



# M011-SEGURETAT INFORMÀTICA i ALTA SEGURETAT

***UF2- Seguretat Activa i Accés remot***

## **PRÀCTICA 6 : Detecció de Intrusos (IDS)**

**Curs:** 2018-19

**CFGS:** ASIX2

**Alumne :** Arnau Subirós Puigarnau

**Data :**

Nom i Cognoms	Data
Arnau Subirós Puigarnau	

## PRACTICA 6 :Eines i sistemes Open Source de Detecció de Intrusos (IDS)

### 1. Instal·lació i configuració de SNORT

(com a eina de detecció de connexions no desitjades.)

De les eines comentades una de les més significatives és el SNORT. Per tant, en un primer moment ens centrarem en aquesta.

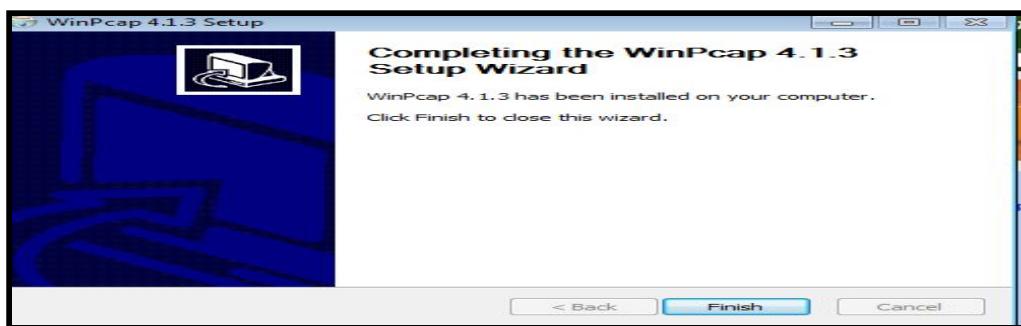
Per fer-ho podem seguir el tutorial que s'adjunta en el següent link. Feu captures de pantalla del procés que aneu seguint. En aquest link trobareu com s'ha de realitzar la instal·lació i configuració de snort i la detecció de una connexió amb Facebook. Vosaltres ho podeu provar amb alguna pàgina web que conegueu. A la realitat us hauríeu d'imaginar que tindríem una llista negra de llocs dels quals hem d'alertar si es produeixen connexions amb alguns d'aquests llocs i snort pot ajudar en aquesta tasca:

<https://www.youtube.com/watch?v=rLY1uPBBuD0>

### SNORT (Windows 7)

- ❖ En sistemes operatius Windows, primer de tot s'ha d'instal·lar **WinPcap** ([www.winpcap.org](http://www.winpcap.org))
  - ❖ **WinPcap** és l'eina estàndard per accedir a la connexió entre capes de xarxa en entorns Windows. Permet a les aplicacions capturar i transmetre els paquets de xarxa pontejant la pila de protocols; i té útils característiques addicionals que inclouen el filtrat de paquets a nivell del nucli, un motor de generació d'estadístiques de xarxa i suport per a captura de paquets WinPcap consisteix en un controlador, que estén el sistema operatiu per a proveir accés de xarxa a baix nivell, i una biblioteca que s'usa per a accedir fàcilment a les capes de xarxa de baix nivell

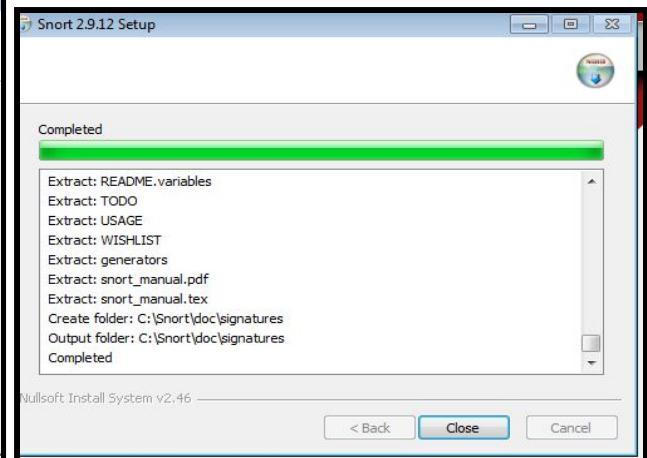
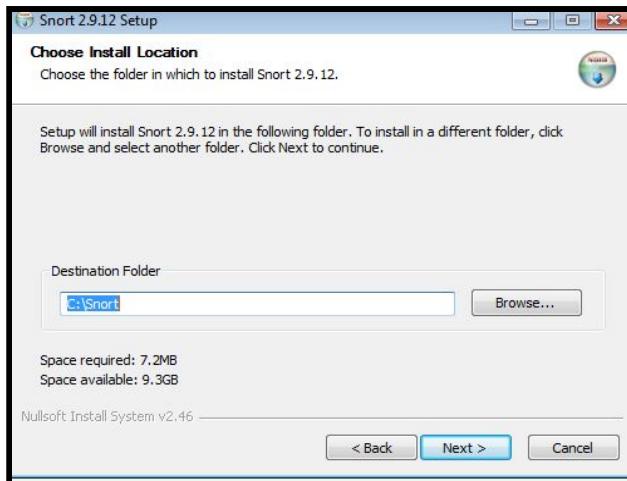
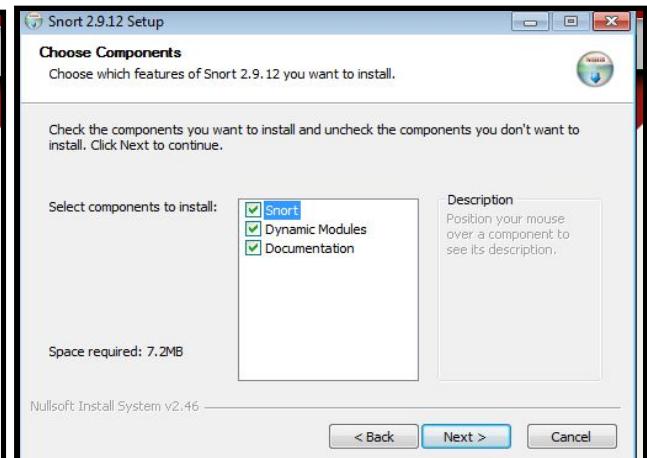
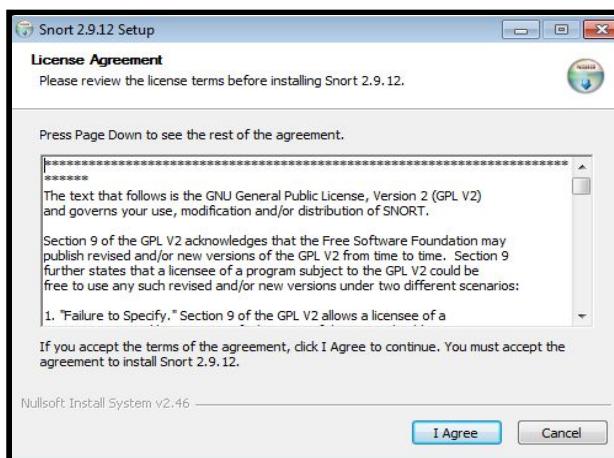
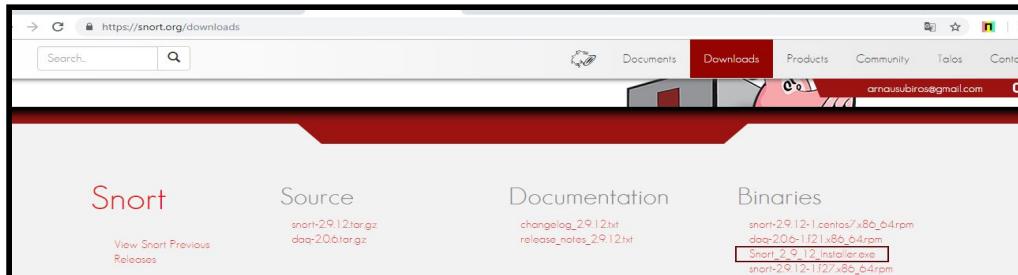
Nom i Cognoms	Data
Arnau Subirós Puigarnau	



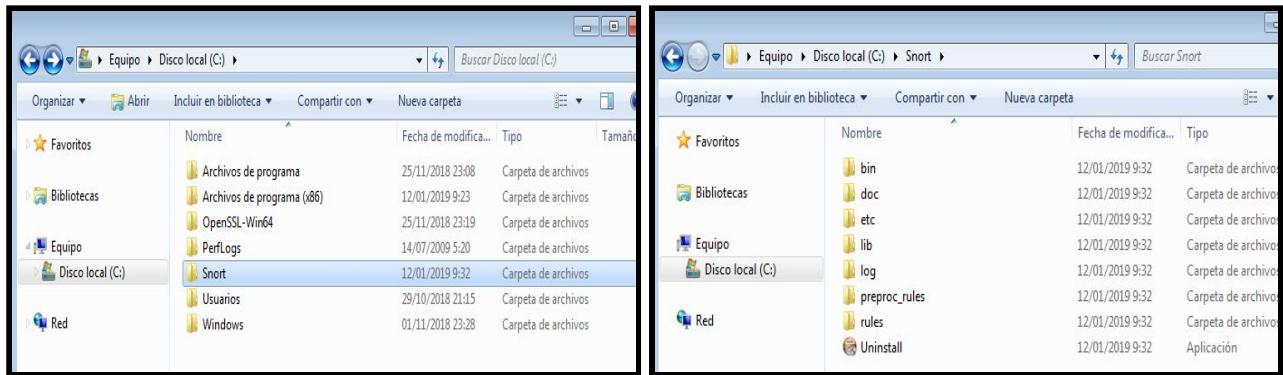
Nom i Cognoms	Data
---------------	------

Arnau Subirós Puigarnau

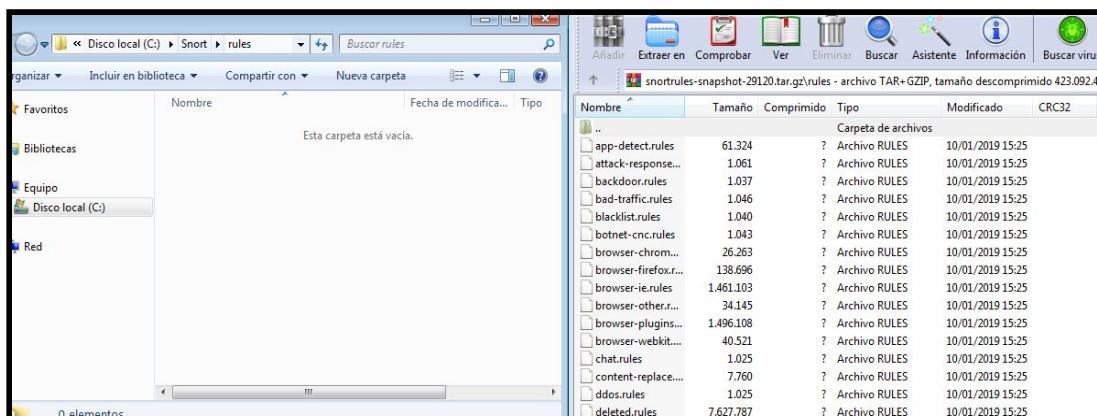
- ❖ Ens descarguem e instal.lem **SNORT** ([www.snort.org](http://www.snort.org))



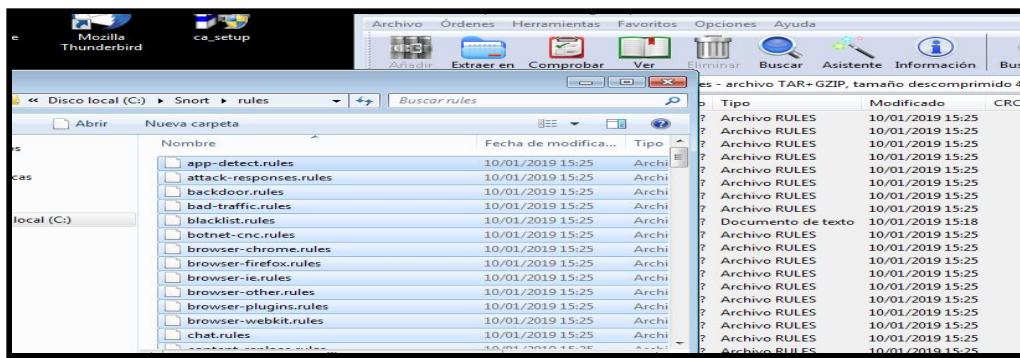
Nom i Cognoms	Data
Arnau Subirós Puigarnau	



- ❖ Durant la instal·lació de Snort crea una estructura de directoris en C:\Snort :
  - C:\snort\bin directori on es troba l'executable de l'eina
  - C:\snort\contrib
  - C:\snort\doc documentació de l'eina
  - C:\snort\etc directori principal per als arxius de configuració
  - C:\snort\log
  - C:\snort\rules jocs de regles ( al descargar SNORT la carpeta està buida, per això ens hem de descargar-les després)
- ❖ El primer que hem de fer és accedir a la carpeta C:\Snort\etc en aquest directori trobarem un fitxer anomenat snort.conf, que és el fitxer de configuració que utilitzarem per a configurar Snort. Accedim al fitxer amb un editor de text que no corrompi el format original de l'arxiu (per exemple notepad++)
- ❖ Ens hem de descargar les regles i hem de sobreescrivir a les carpetes corresponents..Després de descomprimir l'arxiu "regles" (rules) copiarem al contingut a les corresponents carpetes : "rules" i preproc\_rules"



