (content: "root"; nocase; msg: "Suspicious Telnet";
sid: 10000002;)
 alert tcp any any -> any 23 (content: "r"; nocase; msg: "Telnet su raide <r>"; sid:
10000003;)
 alert tcp any any -> any 23 (content: "o"; nocase; msg: "Telnet su raide <o>"; sid:
10000004;)
 alert tcp any any -> any 23 (content: "t"; nocase; msg: "Telnet su raide <t>"; sid:
10000005;)
```

- Ir vėl startuoju naują Snort:

```
root@ldvm1:~# snort -u snort -g snort -c /etc/snort/snort.conf -i enp0s8:enp0s3 --
daq afpacket --daq-mode inline
Running in IDS mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/snort.conf"
PortVar 'HTTP_PORTS' defined :  [ 80:81 311 383 591 593 901 1220 1414 1741 1830 2301
2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000
8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899
9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555 ]
  ...
Set gid to 1001
Set uid to 1001

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.18 GRE (Build 169)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2021 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.9.1 (with TPACKET_V3)
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.2.11

           Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 3.2  <Build 1>
           Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
           Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
           Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
           Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
           Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
           Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
           Preprocessor Object: SF_POP  Version 1.0  <Build 1>
           Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
           Preprocessor Object: SF_S7COMMPLUS  Version 1.0  <Build 1>
           Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
           Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
           Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
           Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
           Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
           Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
Commencing packet processing (pid=103090)
```

- Siunčiu iš kaimyno kompiuterio...
    - ICMP užklausą:

```
osboxes@ldvm2:~$ ping -c1 192.168.10.14
PING 192.168.10.14 (192.168.10.14) 56(84) bytes of data.
64 bytes from 192.168.10.14: icmp_seq=1 ttl=64 time=0.633 ms

--- 192.168.10.14 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.633/0.633/0.633/0.000 ms
```

  - *telnet* užklausą po vieną raidę + tuščias slaptažodis:

```
osboxes@ldvm2:~$ telnet 192.168.10.14
Trying 192.168.10.14...
Connected to 192.168.10.14.
Escape character is '^]'.
Ubuntu 20.04.2 LTS
ldvm1 login: root
Password:

Login incorrect
ldvm1 login:
telnet> Connection closed.
```

  - *telnet* užklausą su visais keturiais simboliais kartu + slaptažodis yra `"o"`:

```
osboxes@ldvm2:~$ telnet -l root 192.168.10.14
Trying 192.168.10.14...
Connected to 192.168.10.14.
Escape character is '^]'.
Password:
telnet> Connection closed.
```

- Deja, `"root"` seka *telnet* sraute nepagaunama, registruojami tik pavieniai simboliai:

```
osboxes@ldvm1:/usr/local/src$ grep 1000000 /var/log/snort/alert
[**] [1:10000001:0] ICMP test [**]
[**] [1:10000003:0] Telnet su raide <r> [**]
[**] [1:10000004:0] Telnet su raide <o> [**]
[**] [1:10000004:0] Telnet su raide <o> [**]
[**] [1:10000005:0] Telnet su raide <t> [**]
[**] [1:10000004:0] Telnet su raide <o> [**]
```

- `"libdaq"` ir Snort 2 versijos yra trijų mėnesių ir mėnesio senumo:

```
osboxes@ldvm1:/usr/local/src$ tar ztvf daq-2.0.7.tar.gz | awk '{$1=$2=$3=$6="";
print}' | sort -u | tail -1
   2021-03-29 07:21
osboxes@ldvm1:/usr/local/src$ tar ztvf snort-2.9.18.tar.gz | awk '{$1=$2=$3=$6="";
print}' | sort -u | tail -1
   2021-06-08 12:23
```

  - 2021-**03-29** 07:21, `daq-2.0.7.tar.gz`
  - 2021-**06-08** 12:23, `snort-2.9.18.tar.gz`
- Viename iš instaliavimo gidų (https://github.com/bensooter/Snort16OnUbuntu) radau užuominą, kad tinklo plokštėms verta išjungti "Large Receive Offload" (LRO) ir "Generic Receive Offload" (GRO) palaikymą.
  Kitaip dalis duomenų bus nukerpami.
  - Instaliuoju `ethtool`:

    ```
    root@ldvm1:~# apt-get install ethtool
    Reading package lists... Done
    Building dependency tree
    Reading state information... Done
    The following NEW packages will be installed:
      ethtool
    0 upgraded, 1 newly installed, 0 to remove and 154 not upgraded.
    Need to get 134 kB of archives.
    After this operation, 461 kB of additional disk space will be used.
    Get:1 http://us.archive.ubuntu.com/ubuntu focal/main amd64 ethtool amd64 1:5.4-1
    [134 kB]
    Fetched 134 kB in 1s (128 kB/s)
    Selecting previously unselected package ethtool.
    (Reading database ... 198230 files and directories currently installed.)
    Preparing to unpack .../ethtool_1%3a5.4-1_amd64.deb ...
    Unpacking ethtool (1:5.4-1) ...
    Setting up ethtool (1:5.4-1) ...
    Processing triggers for man-db (2.9.1-1) ...
    ```

  - Keičiu nustatymus:

    ```
    root@ldvm1:~# ethtool -K enp0s8 gro off
    root@ldvm1:~# ethtool -K enp0s8 lro off
    Cannot change large-receive-offload
    ```

  - Deja, išjungus GRO ir nusiuntus tas pačias užklausas, Snort elgesys nepasikeitė:

    ```
    osboxes@ldvm1:/usr/local/src$ grep 1000000 /var/log/snort/alert
    [**] [1:10000001:0] ICMP test [**]
    [**] [1:10000003:0] Telnet su raide <r> [**]
    [**] [1:10000004:0] Telnet su raide <o> [**]
    [**] [1:10000004:0] Telnet su raide <o> [**]
    [**] [1:10000005:0] Telnet su raide <t> [**]
    [**] [1:10000004:0] Telnet su raide <o> [**]
    [**] [1:10000001:0] ICMP test [**]
    [**] [1:10000004:0] Telnet su raide <o> [**]
    [**] [1:10000003:0] Telnet su raide <r> [**]
    [**] [1:10000004:0] Telnet su raide <o> [**]
    [**] [1:10000004:0] Telnet su raide <o> [**]
    [**] [1:10000005:0] Telnet su raide <t> [**]
    ```

- Pradėjau tyrinėt `snort.conf` pagal tekstą "telnet".
  Įtarimų sukėlė `ftp_telnet` preprocesorius.
- Išjungiu `telnet` normalizaciją tik `telnet` protokolui giminingame preprocesoriuje `ftp_telnet_protocol`:

```
osboxes@ldvm1:/usr/local/src$ cat ~/debug/snort.dont-normalize-telnet.conf
--- snort-2.9.18/etc/snort.conf 2021-06-08 12:23:20.000000000 +0300
+++ /etc/snort/snort.conf       2021-07-07 18:36:16.334477803 +0300
@@ -336,10 +336,10 @@

 # FTP / Telnet normalization and anomaly detection.  For more information, see
README.ftptelnet
 preprocessor ftp_telnet: global inspection_type stateful encrypted_traffic no
check_encrypted
-preprocessor ftp_telnet_protocol: telnet \
-    ayt_attack_thresh 20 \
-    normalize ports { 23 } \
-    detect_anomalies
+# preprocessor ftp_telnet_protocol: telnet \
+#     ayt_attack_thresh 20 \
+#     normalize ports { 23 } \
+#     detect_anomalies
 preprocessor ftp_telnet_protocol: ftp server default \
     def_max_param_len 100 \
     ports { 21 2100 3535 } \
```

- Išvalau laikinas debuginimo taisykles ir atnaujinu jas Snorte:

```
osboxes@ldvm1:/usr/local/src$ cat /etc/snort/rules/local.rules
 alert icmp any any -> 192.168.10.14 any (msg: "ICMP test"; sid:10000001;)
 alert  tcp any any -> 192.168.10.14 23 (content: "root"; nocase; msg: "Suspicious
Telnet"; sid: 10000002;)

osboxes@ldvm1:/usr/local/src$ sudo pkill -SIGHUP snort
```

- Jungiuosi iš kaimyno į virtualų kompiuterį per *telnet* ir su `"root"` vartotoju:

```
osboxes@ldvm2:~$ telnet -l root 192.168.10.14
Trying 192.168.10.14...
Connected to 192.168.10.14.
Escape character is '^]'.
Password:

Login incorrect
ldvm1 login:
telnet> Connection closed.
```

- Pagaliau *telnet* srauto stebėjimas veikia!

```
osboxes@ldvm1:/usr/local/src$ tail -1f /var/log/snort/alert

[**] [1:10000002:0] Suspicious Telnet [**]
[Priority: 0]
07/07-18:53:37.013296 192.168.10.13:38560 -> 192.168.10.14:23
TCP TTL:64 TOS:0x10 ID:56855 IpLen:20 DgmLen:105 DF
***AP*** Seq: 0xFB94525  Ack: 0x47141D77  Win: 0x1F6  TcpLen: 32
TCP Options (3) => NOP NOP TS: 141966812 1508637531
```

11. Bendruomenės taisyklės