Nom i Cognoms	Data
Arnau Subirós Puigarnau	

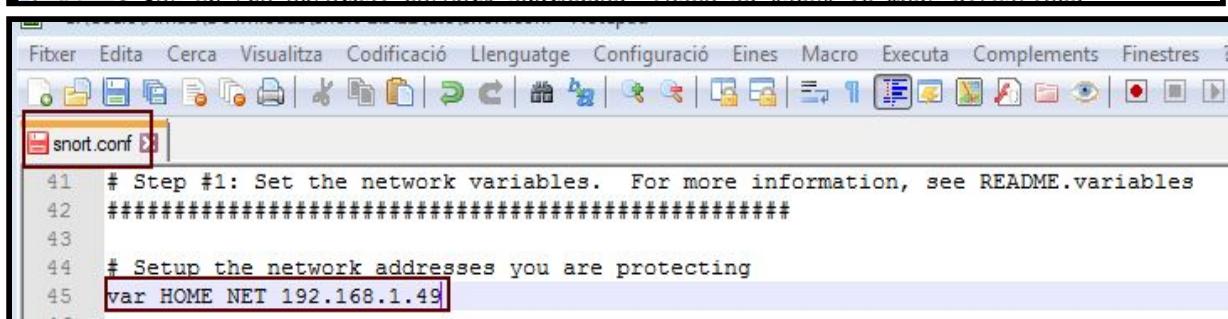
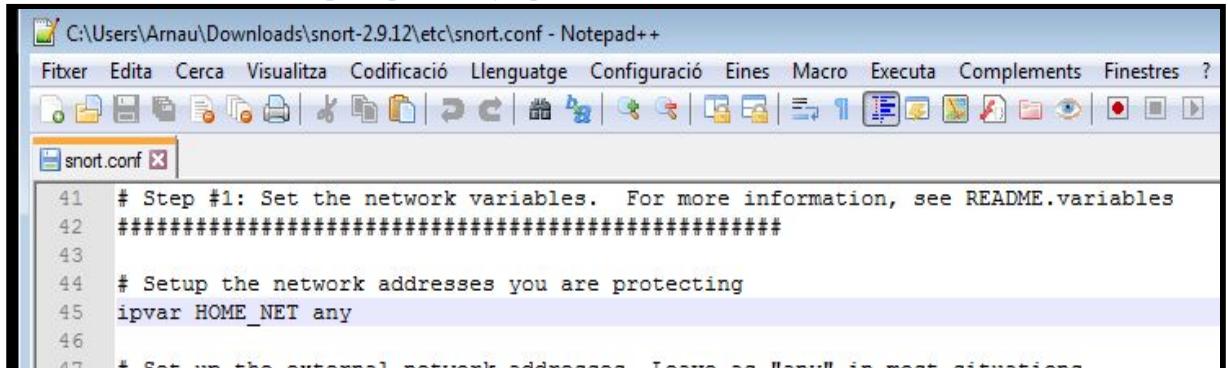


- ❖ Anirem al directori a on està instal·lat SNORT per editar l'arxiu de configuració amb notepad++.  
**En el meu cas c:\Snort\etc\snort.conf**

## **STEPS de l'arxiu SNORT.CONF**

## **STEP 1**

➤ Cambiem **ipvar** per **var** ( ja que ivar s'utilitza al linux i en el nostre cas farem servir Windows)



Nom i Cognoms	Data
Arnau Subirós Puigarnau	

```

46
47 # Set up the external network addresses. Leave as "any" in most situations
48 ipvar EXTERNAL_NET any
49

```

```

50
51 # Set up the external network addresses. Leave as "any" in most situations
52 var EXTERNAL_NET !$HOME_NET
53

```

➤ Comentem la regla so\_rule\_path ( no s'utiliza en Windows)

```

01 # Path to your rules files (this can be a relative path)
02 # Note for Windows users: You are advised to make this an absolute path,
03 # such as: c:\snort\rules
04 var RULE_PATH ../rules
05 var SO_RULE_PATH ../so_rules
06 var PREPROC_RULE_PATH ../preproc_rules
07

```

```

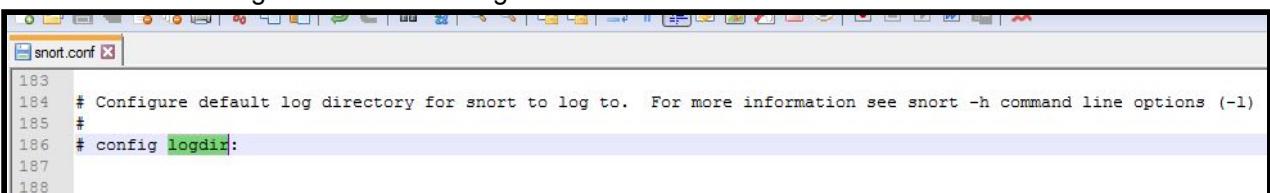
# Path to your rules files (this can be a relative path)
# Note for Windows users: You are advised to make this an absolute path,
# such as: c:\snort\rules
var RULE_PATH c:\snort\rules
var SO_RULE_PATH ../so_rules
var PREPROC_RULE_PATH c:\snort\rules\preproc_rules

# If you are using reputation preprocessor set these
# Currently there is a bug with relative paths, they are relative to where snort is
# not relative to snort.conf like the above variables
# This is completely inconsistent with how other vars work, BUG 89986
# Set the absolute path appropriately
var WHITE_LIST_PATH c:\snort\rules
var BLACK_LIST_PATH c:\snort\rules

```

## STEP 2

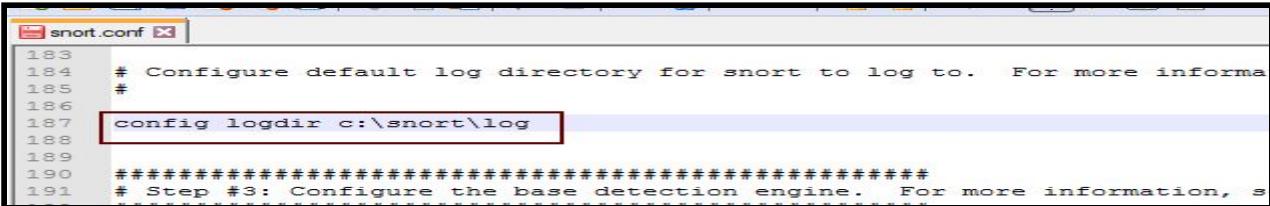
➤ Configurem la ruta dels logs de Snort



```

snort.conf
183
184 # Configure default log directory for snort to log to. For more information see snort -h command line options (-l)
185 #
186 # config logdir:
187
188
189
190
191

```



```

snort.conf
183
184 # Configure default log directory for snort to log to. For more information see snort -h command line options (-l)
185 #
186 config logdir c:\snort\log
187
188
189
190 #####
191 # Step #3: Configure the base detection engine. For more information, see snort(1) man page

```

Nom i Cognoms	Data
Arnau Subirós Puigarnau	

### **STEP 3 ( no fer res)**

- Comentem la regla so\_rule\_path ( no s'utiliza en Windows)

### **STEP 4 ( no fer res)**

- Aquí es configuren algunes llibreries que Snort carga quan arranca

```

241 #####
242 # Step #4: Configure dynamic loaded libraries.
243 # For more information, see Snort Manual, Configuring Snort - Dynamic Modules
244 #####
245
246 # path to dynamic preprocessor libraries
247 dynamicpreprocessor directory /usr/local/lib/snort_dynamicpreprocessor/
248
249 # path to base preprocessor engine
250 dynamicengine /usr/local/lib/snort_dynamicengine/libsf_engine.so
251
252 # path to dynamic rules libraries
253 dynamicdetection directory /usr/local/lib/snort_dynamicrules
254
255

```

- Cambiarem la configuració de les rutes ja que per defecte son configurades per Linux i s'han de modificar per Windows i el nom dels fitxers també cambien

```

#####
# Step #4: Configure dynamic loaded libraries.
# For more information, see Snort Manual, Configuring Snort - Dynamic Module
#####

# path to dynamic preprocessor libraries
dynamicpreprocessor directory c:\snort\lib\snort_dynamicpreprocessor

# path to base preprocessor engine
dynamicengine c:\snort\lib\snort_dynamicpreprocessor

# path to dynamic rules libraries
#dynamicdetection directory /usr/local/lib/snort_dynamicrules

```

### **STEP 5**

- Deixarem comentades totes les línies de "inline preprocessors" (ja que Windows, els preprocessors, no s'executen en la manera "in line. Aquesta és una característica limitada a Linux i Unix, i no hi ha raó de deixar-les en execució):

Nom i Cognoms	Data
Arnau Subirós Puigarnau	

```

6 #####
7 # Step #5: Configure preprocessors
8 # For more information, see the Snort Manual, Configuring Snort - Preproce
9 #####
10
11 # GTP Control Channle Preprocessor. For more information, see README.GTP
12 # processor gtp: ports { 2123 3386 2152 }

13
14 # Inline packet normalization. For more information, see README.normalize
15 # Does nothing in IDS mode
16 processor normalize_ip4
17 processor normalize_tcp: ips ecn stream
18 processor normalize_icmp4
19 processor normalize_ip6
20 processor normalize_icmp6

21
22 # Target-based IP defragmentation. For more inforation, see README.frag3

```

```

23
24 # Inline packet normalization. For more information, see README.normalize
25 # Does nothing in IDS mode
26 #processor normalize_ip4
27 #processor normalize_tcp: ips ecn stream
28 #processor normalize_icmp4
29 #processor normalize_ip6
30 #processor normalize_icmp6

```

- Deixarem comentada una altre línia

```

processor rpc_decode: 111

# Back Orifice detection.
processor bo

```

```

334
335 # Back Orifice detection.
336 #processor bo
337

```

Nom i Cognoms	Data
Arnau Subirós Puigarnau	

- S'activarà alerta escaneig de ports (la línia de codi estava comentada)

```

15      valid_cmds { X-EXPS X-LINK2STATE XADR XAUTH XCIR XEXCH50 XGEN XLICENSE XQUE XSI
16      xlink2state { enabled }
17
18  # Portscan detection. For more information, see README.sfportscan
19  # preprocessor sfportscan: proto { all } memcap { 10000000 } sense_level { low }
20

```

```

# Portscan detection. For more information, see README.sfportscan
preprocessor sfportscan: proto { all } memcap { 10000000 } sense_level { low }

```

- Revisem que els següents arxius que estiguin activats , s'ha de crear la carpeta rules.

```

# 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

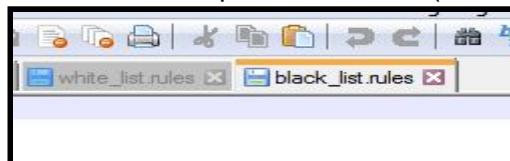
```

```

55     check_CRC
56
57  # Reputation preprocessor. For more information see README.reputation
58  preprocessor reputation: \
59      memcap 500, \
60      priority whitelist, \
61      nested_ip inner, \
62      whitelist $WHITE_LIST_PATH\white_list, \
63      blacklist $BLACK_LIST_PATH\black_list

```

- Tindrem que crear l' arxius( black\_list.rules and white\_list.rules a c:\Snort\rules



Nom i Cognoms	Data
Arnau Subirós Puigarnau	

### STEP 6 ( no fer res, només per Linux)

#### STEP 7

- Descomentarem les línies per activar les regles
- si us es el set de regles “community” (regles que obtens sense registrar-te en la web de snort), has de deixar aquestes línies comentades! I crear un include per a activar les regles community.
- (Cambiamos: / utilitzat en Linux per: \ en las rutas ja que fem servir Windows ).

```

39 ######
40 # Step #7: Customize your rule set
41 # For more information, see Snort Manual, Writing Snort Rules
42 #
43 # NOTE: All categories are enabled in this conf file
44 #####
45
46 # site specific rules
47 include $RULE_PATH/local.rules
48
49 include $RULE_PATH/app-detect.rules
50 include $RULE_PATH/attack-responses.rules
51 include $RULE_PATH/backdoor.rules
52 include $RULE_PATH/bad-traffic.rules
53 include $RULE_PATH/blacklist.rules
54 include $RULE_PATH/botnet-cnc.rules
55 include $RULE_PATH/browser-chrome.rules
56 include $RULE_PATH/browser-firefox.rules
57 include $RULE_PATH/browser-ie.rules
58 include $RULE_PATH/browser-other.rules
59 include $RULE_PATH/browser-plugins.rules
60 include $RULE_PATH/browser-webkit.rules
61 include $RULE_PATH/chat.rules
62 include $RULE_PATH/content-replace.rules
63 include $RULE_PATH/ddos.rules
64 include $RULE_PATH/dns.rules
65 include $RULE_PATH/dos.rules

```

```

5 # site specific rules
6 include $RULE_PATH\local.rules
7
8 include $RULE_PATH\app-detect.rules
9 include $RULE_PATH\attack-responses.rules
10 include $RULE_PATH\backdoor.rules
11 include $RULE_PATH\bad-traffic.rules
12 include $RULE_PATH\blacklist.rules
13 include $RULE_PATH\botnet-cnc.rules
14 include $RULE_PATH\brower-chrome.rules
15 include $RULE_PATH\brower-firefox.rules
16 include $RULE_PATH\brower-ie.rules
17 include $RULE_PATH\brower-other.rules
18 include $RULE_PATH\brower-plugins.rules
19 include $RULE_PATH\brower-webkit.rules
20 include $RULE_PATH\chat.rules
21 include $RULE_PATH\content-replace.rules
22 include $RULE_PATH\dos.rules
23 include $RULE_PATH\dns.rules
24 include $RULE_PATH\dos.rules
25 include $RULE_PATH\experimental.rules
26 include $RULE_PATH\exploit-kit.rules
27 include $RULE_PATH\exploit.rules
28 include $RULE_PATH\file-executable.rules
29 !!!

```

Nom i Cognoms	Data
Arnau Subirós Puigarnau	

### STEP 8

- s'activaran els següents preprocessors

```

653
654 ##### Step #8: Customize your preprocessor and decoder alerts #####
655 # Step #8: Customize your preprocessor and decoder alerts
656 # For more information, see README.decoder_preproc_rules
657 #####
658
659 # decoder and preprocessor event rules
660 # include $PREPROC_RULE_PATH/preprocessor.rules
661 # include $PREPROC_RULE_PATH/decoder.rules
662 # include $PREPROC_RULE_PATH/sensitive-data.rules
663

```

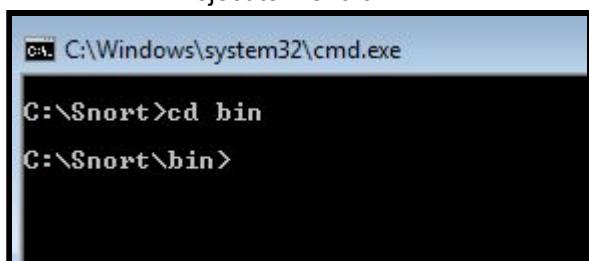
  

```

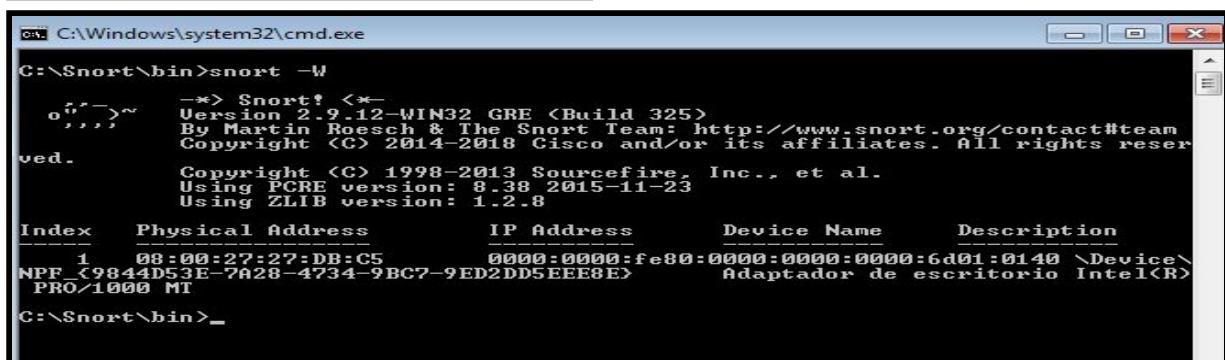
# decoder and preprocessor event rules
include $PREPROC_RULE_PATH/preprocessor.rules
include $PREPROC_RULE_PATH/decoder.rules
include $PREPROC_RULE_PATH/sensitive-data.rules

```

- Ja haurem configurat el **IDS Snort**. Ara hem de fer un TEST
  - Obrirem el CMD( mode administrador)
  - seleccionem la carpeta bin del programa Snort
  - ejecutem snort -w



C:\Windows\system32\cmd.exe  
C:\Snort>cd bin  
C:\Snort\bin>



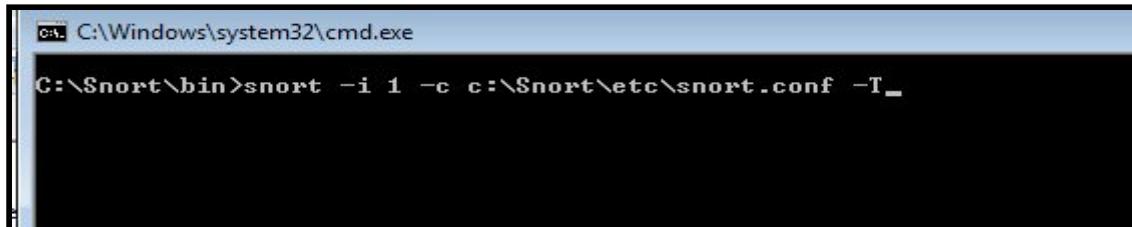
```

C:\Windows\system32\cmd.exe
C:\Snort\bin>snort -W
--> Snort! <--
Version 2.9.12-WIN32 GRE <Build 325>
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright <C> 2014-2018 Cisco and/or its affiliates. All rights reserved.
Copyright <C> 1998-2013 Sourcefire, Inc., et al.
Using PCRE version: 8.38 2015-11-23
Using ZLIB version: 1.2.8
Index Physical Address IP Address Device Name Description
1 08:00:27:27:DB:C5 0000:0000:fe80:0000:0000:6d01:0140 \Device\NPF_{9844D53E-7A28-4734-9BC7-9ED2DD5EEE8E} Adaptador de escritorio Intel(R) PRO/1000 MT
C:\Snort\bin>

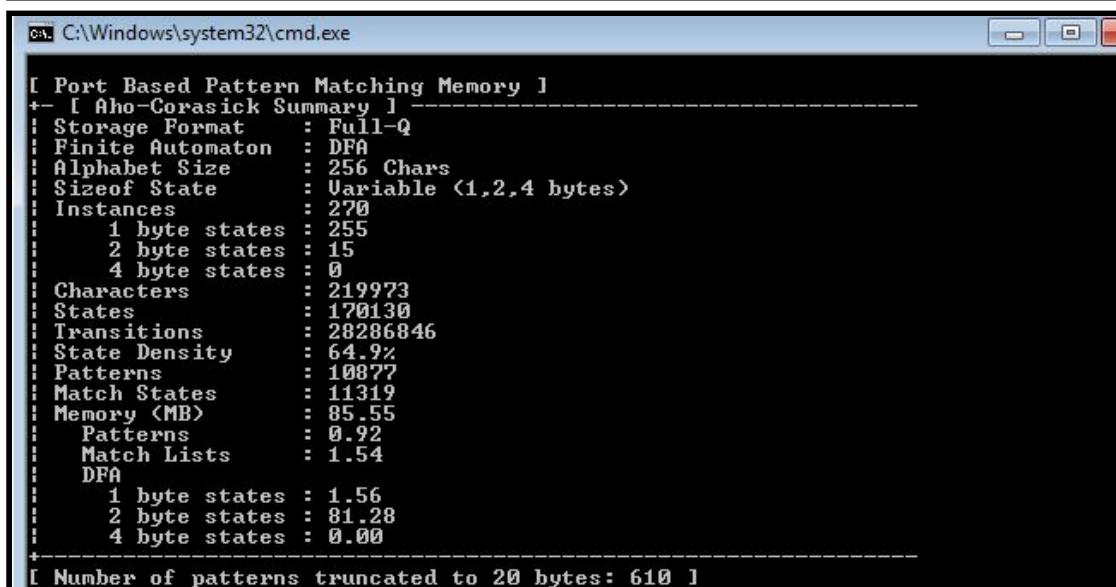
```

Nom i Cognoms	Data
Arnau Subirós Puigarnau	

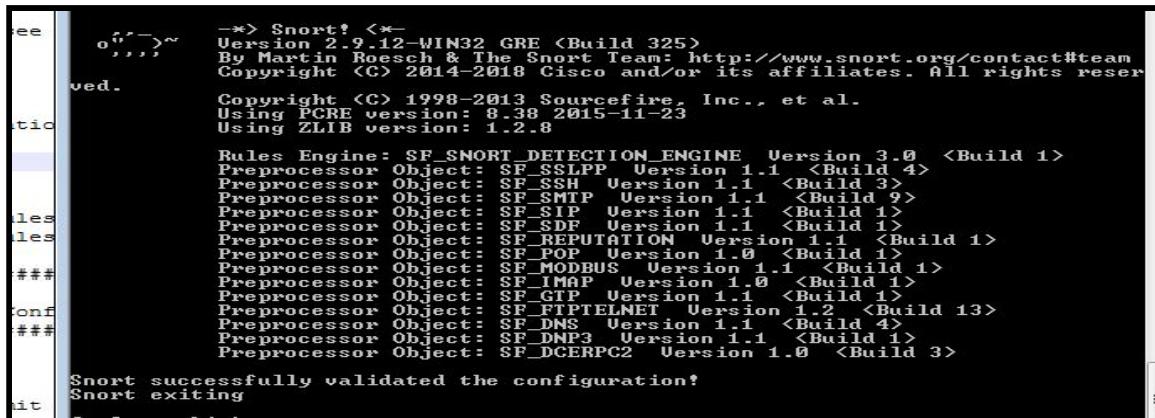
- Ara hem de verificar que tenim un configuració red vàlida



```
C:\Windows\system32\cmd.exe
C:\Snort\bin>snort -i 1 -c c:\Snort\etc\snort.conf -T
```



```
[ 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           : 270
|   1 byte states    : 255
|   2 byte states    : 15
|   4 byte states    : 0
| Characters          : 219973
| States              : 170130
| Transitions         : 28286846
| State Density       : 64.9%
| Patterns            : 10877
| Match States        : 11319
| Memory (MB)         : 85.55
| Patterns            : 0.92
| Match Lists          : 1.54
| DFA
|   1 byte states    : 1.56
|   2 byte states    : 81.28
|   4 byte states    : 0.00
+-
[ Number of patterns truncated to 20 bytes: 610 ]
```



```
--> Snort! <-- Version 2.9.12-WIN32 GRE <Build 325>
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright <C> 2014-2018 Cisco and/or its affiliates. All rights reserved.

Copyright <C> 1998-2013 Sourcefire, Inc., et al.
Using PCRE version: 8.38 2015-11-23
Using ZLIB version: 1.2.8

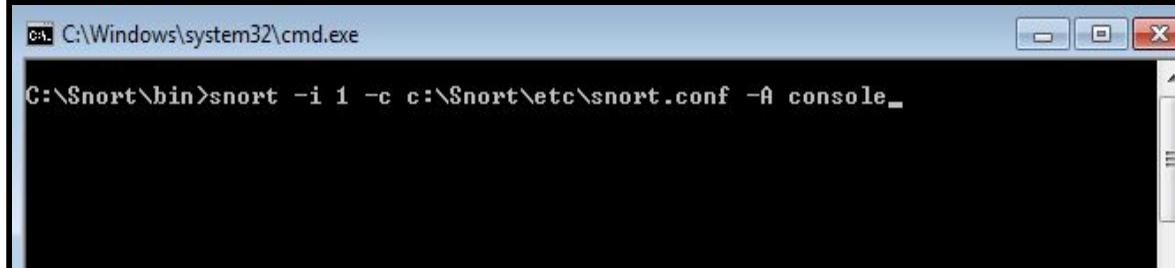
Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.0 <Build 1>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_SDF Version 1.1 <Build 1>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_FPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>

Snort successfully validated the configuration!
Snort exiting
```

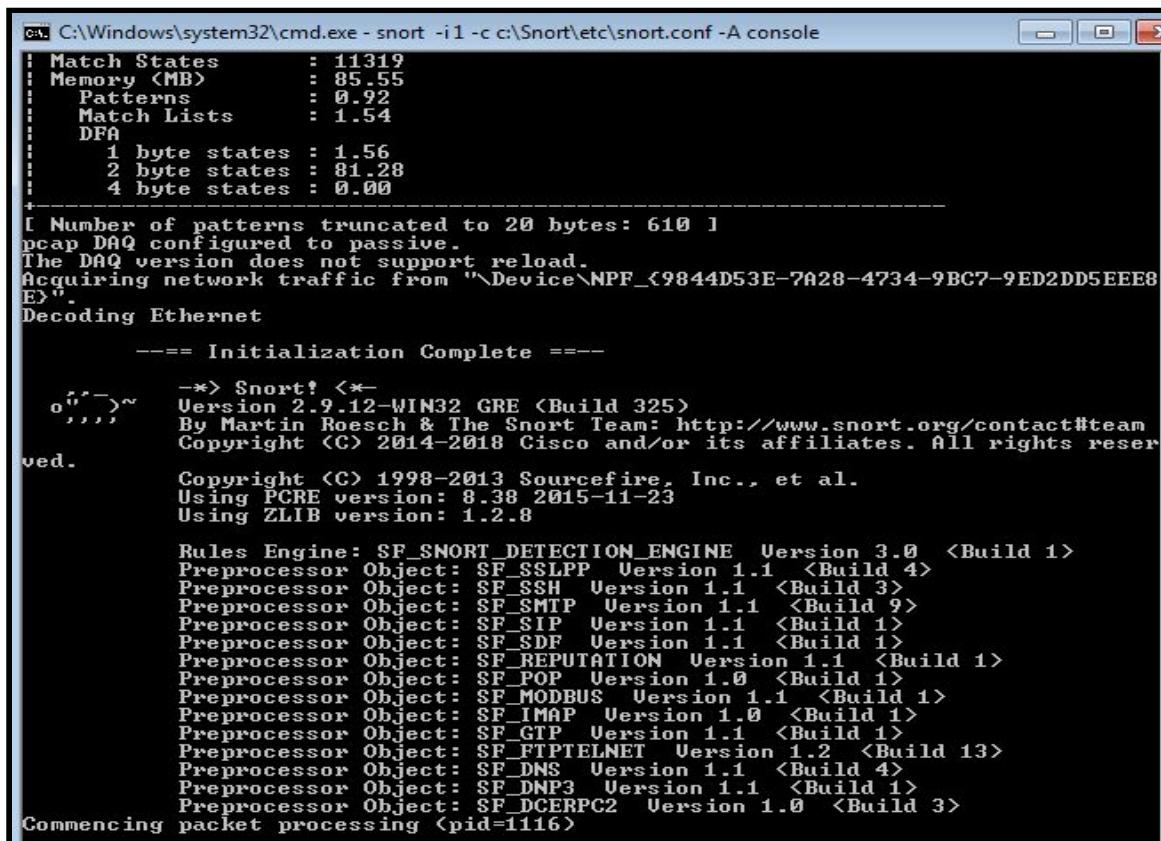
Nom i Cognoms	Data
Arnau Subirós Puigarnau	

- Ara ens toca activar el IDS, per posar-lo en funcionament escriurem :

➤ C:\Snort\bin> snort -i 1 -c c:\Snort\etc\snort.conf -A console



```
C:\Windows\system32\cmd.exe
C:\Snort\bin>snort -i 1 -c c:\Snort\etc\snort.conf -A console
```



```
C:\Windows\system32\cmd.exe - snort -i 1 -c c:\Snort\etc\snort.conf -A console
Match States      : 11319
Memory (MB)       : 85.55
Patterns          : 0.92
Match Lists        : 1.54
DFA
  1 byte states : 1.56
  2 byte states : 81.28
  4 byte states : 0.00
+
[ Number of patterns truncated to 20 bytes: 610 ]
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "\Device\NPF_{9844D53E-7A28-4734-9BC7-9ED2DD5EEE8E}".
Decoding Ethernet
    === Initialization Complete ===
-> Snort! <-
o,,,,>~ Version 2.9.12-WIN32 GRE <Build 325>
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2018 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using PCRE version: 8.38 2015-11-23
Using ZLIB version: 1.2.8

Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.0 <Build 1>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_SDF Version 1.1 <Build 1>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>

Commencing packet processing (pid=1116)
```