```
osboxes@ldvm1:/usr/local/src$ wget https://www.snort.org/downloads/community/com
munity-rules.tar.gz
--2021-07-07 20:57:31--  https://www.snort.org/downloads/community/community-
rules.tar.gz
Resolving www.snort.org (www.snort.org)... 104.18.138.9, 104.18.139.9,
2606:4700::6812:8b09, ...
Connecting to www.snort.org (www.snort.org)|104.18.138.9|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://snort-org-
site.s3.amazonaws.com/production/release_files/files/000/018/901/original/community-
rules.tar.gz?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-
Credential=AKIAIXACIED2SPMSC7GA%2F20210707%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-
Date=20210707T175732Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-
Signature=692fc950b7285a4c9b4579ed31b95a8d9a7da5c17e7da20ab076c2cc9aee9088 [following]
--2021-07-07 20:57:32--  https://snort-org-
site.s3.amazonaws.com/production/release_files/files/000/018/901/original/community-
rules.tar.gz?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-
Credential=AKIAIXACIED2SPMSC7GA%2F20210707%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-
Date=20210707T175732Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-
Signature=692fc950b7285a4c9b4579ed31b95a8d9a7da5c17e7da20ab076c2cc9aee9088
Resolving snort-org-site.s3.amazonaws.com (snort-org-site.s3.amazonaws.com)...
52.216.107.84
Connecting to snort-org-site.s3.amazonaws.com (snort-org-
site.s3.amazonaws.com)|52.216.107.84|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 337941 (330K) [application/gzip]
Saving to: ‘community-rules.tar.gz’

community-rules.tar 100%[===================>] 330.02K   252KB/s    in 1.3s

2021-07-07 20:57:34 (252 KB/s) - ‘community-rules.tar.gz’ saved [337941/337941]
```

- LD aprašo nuoroda netiksli, susirandu susiradau (https://www.snort.org/downloads) veikiančią.

```
osboxes@ldvm1:/usr/local/src$ pwd
/usr/local/src

osboxes@ldvm1:/usr/local/src$ cd /etc/snort

osboxes@ldvm1:/etc/snort$ sudo tar zxvf /usr/local/src/community-rules.tar.gz
community-rules/
community-rules/community.rules
community-rules/VRT-License.txt
community-rules/LICENSE
community-rules/AUTHORS
community-rules/snort.conf
community-rules/sid-msg.map
osboxes@ldvm1:/etc/snort$
```

- Manau, kad išarchyvuota į nekorektišką direktoriją:
  (galbūt aprašas ir čia paseno?)

  ```
  osboxes@ldvm1:/etc/snort$ ll
  total 420
  drwxr-xr-x   4 snort snort   4096 Jul  7 21:02 ./
  drwxr-xr-x 133 root  root   12288 Jul  7 16:54 ../
  -r-xr-xr-x   1 root  root    1281 Jul  7 16:54 attribute_table.dtd*
  -r--r--r--   1 root  root    3757 Jul  7 16:54 classification.config
  drwxr-xr-x   2  1210 root    4096 Jul  7 18:54 community-rules/
  -r--r--r--   1 root  root   23654 Jul  7 16:54 file_magic.conf
  -r--r--r--   1 root  root   33272 Jul  7 16:54 gen-msg.map
  -r--r--r--   1 root  root     190 Jul  7 16:54 Makefile.am
  -rw-r--r--   1 root  root   12306 Jul  7 16:54 Makefile.in
  -r--r--r--   1 root  root     687 Jul  7 16:54 reference.config
  drwxr-xr-x   2 root  root   12288 Jul  7 18:53 rules/
  -rw-r--r--   1 root  root   27010 Jul  7 18:39 snort.conf
  -rw-r-----   1 root  root   28880 Jul  7 12:39 snort.conf.orig
  -rw-r-----   1 root    136  28880 Apr  3  2018 snort.conf.ORIGINAL
  -rw-r--r--   1 root  root   40960 Jul  7 18:37 .snort.conf.swp
  -r--r--r--   1 root  root    2335 Jul  7 16:54 threshold.conf
  -r--r--r--   1 root  root  160606 Jul  7 16:54 unicode.map
  ```

- Perkeliu į įprastą direktoriją:

  ```
  osboxes@ldvm1:/etc/snort$ sudo mv -v community-rules rules/
  renamed 'community-rules' -> 'rules/community-rules'
  ```

- Direktorijos struktūros supratimui instaliuoju papildomą įrankį `tree`:

```
osboxes@ldvm1:/etc/snort$ sudo apt-get install tree
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  tree
0 upgraded, 1 newly installed, 0 to remove and 154 not upgraded.
Need to get 43.0 kB of archives.
After this operation, 115 kB of additional disk space will be used.
Get:1 http://us.archive.ubuntu.com/ubuntu focal/universe amd64 tree amd64 1.8.0-1
[43.0 kB]
Fetched 43.0 kB in 1s (50.4 kB/s)
Selecting previously unselected package tree.
(Reading database ... 198242 files and directories currently installed.)
Preparing to unpack .../tree_1.8.0-1_amd64.deb ...
Unpacking tree (1.8.0-1) ...
Setting up tree (1.8.0-1) ...
Processing triggers for man-db (2.9.1-1) ...
```

12. Skenavimas įgalinus bendruomenės taisykles

- Pirmiausia įtariu, kad išarchyvuotosios taisyklės nebus savaime įtrauktos į Snort veikimą.
- Ieškau `community.rules` faile `snort.conf`:

```
osboxes@ldvm1:/etc/snort$ grep -c community.rules snort.conf
0
osboxes@ldvm1:/etc/snort$ grep -ci community snort.conf
0
```

- Faile nėra jokių nuorodų į šias taisykles.
- Išsisaugau Snort *Self-test* išvestį prieš bendruomenės taisyklių įtraukimą:

```
root@ldvm1:~# snort -u snort -g snort -c /etc/snort/snort.conf -i enp0s8 -T 2>&1 |
tee ~osboxes/debug/14.Snort-selftest-local.rules-only.txt | wc -l
446
```

- Įtraukiu taisykles rankomis, remdamasis pavyzdžiu
  (https://upcloud.com/community/tutorials/install-snort-ubuntu/):

```
osboxes@ldvm1:/etc/snort$ diff -u snort.conf.v2 snort.conf | colordiff
--- snort.conf.v2       2021-07-07 18:39:36.620734396 +0300
+++ snort.conf  2021-07-08 00:28:41.882814390 +0300
@@ -545,6 +545,8 @@

 # site specific rules
 include $RULE_PATH/local.rules
+# community rules
+include $RULE_PATH/community-rules/community.rules

 #include $RULE_PATH/app-detect.rules
 #include $RULE_PATH/attack-responses.rules
```

- Išsisaugau Snort *Self-test* išvestį *po* bendruomenės taisyklių įtraukimo:

```
root@ldvm1:~# snort -u snort -g snort -c /etc/snort/snort.conf -i enp0s8 -T 2>&1 |
tee ~osboxes/debug/15.Snort-selftest-+-community.rules.txt | wc -l
483
```

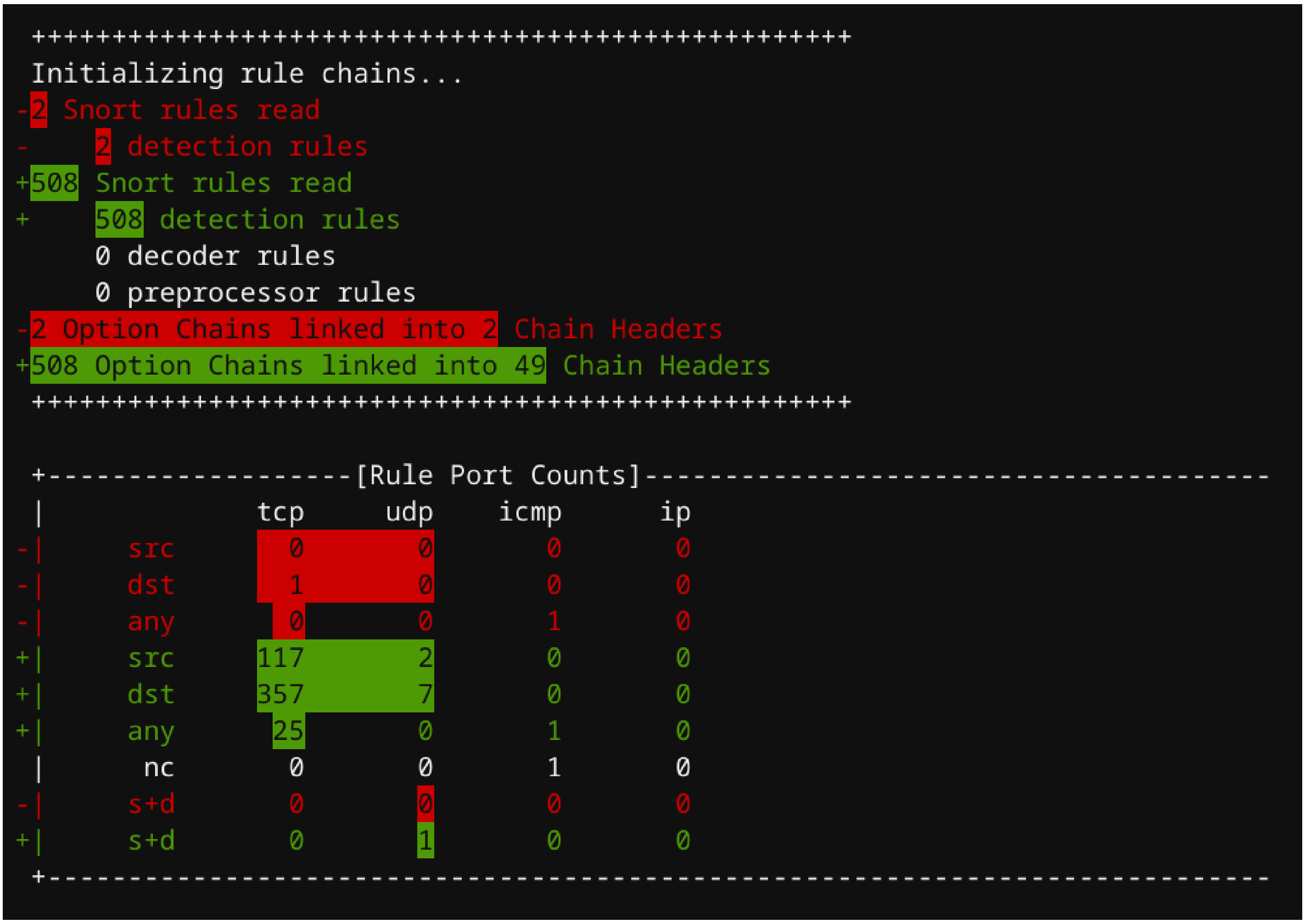
- Palyginu abi Snorto *Self-test* išvestis po eilutę:

```
root@ldvm1:~# diff -u ~osboxes/debug/{14,15}*.txt
--- /home/osboxes/debug/14.Snort-selftest-local.rules-only.txt  2021-07-08
00:44:03.473876602 +0300
+++ /home/osboxes/debug/15.Snort-selftest-+-community.rules.txt 2021-07-08
00:44:16.696176899 +0300
@@ -172,7 +172,7 @@
     alert_large_fragments: INACTIVE
     alert_incomplete: INACTIVE
     alert_multiple_requests: INACTIVE
-MaxRss at the end of static preproc config:27200
+MaxRss at the end of static preproc config:27168
 FTPTelnet Config:
     GLOBAL CONFIG
       Inspection Type: stateful
@@ -336,30 +336,29 @@
     Check Link-Layer CRCs: ENABLED
     Ports:
        20000
-MaxRss at the end of dynamic preproc config:30956
+MaxRss at the end of dynamic preproc config:30916

 +++++++++++++++++++++++++++++++++++++++++++++++++++
 Initializing rule chains...
-2 Snort rules read
-    2 detection rules
+508 Snort rules read
+    508 detection rules
     0 decoder rules
     0 preprocessor rules
-2 Option Chains linked into 2 Chain Headers
+508 Option Chains linked into 49 Chain Headers
 +++++++++++++++++++++++++++++++++++++++++++++++++++

 +-------------------[Rule Port Counts]---------------------------------------
 |             tcp     udp    icmp      ip
-|     src       0       0       0       0
-|     dst       1       0       0       0
-|     any       0       0       1       0
+|     src     117       2       0       0
+|     dst     357       7       0       0
+|     any      25       0       1       0
 |      nc       0       0       1       0
-|     s+d       0       0       0       0
+|     s+d       0       1       0       0
 +----------------------------------------------------------------------------

 +-----------------------[detection-filter-config]------------------------------
 | memory-cap : 1048576 bytes
 +-----------------------[detection-filter-rules]-------------------------------
-| none
 -------------------------------------------------------------------------------

 +-----------------------[rate-filter-config]-----------------------------------
@@ -378,8 +377,46 @@
 -------------------------------------------------------------------------------
 Rule application order: pass->drop->sdrop->reject->alert->log
 Verifying Preprocessor Configurations!
+WARNING: flowbits key 'file.exploit_kit.pe' is set but not ever checked.
+WARNING: flowbits key 'file.oless.v4' is set but not ever checked.
+WARNING: flowbits key 'acunetix-scan' is set but not ever checked.
+WARNING: flowbits key 'file.smi' is set but not ever checked.
+WARNING: flowbits key 'file.xm' is set but not ever checked.
+WARNING: flowbits key 'smb.trans2.findfirst2' is set but not ever checked.
+WARNING: flowbits key 'file.exploit_kit.flash' is set but not ever checked.
+WARNING: flowbits key 'ttyprompt' is set but not ever checked.
+WARNING: flowbits key 'file.dmg' is set but not ever checked.
+WARNING: flowbits key 'file.png' is set but not ever checked.
+WARNING: flowbits key 'smb.trans2.mid66' is set but not ever checked.
+WARNING: flowbits key 'file.xul' is set but not ever checked.
+WARNING: flowbits key 'smb.trans2.fileinfo' is set but not ever checked.
+WARNING: flowbits key 'file.fpx' is set but not ever checked.
+WARNING: flowbits key 'file.jar.agent_helper' is set but not ever checked.
+WARNING: flowbits key 'smb.trans2.mid65' is set but not ever checked.
+WARNING: flowbits key 'file.exploit_kit.pdf' is set but not ever checked.
+WARNING: flowbits key 'file.emf' is set but not ever checked.
+WARNING: flowbits key 'file.xlsb' is set but not ever checked.
+WARNING: flowbits key 'file.pdf' is set but not ever checked.
+WARNING: flowbits key 'file.zip.winrar.spoof' is set but not ever checked.
+WARNING: flowbits key 'file.rmp' is set but not ever checked.
+WARNING: flowbits key 'hawk.lgr' is set but not ever checked.
+WARNING: flowbits key 'file.realplayer.playlist' is set but not ever checked.
+WARNING: flowbits key 'file.rtf.embed' is set but not ever checked.
+WARNING: flowbits key 'file.jpeg' is set but not ever checked.
+WARNING: flowbits key 'file.bmp' is set but not ever checked.
+WARNING: flowbits key 'file.exploit_kit.silverlight' is set but not ever checked.
+WARNING: flowbits key 'smb.trans2.get_dfs_referral' is set but not ever checked.
+WARNING: flowbits key 'file.xml' is set but not ever checked.
+WARNING: flowbits key 'file.doc' is set but not ever checked.
+WARNING: flowbits key 'smb.trans2' is set but not ever checked.
+WARNING: flowbits key 'backdoor.y3krat_15.client.response' is set but not ever
checked.
+WARNING: flowbits key 'file.exploit_kit.jar' is set but not ever checked.
+WARNING: flowbits key 'file.ani' is set but not ever checked.
+WARNING: flowbits key 'smb.null_session' is set but not ever checked.
+WARNING: flowbits key 'file.wmf' is set but not ever checked.
+45 out of 1024 flowbits in use.