Nom i Cognoms	Data
Arnau Subirós Puigarnau	

- **CTRL+C** per sortir de Snort, abans ens sortirà per pantalla el seu anàlisis

```
C:\Windows\system32\cmd.exe
*** Caught Int-Signal
=====
Run time for packet processing was 1144.120000 seconds
Snort processed 7052702 packets.
Snort ran for 0 days 0 hours 19 minutes 4 seconds
Pkts/min: 371194
Pkts/sec: 6164
=====
Packet I/O Totals:
Received: 7088260
Analyzed: 7052702 ( 99.498%)
Dropped: 34973 ( 0.491%)
Filtered: 0 ( 0.000%)
Outstanding: 35558 ( 0.502%)
Injected: 0
=====
```

```
C:\Windows\system32\cmd.exe
=====
dcerpc2 Preprocessor Statistics
Total sessions: 0
=====
SSL Preprocessor:
SSL packets decoded: 1092
Client Hello: 0
Server Hello: 217
Certificate: 190
Server Done: 322
Client Key Exchange: 0
Server Key Exchange: 168
Change Cipher: 220
Finished: 0
Client Application: 65
Server Application: 197
Alert: 0
Unrecognized records: 462
Completed handshakes: 0
Bad handshakes: 20
Sessions ignored: 103
Detection disabled: 66
=====
SIP Preprocessor Statistics
Total sessions: 0
=====
Reputation Preprocessor Statistics
Total Memory Allocated: 0
=====
Snort exiting
```

Nom i Cognoms	Data
Arnau Subirós Puigarnau	

## SNORT (Kali Linux)

A continuació es mostraran les captures de la instal.lació de Snort on es pot veure que el procés més ràpid ja que està configurat per sistemes Unix/Linux i perquè funcioni amb Windows s'ha de fer varie modificacions adicionals i instal.lar un altre software.

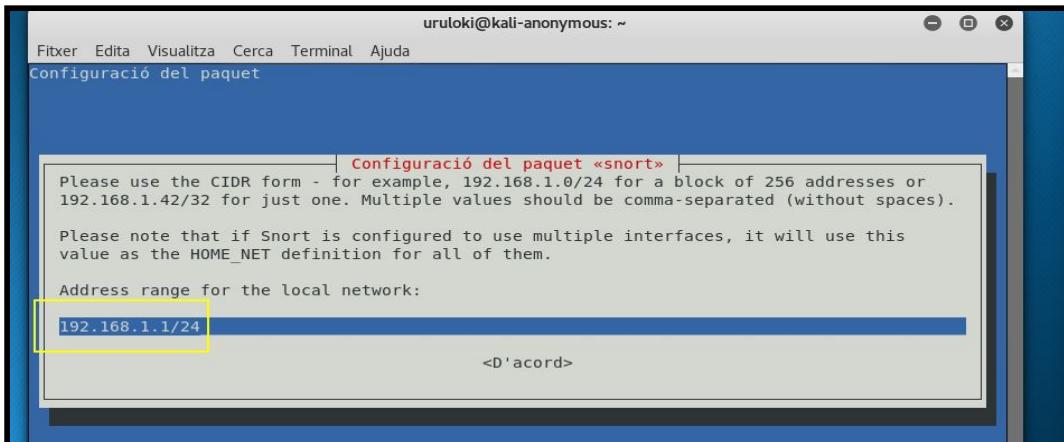
```
uruloki@kali-anonymous:~$ sudo apt-get install snort
S'està llegint la llista de paquets... Fet
S'està construint l'arbre de dependències
S'està llegint la informació de l'estat... Fet
S'instal·laran els següents paquets extres:
  libdaq2 oinkmaster snort-common snort-common-libraries snort-rules-default
Paquets suggerits:
  snort-doc
S'instal·laran els paquets NOUS següents:
  libdaq2 oinkmaster snort snort-common snort-common-libraries snort-rules-default
0 actualitzats, 6 nous a instal·lar, 0 a suprimir i 1625 no actualitzats.
S'ha d'obtenir 2230 kB d'arxius.
Després d'aquesta operació s'empraran 7325 kB d'espai en disc addicional.
Voleu continuar? [S/n]
```

Revisem la IP de la gateway de l'ordinador físic

The screenshot shows a terminal window with the title "Configuració del paquet". The window contains the following text:

```
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  
  
<D'acord>
```

Nom i Cognoms	Data
Arnau Subirós Puigarnau	



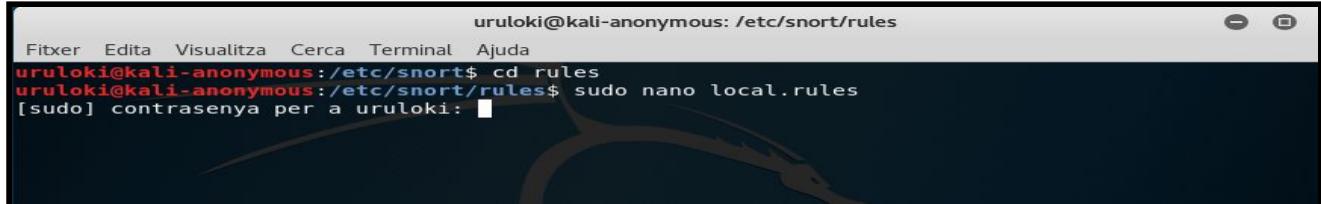
```
uruloki@kali-anonymous: ~
Fitxer Edita Visualitza Cerca Terminal Ajuda
S'està preparant per a desempaquetar .../2-snort-rules-default_2.9.7.0-5_all.deb...
S'està desempaquetant snort-rules-default (2.9.7.0-5)...
S'està seleccionant el paquet snort-common prèviament no seleccionat.
S'està preparant per a desempaquetar .../3-snort-common_2.9.7.0-5_all.deb...
S'està desempaquetant snort-common (2.9.7.0-5)...
S'està seleccionant el paquet snort prèviament no seleccionat.
S'està preparant per a desempaquetar .../4-snort_2.9.7.0-5_amd64.deb...
S'està desempaquetant snort (2.9.7.0-5)...
S'està seleccionant el paquet oinkmaster prèviament no seleccionat.
S'està preparant per a desempaquetar .../5-oinkmaster_2.0-4_all.deb...
S'està desempaquetant oinkmaster (2.0-4)...
S'està configurant oinkmaster (2.0-4)...
S'està configurant snort-common (2.9.7.0-5)...
S'està configurant snort-rules-default (2.9.7.0-5)...
S'està configurant libdaq2 (2.0.4-3+b1)...
S'estan processant els activadors per a libc-bin (2.27-5)...
S'estan processant els activadors per a systemd (239-7)...
S'estan processant els activadors per a man-db (2.8.3-2)...
S'està configurant snort-common-libraries (2.9.7.0-5)...
S'està configurant snort (2.9.7.0-5)...
update-rc.d: We have no instructions for the snort init script.
update-rc.d: It looks like a network service, we disable it.
S'estan processant els activadors per a systemd (239-7)...
uruloki@kali-anonymous: ~
```

**IMPORTANT!!!** la instal.lació s'ha fet a la red de casa on la gateway es 192.168.1.1. Un cop instal.lat i donat el cas que estic a una altre red( la de l'escola on la seva gateway és 172.20.23.254, hauriem de reconfigurar amb el comando

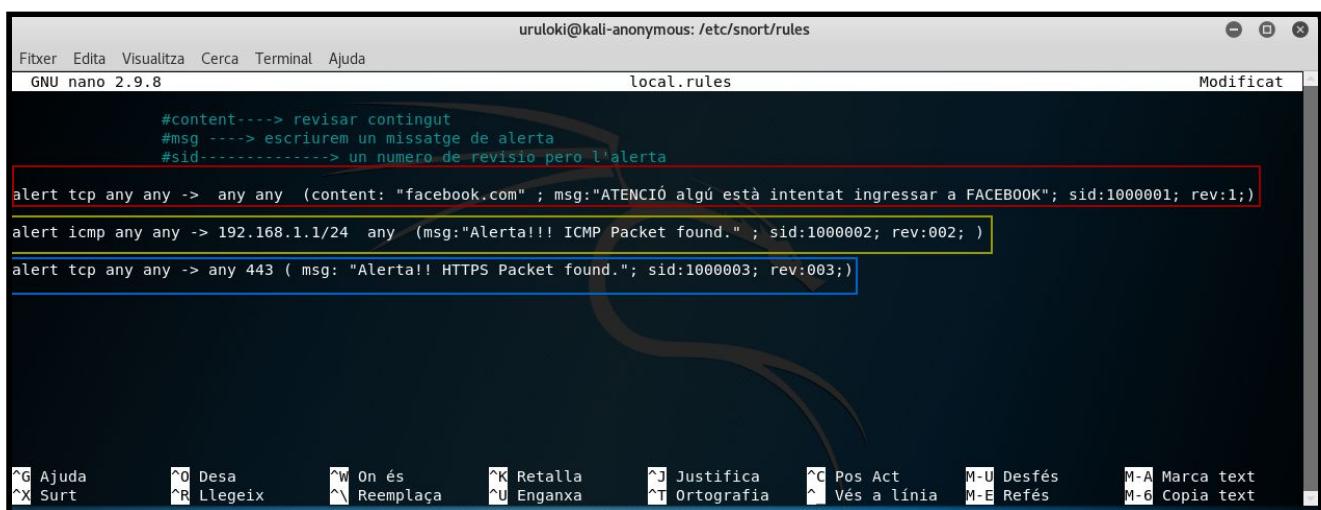
```
uruloki@kali-anonymous: /etc/snort
Fitxer Edita Visualitza Cerca Terminal Ajuda
uruloki@kali-anonymous:/etc/snort$ sudo dpkg-reconfigure snort
```

Nom i Cognoms	Data
Arnau Subirós Puigarnau	

Accedirem a la carpeta **rules** i crearem 3 alertes a l'arxiu **local.rules**



```
uruloki@kali-anonymous: /etc/snort/rules
Fitxer Edita Visualitza Cerca Terminal Ajuda
uruloki@kali-anonymous: /etc/snort$ cd rules
uruloki@kali-anonymous: /etc/snort/rules$ sudo nano local.rules
[sudo] contrasenya per a uruloki: ■
```

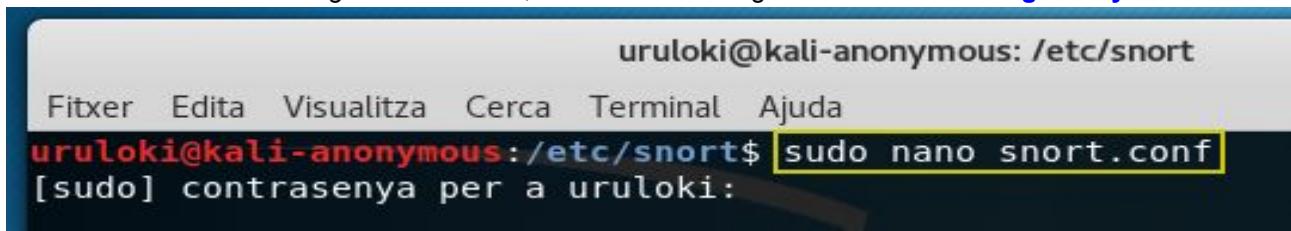


```
uruloki@kali-anonymous: /etc/snort/rules
Fitxer Edita Visualitza Cerca Terminal Ajuda
GNU nano 2.9.8 local.rules Modificat
#content----> revisar contingut
#msg ----> escriurem un missatge de alerta
#sid-----> un numero de revisio pero l'alerta
alert tcp any any -> any any (content: "facebook.com" ; msg:"ATENCIÓ algú està intentat ingressar a FACEBOOK"; sid:1000001; rev:1;)
alert icmp any any -> 192.168.1.1/24 any (msg:"Alerta!!! ICMP Packet found." ; sid:1000002; rev:002; )
alert tcp any any -> any 443 ( msg: "Alerta!! HTTPS Packet found."; sid:1000003; rev:003;)
```

Keyboard shortcuts at the bottom:

- G Ajuda
- X Surt
- ^O Desa
- ^R Llegeix
- ^W On és
- ^K Retalla
- ^U Enganxa
- ^J Justifica
- ^C Pos Act
- M-U Desfés
- M-E Refés
- M-A Marca text
- M-6 Copia text

Accedirem a l'arxiu de configuració de Snort, **snort.conf** on afegirem la **IP del nostre gateway**



```
uruloki@kali-anonymous: /etc/snort
Fitxer Edita Visualitza Cerca Terminal Ajuda
uruloki@kali-anonymous: /etc/snort$ sudo nano snort.conf
[sudo] contrasenya per a uruloki: ■
```

Nom i Cognoms	Data
Arnau Subirós Puigarnau	

uruloki@kali-anonymous: /etc/snort

```

Fitxer Edita Visualitza Cerca Terminal Ajuda
GNU nano 2.9.8                                         snort.conf

# 9) Customize shared object rule set; SF GTP Version 1.1 <Build 1>
#####
# Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
#####
# Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>
#####
# Step #1: Set the network variables. For more information, see README.variables
#####
# Commencing packet processing (pid=2835)
# Setup the network addresses you are protecting:3] Alerta!! HTTPS Packet found. [**] [Pr
# 01/15-00:47:52.387773 [**] [1:1000003:3] Alerta!! HTTPS Packet found. [**] [Pr
# Note to Debian users: this value is overriden when starting HTTPS Packet found. [**] [Pr
# up the Snort daemon through the init.d script by the
# value of $DEBIAN_SNORT_HOME_NET is defined in the 3] Alerta!! HTTPS Packet found. [**] [Pr
# /etc/snort/snort.debian configuration file 3] Alerta!! HTTPS Packet found. [**] [Pr
# 01/15-00:48:11.152339 [**] [1:1000001:1] ATENCIÓ algú està intentat ingressar
ipvar HOME_NET 192.168.1.1/24
01/15-00:48:11.152339 [**] [1:1000001:1] ATENCIÓ algú està intentat ingressar

```

uruloki@kali-anonymous: /etc/snort

```

Fitxer Edita Visualitza Cerca Terminal Ajuda
uruloki@kali-anonymous:/etc/snort$ sudo snort -c snort.conf -A console -i eth1 | more
Running in IDS mode
--== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "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 7000:700
1 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 9090:9
091 9443 9999 11371 34443:34444 41080 50002 55555 ]
PortVar 'HELLCODE_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 9090:9
091 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

```

Nom i Cognoms	Data
---------------	------

Arnau Subirós Puigarnau

```

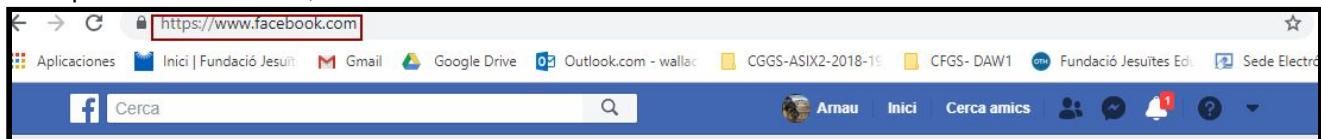
Fitxer Edita Visualitza Cerca Terminal Ajuda
--- Initialization Complete ---
o" ,--> Snort! <--*
Version 2.9.7.0 GRE (Build 149)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.8.1
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_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_SSLLP Version 1.1 <Build 4>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: SF_SDF Version 1.1 <Build 1>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Commencing packet processing (pid=5216)

```

## PROVES amb l'IDS SNORT

Un cop tenim activat l'IDS, accedim al facebook.