-MaxRss at the end of rules:45276
+MaxRss at the end of rules:48340

 [ Port Based Pattern Matching Memory ]
 +- [ Aho-Corasick Summary ] -------------------------------------
@@ -387,27 +424,27 @@
 | Finite Automaton  : DFA
 | Alphabet Size     : 256 Chars
 | Sizeof State      : Variable (1,2,4 bytes)
-| Instances         : 1
-|     1 byte states : 1
-|     2 byte states : 0
+| Instances         : 35
+|     1 byte states : 30
+|     2 byte states : 5
 |     4 byte states : 0
```

```
-| Characters        : 4
-| States            : 5
-| Transitions       : 8
-| State Density     : 0.6%
-| Patterns          : 1
-| Match States      : 1
-| Memory (KB)       : 10.68
-|   Pattern         : 0.09
-|   Match Lists     : 0.12
+| Characters        : 6712
+| States            : 5382
+| Transitions       : 94214
+| State Density     : 6.8%
+| Patterns          : 523
+| Match States      : 499
+| Memory (MB)       : 2.62
+|   Patterns        : 0.05
+|   Match Lists     : 0.10
 |   DFA
-|     1 byte states : 1.30
-|     2 byte states : 0.00
+|     1 byte states : 0.28
+|     2 byte states : 2.14
 |     4 byte states : 0.00
 +----------------------------------------------------------------
-[ Number of patterns truncated to 20 bytes: 0 ]
+[ Number of patterns truncated to 20 bytes: 9 ]

-MaxRss at the end of detection rules:45276
+MaxRss at the end of detection rules:54988
 pcap DAQ configured to passive.
 Acquiring network traffic from "enp0s8".
 Set gid to 1001
@@ -441,6 +478,6 @@
            Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
            Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>

-Total snort Fixed Memory Cost - MaxRss:45672
+Total snort Fixed Memory Cost - MaxRss:54988
 Snort successfully validated the configuration!
 Snort exiting
```

Snorto *Self-test* išvedimas pasikeitė taip (atmetus smulkmenas):

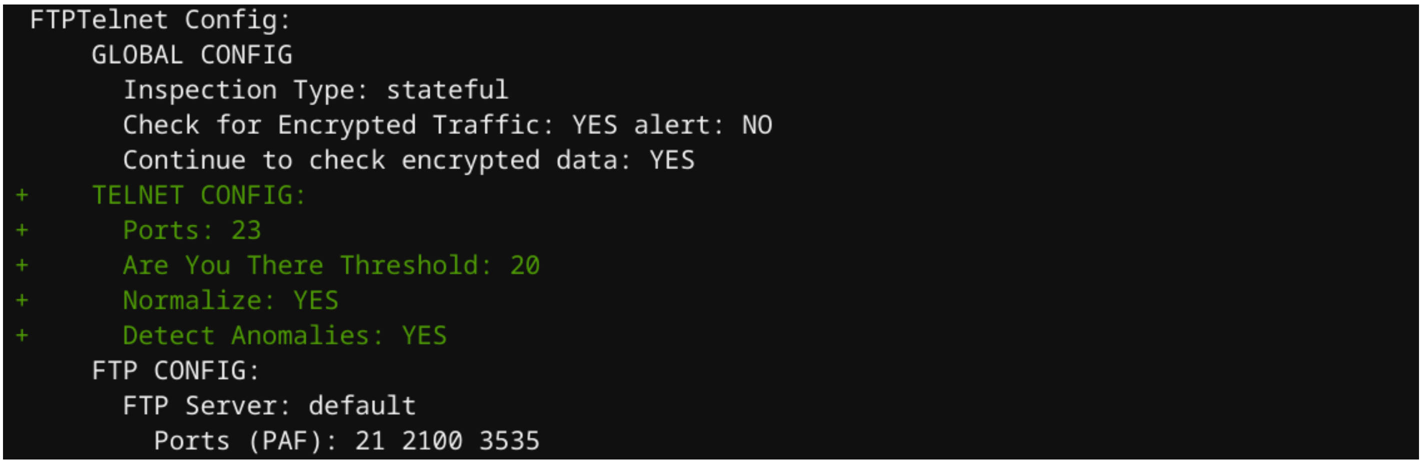
```
 +++++++++++++++++++++++++++++++++++++++++++++++++++
 Initializing rule chains...
-2 Snort rules read
-    2 detection rules
+508 Snort rules read
+    508 detection rules
     0 decoder rules
     0 preprocessor rules
-2 Option Chains linked into 2 Chain Headers
+508 Option Chains linked into 49 Chain Headers
 +++++++++++++++++++++++++++++++++++++++++++++++++++