S'han activat 2 alertes : que estan accedint a una conexió https(port 443) i s'està ingressant al facebook

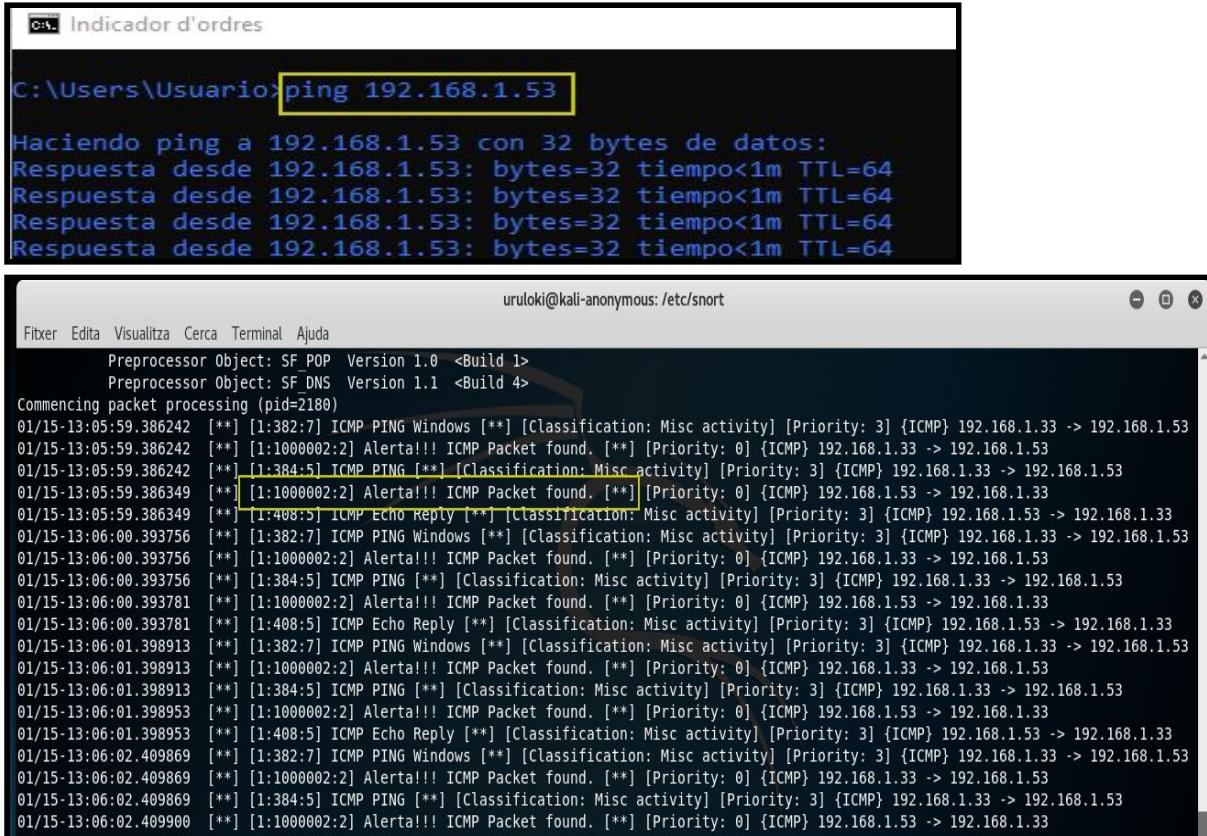
```

Commencing packet processing (pid=2835)
01/15-00:47:52.381388 [**] [1:1000003:3] Alerta!! HTTPS Packet found. [**] [Priority: 0] {TCP} 192.168.1.53:34856 -> 31.13.83.8:443
01/15-00:47:52.387773 [**] [1:1000003:3] Alerta!! HTTPS Packet found. [**] [Priority: 0] {TCP} 192.168.1.53:54076 -> 31.13.83.36:443
01/15-00:47:52.387787 [**] [1:1000003:3] Alerta!! HTTPS Packet found. [**] [Priority: 0] {TCP} 192.168.1.53:54076 -> 31.13.83.36:443
01/15-00:47:52.387793 [**] [1:1000003:3] Alerta!! HTTPS Packet found. [**] [Priority: 0] {TCP} 192.168.1.53:54076 -> 31.13.83.36:443
01/15-00:47:52.393409 [**] [1:1000003:3] Alerta!! HTTPS Packet found. [**] [Priority: 0] {TCP} 192.168.1.53:34856 -> 31.13.83.8:443
01/15-00:47:52.456150 [**] [1:1000003:3] Alerta!! HTTPS Packet found. [**] [Priority: 0] {TCP} 192.168.1.53:34838 -> 31.13.83.8:443
01/15-00:48:11.129958 [**] [1:1000001:1] ATENCIÓ algú està intentat ingressar a FACEBOOK [**] [Priority: 0] {TCP} 31.13.83.36:443 -> 192.168.1.53:146
01/15-00:48:11.152339 [**] [1:1000001:1] ATENCIÓ algú està intentat ingressar a FACEBOOK [**] [Priority: 0] {TCP} 31.13.83.36:443 -> 192.168.1.53:148
01/15-00:48:11.414994 [**] [1:1000001:1] ATENCIÓ algú està intentat ingressar a FACEBOOK [**] [Priority: 0] {TCP} 31.13.83.4:443 -> 192.168.1.53:638
01/15-00:48:11.415946 [**] [1:1000001:1] ATENCIÓ algú està intentat ingressar a FACEBOOK [**] [Priority: 0] {TCP} 31.13.83.4:443 -> 192.168.1.53:640
01/15-00:48:11.417793 [**] [1:1000001:1] ATENCIÓ algú està intentat ingressar a FACEBOOK [**] [Priority: 0] {TCP} 31.13.83.4:443 -> 192.168.1.53:6

```

Nom i Cognoms	Data
Arnau Subirós Puigarnau	

L'última alerta, s'ha fet ping(protocol icmp) desde el host físic



The image shows two terminal windows. The top window is titled 'Indicador d'ordres' and displays a command-line interface with the following text:

```
C:\Users\Usuario>ping 192.168.1.53

Haciendo ping a 192.168.1.53 con 32 bytes de datos:
Respuesta desde 192.168.1.53: bytes=32 tiempo<1m TTL=64
```

The bottom window is titled 'uruloki@kali-anonymous: /etc/snort' and displays a log of network traffic analysis. The log shows numerous ICMP PING requests and responses between two hosts at 192.168.1.33 and 192.168.1.53. The log entries are as follows:

```
Fitxer Edita Visualitza Cerca Terminal Ajuda
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Commencing packet processing (pid=2180)
01/15-13:05:59.386242 [**] [1:382:7] ICMP PING Windows [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.1.33 -> 192.168.1.53
01/15-13:05:59.386242 [**] [1:1000002:2] Alerta!!! ICMP Packet found. [**] [Priority: 0] {ICMP} 192.168.1.33 -> 192.168.1.53
01/15-13:05:59.386242 [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.1.33 -> 192.168.1.53
01/15-13:05:59.386349 [**] [1:1000002:2] Alerta!!! ICMP Packet found. [**] [Priority: 0] {ICMP} 192.168.1.53 -> 192.168.1.33
01/15-13:05:59.386349 [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.1.53 -> 192.168.1.33
01/15-13:06:00.393756 [**] [1:382:7] ICMP PING Windows [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.1.33 -> 192.168.1.53
01/15-13:06:00.393756 [**] [1:1000002:2] Alerta!!! ICMP Packet found. [**] [Priority: 0] {ICMP} 192.168.1.33 -> 192.168.1.53
01/15-13:06:00.393756 [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.1.33 -> 192.168.1.53
01/15-13:06:00.393781 [**] [1:1000002:2] Alerta!!! ICMP Packet found. [**] [Priority: 0] {ICMP} 192.168.1.53 -> 192.168.1.33
01/15-13:06:00.393781 [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.1.53 -> 192.168.1.33
01/15-13:06:01.398913 [**] [1:382:7] ICMP PING Windows [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.1.33 -> 192.168.1.53
01/15-13:06:01.398913 [**] [1:1000002:2] Alerta!!! ICMP Packet found. [**] [Priority: 0] {ICMP} 192.168.1.33 -> 192.168.1.53
01/15-13:06:01.398913 [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.1.33 -> 192.168.1.53
01/15-13:06:01.398953 [**] [1:1000002:2] Alerta!!! ICMP Packet found. [**] [Priority: 0] {ICMP} 192.168.1.53 -> 192.168.1.33
01/15-13:06:01.398953 [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.1.53 -> 192.168.1.33
01/15-13:06:02.409869 [**] [1:382:7] ICMP PING Windows [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.1.33 -> 192.168.1.53
01/15-13:06:02.409869 [**] [1:1000002:2] Alerta!!! ICMP Packet found. [**] [Priority: 0] {ICMP} 192.168.1.33 -> 192.168.1.53
01/15-13:06:02.409869 [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.1.33 -> 192.168.1.53
01/15-13:06:02.409900 [**] [1:1000002:2] Alerta!!! ICMP Packet found. [**] [Priority: 0] {ICMP} 192.168.1.53 -> 192.168.1.33
```

Nom i Cognoms	Data
Arnau Subirós Puigarnau	

## 2. Instal·lació de Secure Onion

Secure Onion és una distribució Linux que podem tenir instal·lada com un servidor intermig amb una sèrie d'eines interessants en la detecció i prevenció d'intrusos en una xarxa. En el següent link trobareu com instal·lar i utilitzar la eina squil (minut 8:00 del vídeo). Així doncs seguiu les instruccions del següent link i feu les captures de pantalla conforme heu anat seguint els passos.

<https://www.youtube.com/watch?v=kqD3IzhKUQI>

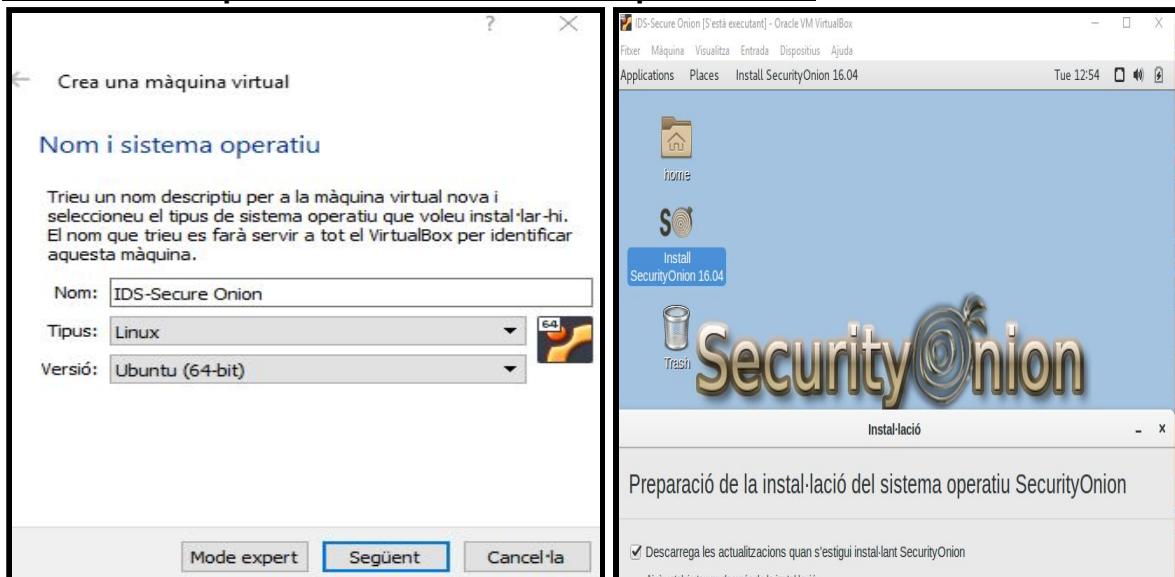
### Procés d'instal·lació de Secure Onion

**Security Onion** és una distribució, basada en Ubuntu, que recopila un gran nombre d'eines destinades a l'anàlisi forense, tant de xarxes com de sistemes, de manera que puguem garantir el correcte funcionament de tots ells i la inexistència de tota mena d'intrusos en la xarxa.

Security Onion ve amb una gran varietat de paquets i eines per detectar per a auditar la seguretat de tota mena de xarxes, entre les quals podem destacar:

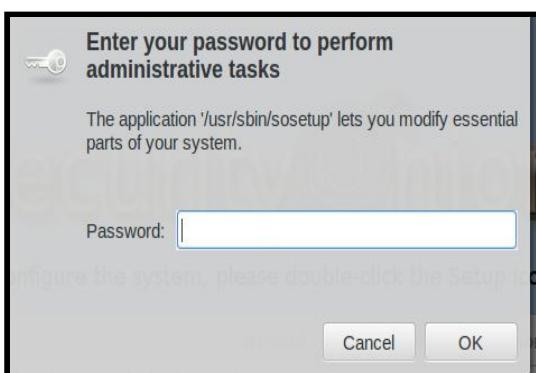
- Snort / Suricata (Sistemes de detecció d'intrusos).
- Squert / Sguil (Monitors d'esdeveniments).
- Wireshark / NetworkMiner (Analitzadors PCAP).
- Bro / Xplico (Eines per a anàlisis forense).

### A continuació procedim a instal·lar la màquina virtual



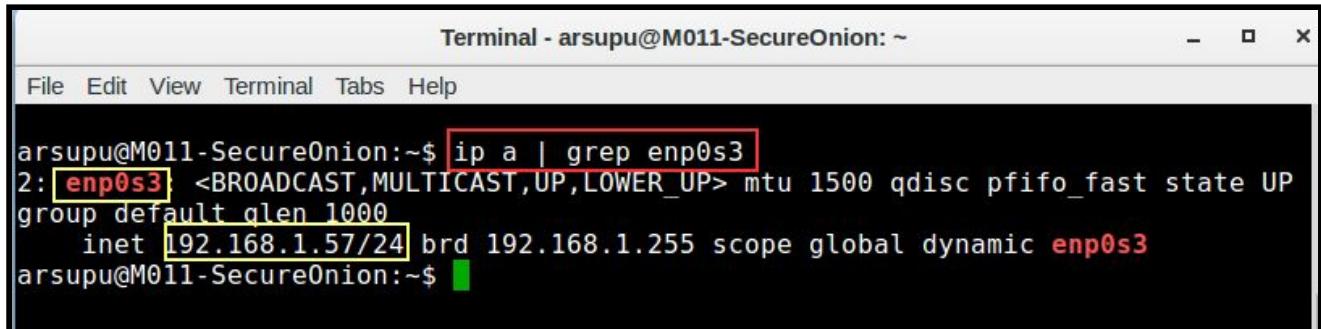
Nom i Cognoms	Data
Arnau Subirós Puigarnau	

Un cop s'ha instal·lat procedim a la configuració



Nom i Cognoms	Data
Arnau Subirós Puigarnau	

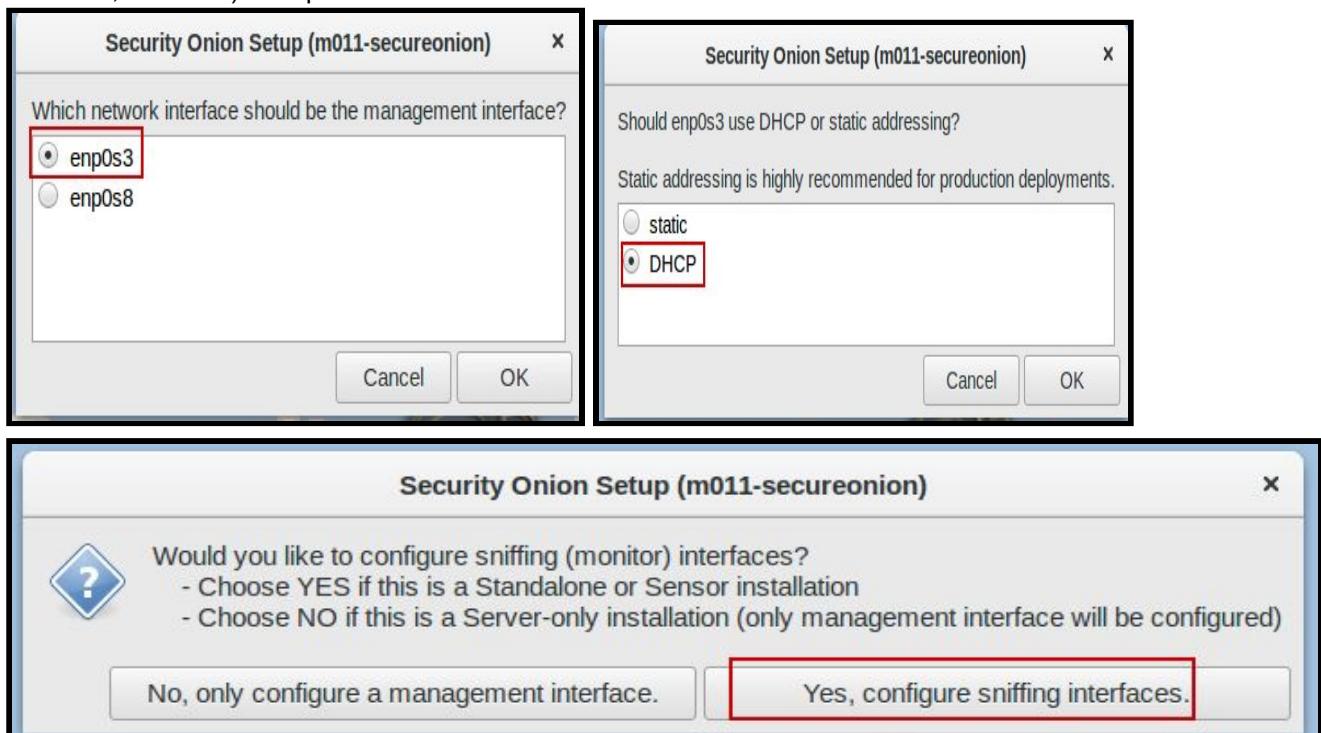
Abans de continuar, obriré el terminal per saber la interfície i la meva IP privada



```
Terminal - arsupu@M011-SecureOnion: ~
File Edit View Terminal Tabs Help

arsupu@M011-SecureOnion:~$ ip a | grep enp0s3
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
group default qlen 1000
    inet 192.168.1.57/24 brd 192.168.1.255 scope global dynamic enp0s3
arsupu@M011-SecureOnion:~$
```

seguim amb la configuració, interfície enps03. He seleccionat IP dinàmica ( ja que cambio constantment de red: casa, escola...) tot i que aconsellen la IP estàtica



Security Onion Setup (m011-secureonion)

Which network interface should be the management interface?

- enp0s3
- enp0s8

Cancel OK

Security Onion Setup (m011-secureonion)

Should enp0s3 use DHCP or static addressing?

Static addressing is highly recommended for production deployments.

- static
- DHCP

Cancel OK

Security Onion Setup (m011-secureonion)

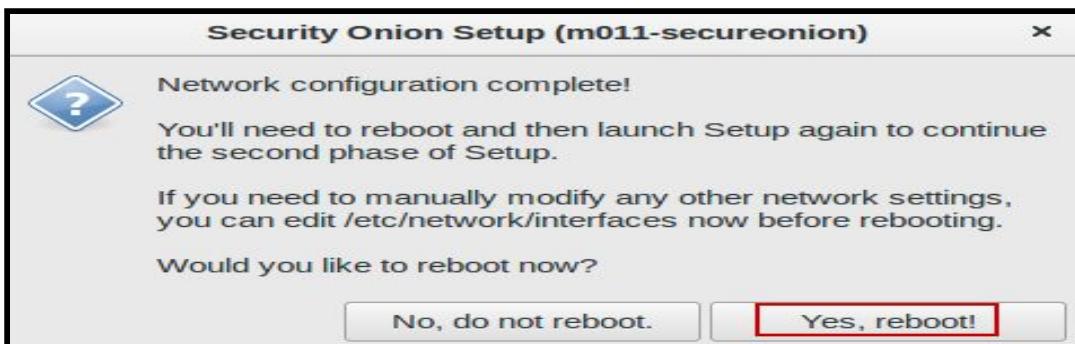
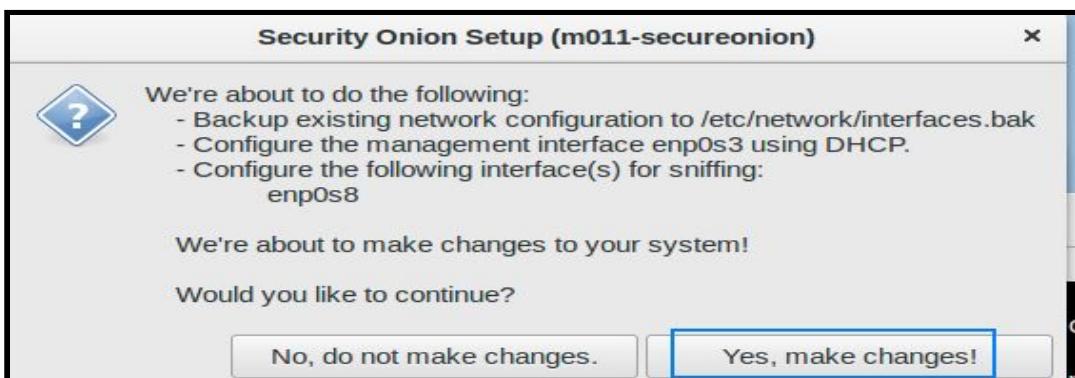
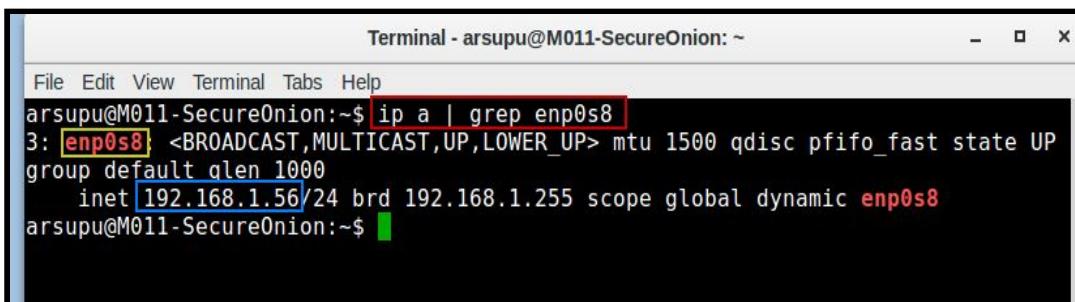
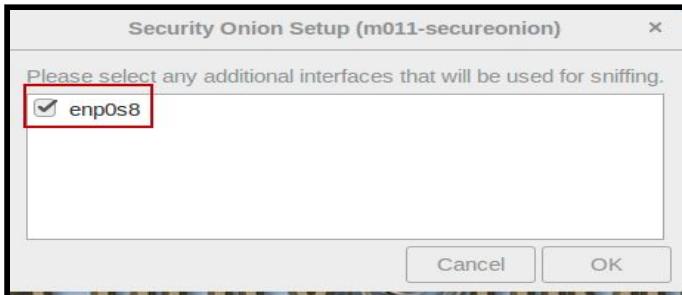
Would you like to configure sniffing (monitor) interfaces?

- Choose YES if this is a Standalone or Sensor installation
- Choose NO if this is a Server-only installation (only management interface will be configured)

No, only configure a management interface. Yes, configure sniffing interfaces.

Nom i Cognoms	Data
Arnau Subirós Puigarnau	

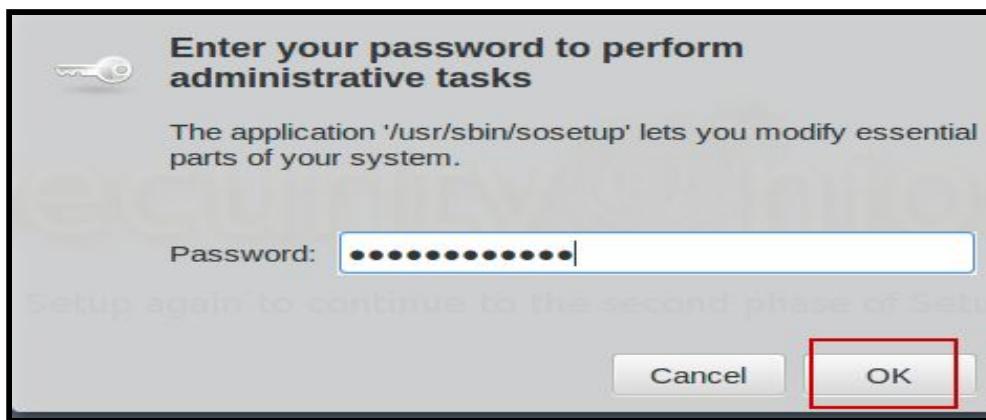
La 2 interfície que he creat **enps08** farà de **sniffer**



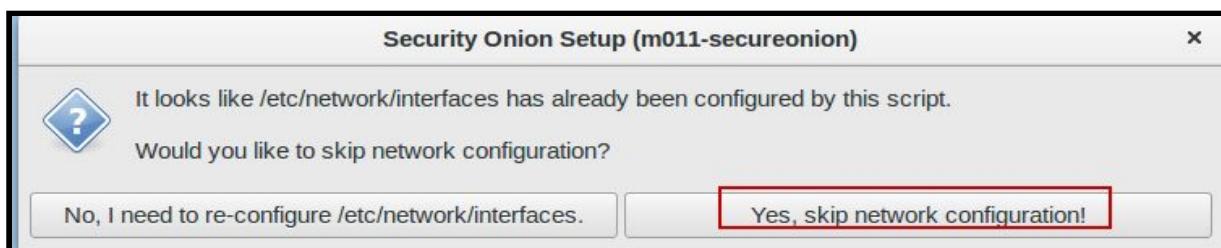
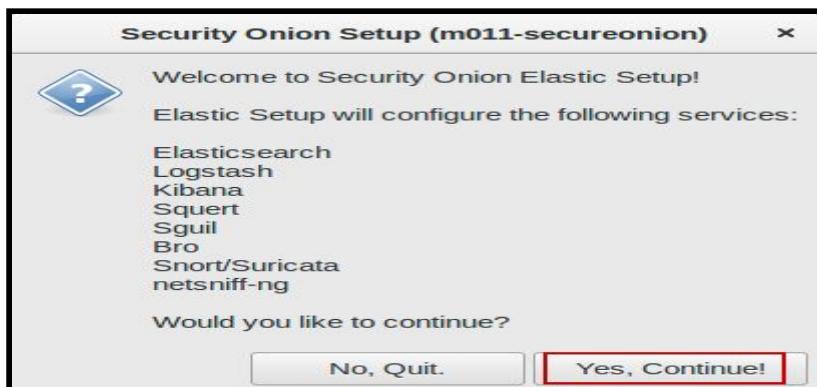
Nom i Cognoms	Data
Arnau Subirós Puigarnau	