 +-------------------[Rule Port Counts]---------------------------------------
 |             tcp     udp    icmp      ip
-|     src       0       0       0       0
-|     dst       1       0       0       0
-|     any       0       0       1       0
+|     src     117       2       0       0
+|     dst     357       7       0       0
+|     any      25       0       1       0
 |      nc       0       0       1       0
-|     s+d       0       0       0       0
+|     s+d       0       1       0       0
 +----------------------------------------------------------------------------
```



```
 +++++++++++++++++++++++++++++++++++++++++++++++++++
 Initializing rule chains...
-2 Snort rules read
-    2 detection rules
+508 Snort rules read
+    508 detection rules
     0 decoder rules
     0 preprocessor rules
-2 Option Chains linked into 2 Chain Headers
+508 Option Chains linked into 49 Chain Headers
 +++++++++++++++++++++++++++++++++++++++++++++++++++

 +-------------------[Rule Port Counts]---------------------------------------
 |             tcp     udp    icmp      ip
-|     src       0       0       0       0
-|     dst       1       0       0       0
-|     any       0       0       1       0
+|     src     117       2       0       0
+|     dst     357       7       0       0
+|     any      25       0       1       0
 |      nc       0       0       1       0
-|     s+d       0       0       0       0
+|     s+d       0       1       0       0
 +----------------------------------------------------------------------------
```

- Taip pat įjungiu ir vienuoliktame žingsnyje išjungtą `ftp_telnet_protocol` preprocesorių:

```
--- snort-2.9.18/etc/snort.conf 2021-06-08 12:23:20.000000000 +0300
+++ /etc/snort/snort.conf       2021-07-07 18:36:16.334477803 +0300
@@ -336,10 +336,10 @@

 # FTP / Telnet normalization and anomaly detection.  For more information, see
README.ftptelnet
 preprocessor ftp_telnet: global inspection_type stateful encrypted_traffic no
check_encrypted
-preprocessor ftp_telnet_protocol: telnet \
-    ayt_attack_thresh 20 \
-    normalize ports { 23 } \
-    detect_anomalies
+# preprocessor ftp_telnet_protocol: telnet \
+#     ayt_attack_thresh 20 \
+#     normalize ports { 23 } \
+#     detect_anomalies
 preprocessor ftp_telnet_protocol: ftp server default \
     def_max_param_len 100 \
     ports { 21 2100 3535 } \

root@ldvm1:~# cat ~osboxes/debug/snort.dont-normalize-telnet.conf | patch -R
/etc/snort/snort.conf
patching file /etc/snort/snort.conf

root@ldvm1:~# snort -u snort -g snort -c /etc/snort/snort.conf -i enp0s8 -T 2>&1 |
tee ~osboxes/debug/16.Snort-selftest-ftp_telnet_protocol-enabled.txt | wc -l
488

root@ldvm1:~# diff -u ~osboxes/debug/{15,16}*.txt | colordiff | perl
/usr/share/doc/git/contrib/diff-highlight/diff-highlight
  ...
 FTPTelnet Config:
     GLOBAL CONFIG
       Inspection Type: stateful
       Check for Encrypted Traffic: YES alert: NO
       Continue to check encrypted data: YES
+    TELNET CONFIG:
+      Ports: 23
+      Are You There Threshold: 20
+      Normalize: YES
+      Detect Anomalies: YES
     FTP CONFIG:
       FTP Server: default
         Ports (PAF): 21 2100 3535
```



```
 FTPTelnet Config:
     GLOBAL CONFIG
       Inspection Type: stateful
       Check for Encrypted Traffic: YES alert: NO
       Continue to check encrypted data: YES
+    TELNET CONFIG:
+      Ports: 23
+      Are You There Threshold: 20
+      Normalize: YES
+      Detect Anomalies: YES
     FTP CONFIG:
       FTP Server: default
         Ports (PAF): 21 2100 3535
```

- `ftp_telnet_protocol` preprocesorius grąžintas.
- Deja, jokio įrašo `alert` loge Snort nesukuria
- Atkomentuoju užkomentuotas `community.rules` taisykles:

```
osboxes@ldvm1:/etc/snort$ sudo sed -i 's/^# alert/alert/' rules/community-rules/community.rules
osboxes@ldvm1:/etc/snort$ cat rules/community-rules/community.rules | grep -vc ^#
3970
osboxes@ldvm1:/etc/snort$ sudo pkill -SIGHUP snort
```

- Taisyklių skaičius paaugo nuo 508 iki 3970.
- Kartoju skenavimą su `nmap` – ir vėl jokio įrašo.
- Ieškau internete ir perkonfigūruoju preprocesorių `sfportscan` pagal How to Use Snort to detect NMAP default SYN scan? (https://stackoverflow.com/questions/52411580/how-to-use-snort-to-detect-nmap-default-syn-scan/52421369#52421369)

```
osboxes@ldvm1:/etc/snort$ sudo nano snort.conf


Use "fg" to return to nano.