Després de reiniciar , en el fons de pantalla em demana que torni a utilitzar setup per la 2 fase la configuració



Nom i Cognoms	Data
Arnau Subirós Puigarnau	

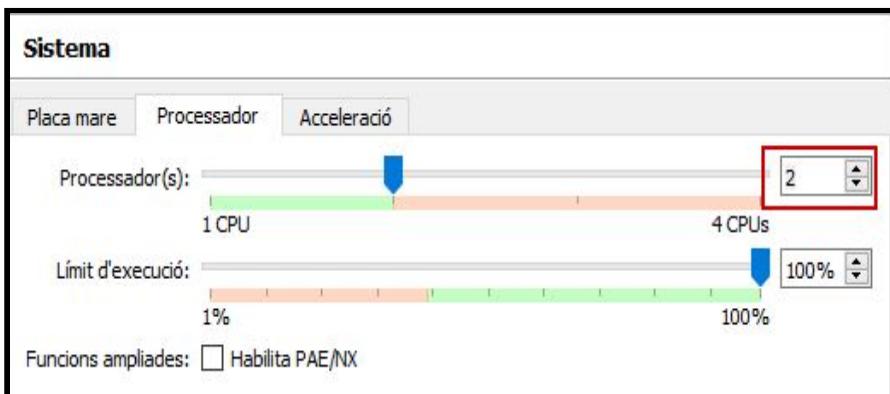
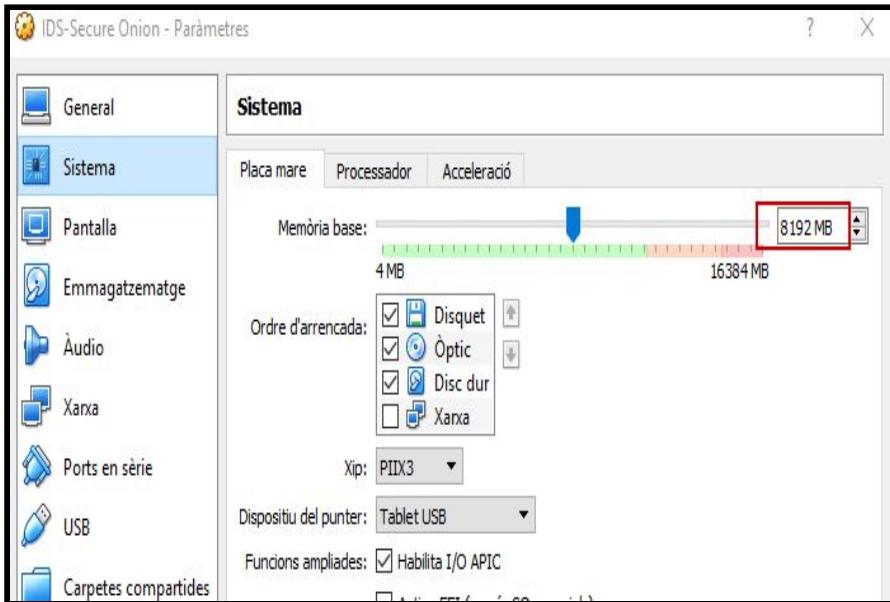


Al crear la màquina, la vaig configurar amb 4 gb de ram i 1 processador, per evitar problemes cancel·lo la 2 part de la configuració per ampliar la memòria de la màquina, per evitar problemes posteriors.

<p>Security Onion Setup (m011-secureonion)</p> <p>This machine currently has 4GB of RAM allocated. For best performance, please ensure the machine is allocated at least 8GB of RAM.</p> <p>Please consult the following link for more information: <a href="https://github.com/Security-Onion-Solutions/security-onion/wiki/Hardware">https://github.com/Security-Onion-Solutions/security-onion/wiki/Hardware</a></p> <p>Click 'No' to stop setup and adjust the amount of RAM allocated to this machine. Otherwise, click 'Yes' to continue.</p> <p>No, Quit. Yes, Continue!</p>	<p>Security Onion Setup (m011-secureonion)</p> <p>This machine currently has 1 processor core(s) allocated. For best performance, please ensure the machine is allocated at least 2 processor cores.</p> <p>Please consult the following link for more information: <a href="https://github.com/Security-Onion-Solutions/security-onion/wiki/Hardware">https://github.com/Security-Onion-Solutions/security-onion/wiki/Hardware</a></p> <p>Click 'No' to stop setup and adjust the number of processor cores allocated to this machine. Otherwise, click 'Yes' to continue.</p> <p>No, Quit. Yes, Continue!</p>
---	---

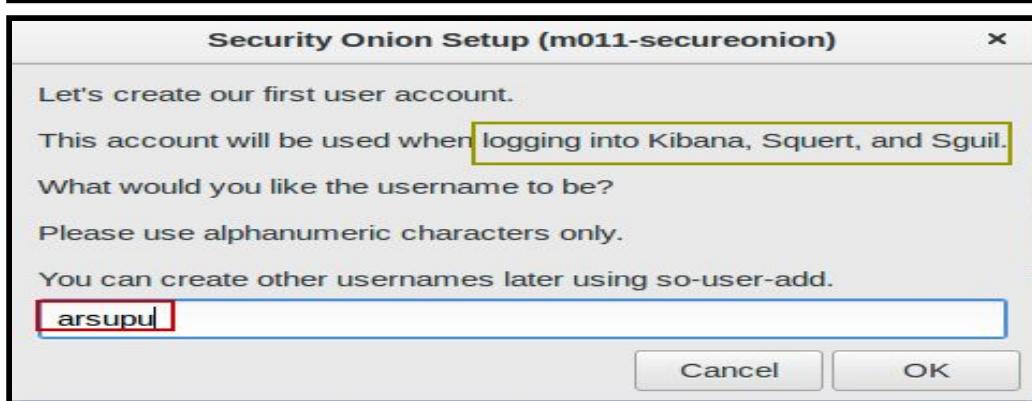
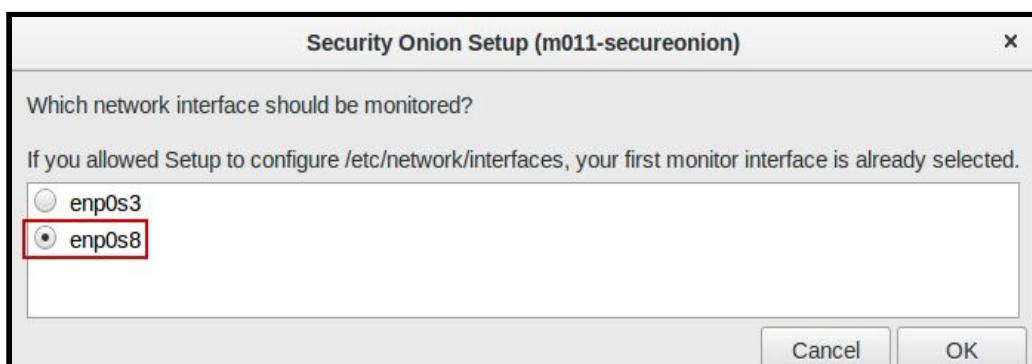
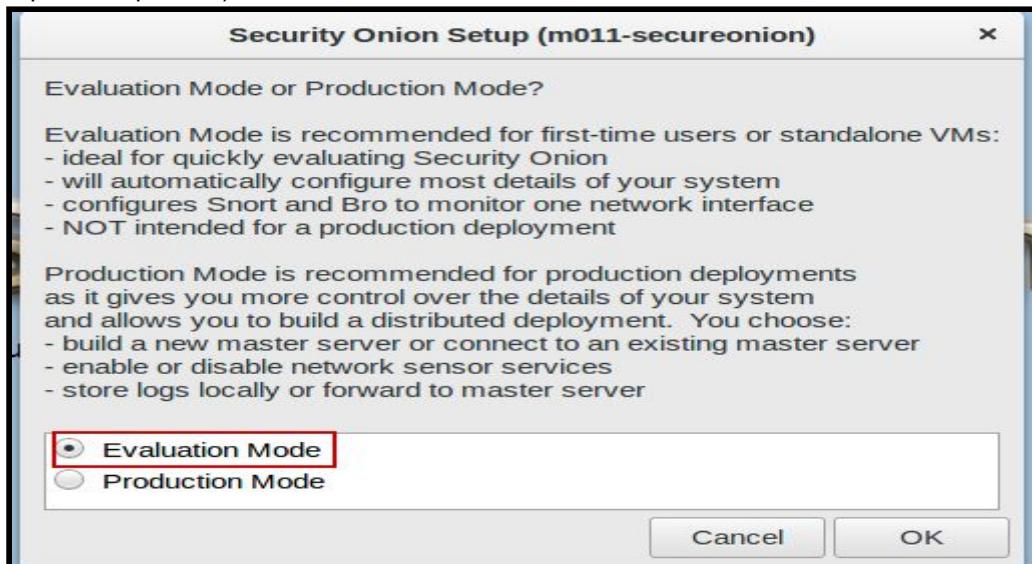
Nom i Cognoms	Data
Arnau Subirós Puigarnau	

Un cop afegit 4 gb més de memoria ram i 1 processador més, torno a engegar la màquina i seguiré amb l'instal.lació(2 fase).

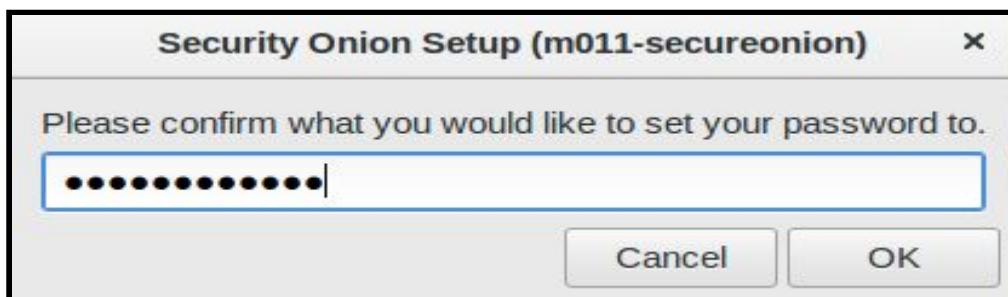
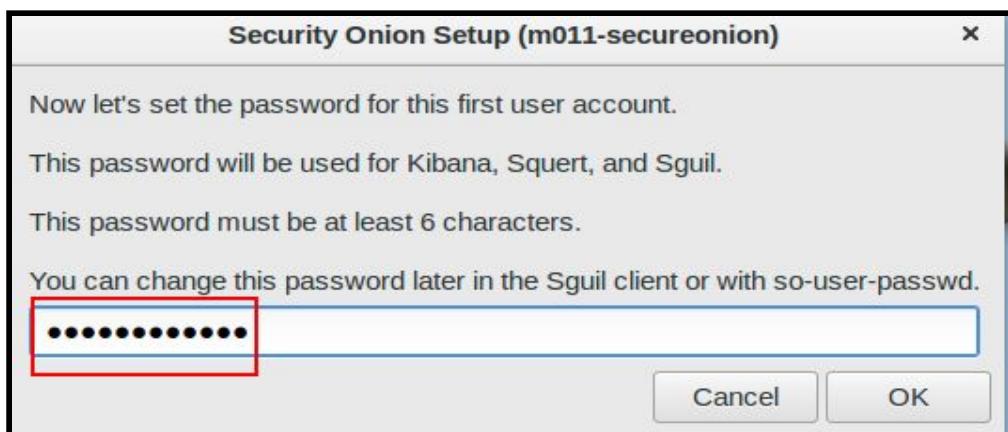


Nom i Cognoms	Data
Arnau Subirós Puigarnau	

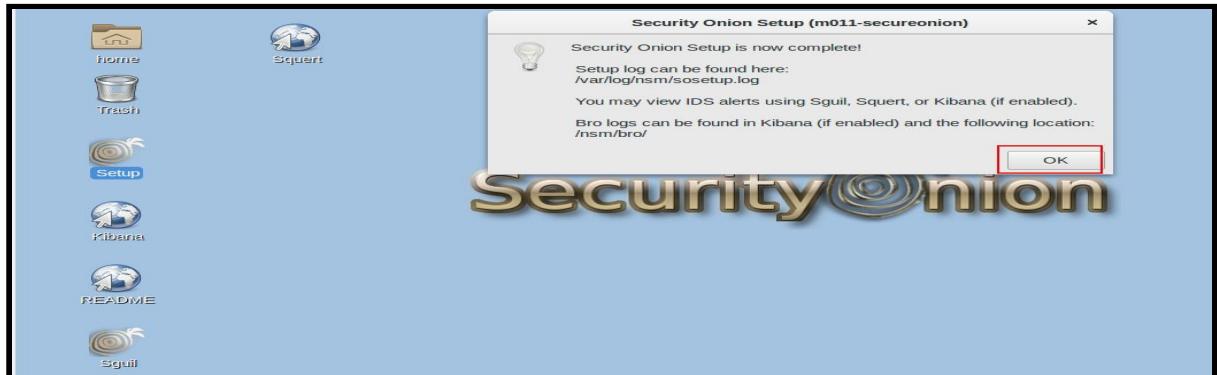
A continuació mostraré desde a partir del “**No, Quit**”, en la cancel.lació de la configuració (per evitar fer captures repetides)