[3]+  Stopped                 sudo nano snort.conf

osboxes@ldvm1:/etc/snort$ diff -u snort.conf.v3 snort.conf | colordiff
--- snort.conf.v3       2021-07-08 09:15:06.473158930 +0300
+++ snort.conf  2021-07-08 09:16:11.260650206 +0300
@@ -415,7 +415,7 @@
     xlink2state { enabled }

 # Portscan detection.  For more information, see README.sfportscan
-preprocessor sfportscan: proto  { all } memcap { 10000000 } sense_level { low }
+preprocessor sfportscan: proto  { all } memcap { 10000000 } sense_level { high }
scan_type { all } include_midstream detect_ack_scans logfile { alert }

 # ARP spoof detection.  For more information, see the Snort Manual - Configuring
Snort - Preprocessors - ARP Spoof Preprocessor
 # preprocessor arpspoof

osboxes@ldvm1:/etc/snort$ sudo pkill -SIGHUP snort
```

- Vėl skenuoju su ta pačia `nmap` komanda.

13. MySQL konfigūravimas

- įeinu į MySQL komandinį režimą:

```
osboxes@ldvm1:/etc/snort$ sudo mysql -u root -p mypass
Enter password:
ERROR 1049 (42000): Unknown database 'mypass'
```

- Iškart kliūtis:
    - `mysql` ignoruoja CLI slaptažodį;
    - `mysql` neranda DB `"mypass"`.
- Manau, kad LD aprašas pasenęs ir CLI pasikeitė. (Uždraudė slaptažodžių pateikimą per CLI kaip nesaugų)
- Pašalinsiu slaptažodį iš komandinės eilutės.

```
mysql> SET PASSWORD FOR snort@localhost=PASSWORD('mypass');
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that
corresponds to your MySQL server version for the right syntax to use near
'PASSWORD('mypass')' at line 1
mysql>
```

- Ir vėl neatitikimas. Įtariu tą patį LD aprašo pasenimą.
- Sprendžiu pagal https://stackoverflow.com/a/57718773/1025073 (https://stackoverflow.com/questions/36099028/error-1064-42000-you-have-an-error-in-your-sql-syntax-want-to-configure-a-pa/57718773#57718773)
  :

  ```
  mysql> ALTER USER snort@localhost IDENTIFIED WITH mysql_native_password BY 'mypass';
  Query OK, 0 rows affected (0.17 sec)

  mysql>
  ```

14. Snort DB importavimas

```
osboxes@ldvm1:/etc/snort$ cd /usr/local/src/snort-2.9.18/schemas
-bash: cd: /usr/local/src/snort-2.9.18/schemas: No such file or directory
```

- Tokios direktorijos nėra.
- Ieškau susijusių pavadinimų:

  ```
  osboxes@ldvm1:/etc/snort$ find /usr/local/src/snort-2.9.18 -name '*schem*'

  osboxes@ldvm1:/etc/snort$ find /usr/local/src/snort-2.9.18 -name '*sql*'
  /usr/local/src/snort-2.9.18/src/dynamic-preprocessors/appid/service_plugins/service_mysql.h
  /usr/local/src/snort-2.9.18/src/dynamic-preprocessors/appid/service_plugins/service_mysql.c
  /usr/local/src/snort-2.9.18/src/dynamic-plugins/sf_engine/examples/misc_mysql_com_table_dump.c
  /usr/local/src/snort-2.9.18/src/dynamic-plugins/sf_engine/examples/misc_mysql_com_table_dump.lo
  /usr/local/src/snort-2.9.18/src/dynamic-plugins/sf_engine/examples/misc_mysql_com_table_dump.o
  /usr/local/src/snort-2.9.18/src/dynamic-plugins/sf_engine/examples/.libs/misc_mysql_com_table_dump.o
  ```

- Tikrinu `"./configure"` skripto siūlomas galimybes:

  ```
  osboxes@ldvm1:/usr/local/src/snort-2.9.18$ ./configure --help | grep -i mysql
  osboxes@ldvm1:/usr/local/src/snort-2.9.18$ ./configure --help | grep -i sql
  osboxes@ldvm1:/usr/local/src/snort-2.9.18$ ./configure --help | grep -i sch
  ```

- Nieko bendro su MySQL neradau.
- Turiu vienintelį spėjimą pagal `"src/dynamic-preprocessors/appid/service_plugins/service_mysql.c"` failą:
  galbūt MySQL palaikymui reikalingas įjungtas OpenAppID palaikymas.
  O pastarąjį esu išjungęs kompiliatoriaus konfigūravimo fazėje.