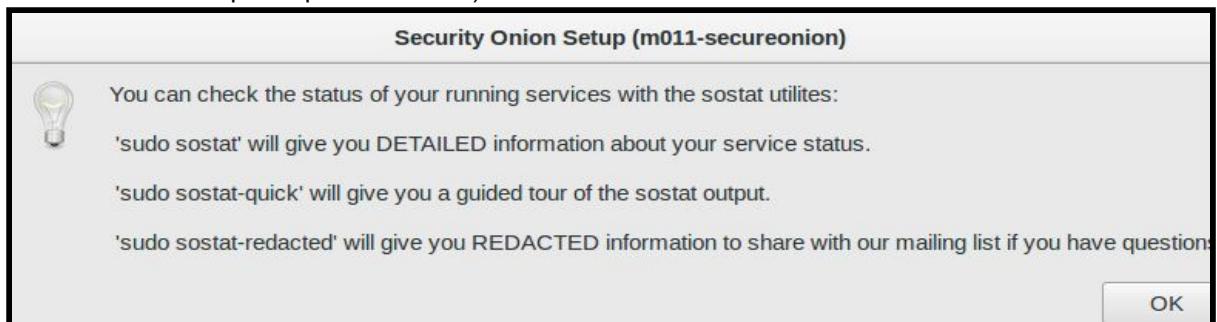
Nom i Cognoms	Data
Arnau Subirós Puigarnau	



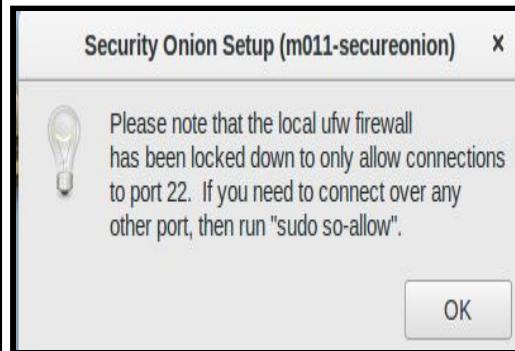
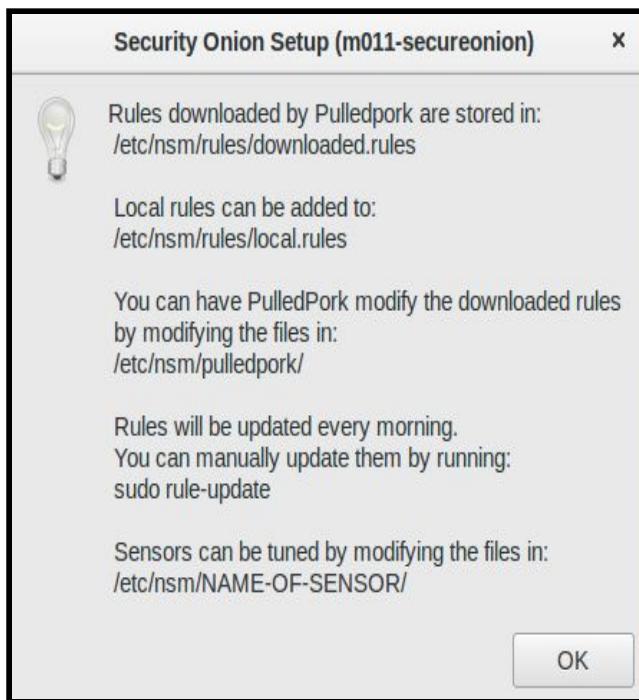
Nom i Cognoms	Data
Arnau Subirós Puigarnau	



Abans d'acabar es mostren varis missatges d'ajuda i recomenacions ( per veure ,status, regles, el port i informació de links per suport comercial)



Nom i Cognoms	Data
Arnau Subirós Puigarnau	



Un cop instal·lat SECURE ONION obrim el SGUIL que és un software per monitoritzar la seguretat a la red (NSM) i l'anàlisis de l'alertes IDS



Nom i Cognoms	Data
Arnau Subirós Puigarnau	

**SGUIL-0.9.0**

Sguil - A tcl/tk interface for network security monitoring  
 Copyright (C) 2002-2013 Robert (Bamm) Visscher <bamm@sguil.net>  
 This program is distributed under the terms of version 3 of the  
 GNU Public License. See LICENSE for further details.  
 This program is distributed in the hope that it will be useful,  
 but WITHOUT ANY WARRANTY; without even the implied warranty of  
 MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

Select Network(s) to Monitor

<input checked="" type="checkbox"/> m011-secureonion-enp0s8 unmonitored	<input checked="" type="checkbox"/> m011-secureonion-ossec unmonitored
--	---

Select All      Start SGUIL      Exit

**SGUIL-0.9.0 - Connected To localhost**

File    Query    Reports    Sound: Off    ServerName: localhost    UserName: arsupu    UserID: 2    2019-01-18 10:40:34 GMT

RealTime Events   Escalated Events

ST	CNT	Sensor	Alert ID	Date/Time	△	Src IP	SPort	Dst IP	DPort	Pr	Event Me
RT	8	m011-secureonion-ossec	3.1	2019-01-18 10:01:58	0	0.0.0.0		0.0.0.0		0	[OSSEC]
RT	8	m011-secureonion-ossec	3.14	2019-01-18 10:01:58	0	0.0.0.0		0.0.0.0		0	[OSSEC]
RT	2	m011-secureonion-ossec	3.15	2019-01-18 10:06:16	0	0.0.0.0		0.0.0.0		0	[OSSEC]
RT	1	m011-secureonion-ossec	3.16	2019-01-18 10:10:16	0	0.0.0.0		0.0.0.0		0	[OSSEC]
RT	5	m011-secureonion-ossec	3.19	2019-01-18 10:21:32	0	0.0.0.0		0.0.0.0		0	[OSSEC]
RT	8	m011-secureonion-ossec	3.22	2019-01-18 10:21:34	0	0.0.0.0		0.0.0.0		0	[OSSEC]
RT	4	m011-secureonion-ossec	3.20	2019-01-18 10:21:34	0	0.0.0.0		0.0.0.0		0	[OSSEC]
RT	1	m011-secureonion-enp0s8-1	2.1	2019-01-18 10:23:29	0	192.168.1.57	44362	91.189.88.161	80	6	ET POLI.
RT	2	m011-secureonion-ossec	3.36	2019-01-18 10:23:35	0	0.0.0.0		0.0.0.0		0	[OSSEC]
RT	2	m011-secureonion-ossec	3.37	2019-01-18 10:23:35	0	0.0.0.0		0.0.0.0		0	[OSSEC]
RT	31	m011-secureonion-ossec	3.40	2019-01-18 10:28:42	0	0.0.0.0		0.0.0.0		0	[OSSEC]

IP Resolution   Agent Status   Snort Statistics   System M

Sid	Net	Hostname	Type	
1	m011-secur...	m011-secur...	pcap	2019-01
2	m011-secur...	m011-secur...	snort	2019-01
3	m011-secur...	m011-secur...	ossec	2019-01

Display Detail

Nom i Cognoms	Data
Arnau Subirós Puigarnau	

### 3. Investigar sobre les altres eines

Escolliu 3 eines de les que s'han explicat a la introducció (no SNORT no Secure Onion) i amplieu-ne la informació i utilitzeu-les en un entorn virtualitzat.

## 1. SURICATA

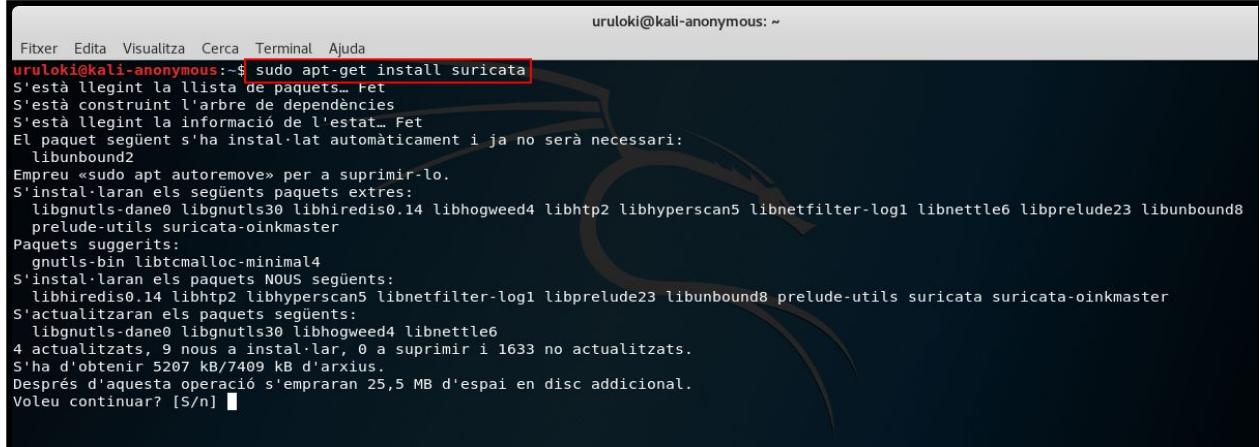
- Suricata és un motor de detecció d'amenaces de xarxa lliure, de codi obert, madur, ràpid i robust.

El motor Suricata és capaç de:

- detecció d'intrusió en temps real (IDS)
- prevenció d'intrusió en línia (IPS)
- monitoratge de seguretat de xarxa (NSM)
- processament de pcap fos de línia. per a anàlisi forense).

- Suricata inspecciona el trànsit de la xarxa utilitzant un llenguatge de signatures i regles poderoses i extenses, i té un potent suport de **scripts Lua** per a la **detecció d'amenaces complexes**.
- Amb formats d'entrada i sortida estàndard com YAML i JSON, les integracions amb eines com SIEMs existents, Splunk, Logstash / Elasticsearch, Kibana i altres bases de dades es tornen sense esforç.
- El ràpid desenvolupament impulsat per la comunitat de Suricata se centra en la seguretat, la facilitat d'ús i l'eficiència.
- El projecte i el codi de Suricata són propietat i estan recolzats per la **Open InformationSecurity Foundation ( OISF )**, una fundació sense finalitats de lucre compromesa a garantir el desenvolupament i l'èxit sostingut de Suricata com un projecte de codi obert.

→ En aquest cas instal·larem el software en la màquina virtual Kali Linux



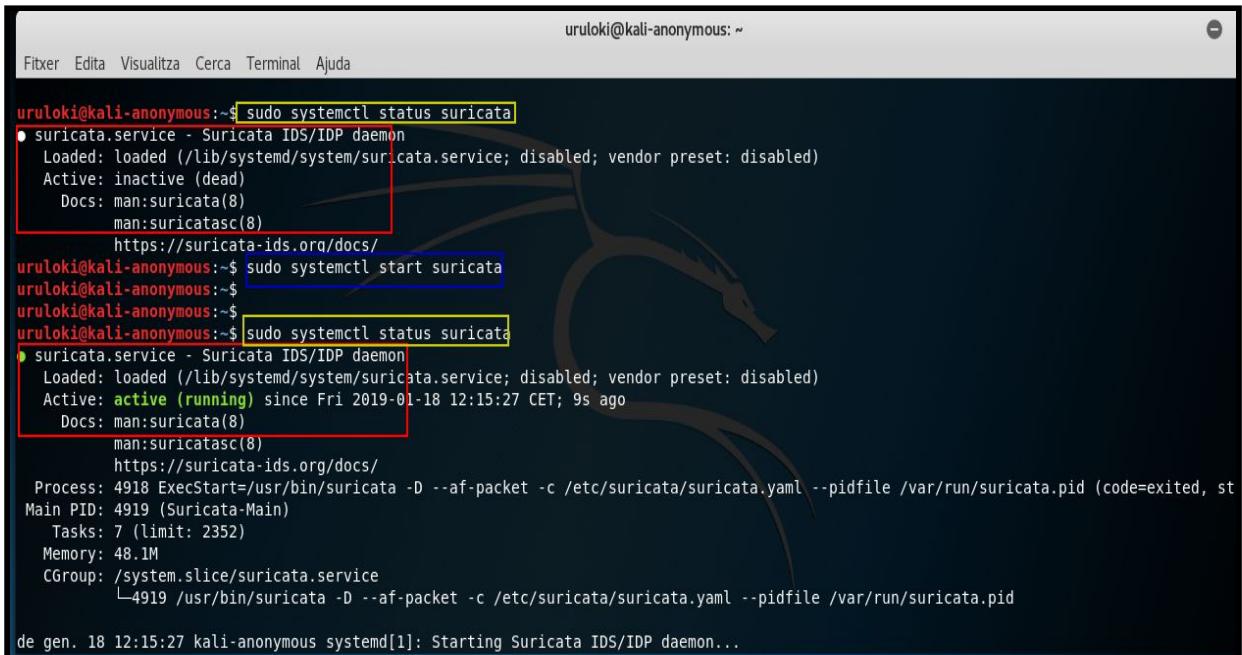
```

Fitxer Edita Visualitza Cerca Terminal Ajuda
uruloki@kali-anonymous:~$ sudo apt-get install suricata
S'està llegint la llista de paquets... ret
S'està construint l'arbre de dependències
S'està llegint la informació de l'estat... Fet
El paquet següent s'ha instal·lat automàticament i ja no serà necessari:
 libunbound2
Empreu «sudo apt autoremove» per a suprimir-lo.
S'instal·laran els següents paquets extres:
 libgnutls-dane0 libgnutls30 libhiredis0.14 libhogweed4 libhttp2 libhyperscan5 libnetfilter-log1 libnettle6 libprelude23 libunbound8
 prelude-utils suricata-oinkmaster
Paquets suggerits:
 gnutls-bin libtcmalloc-minimal4
S'instal·laran els paquets NOUS següents:
 libhiredis0.14 libhttp2 libhyperscan5 libnetfilter-log1 libprelude23 libunbound8 prelude-utils suricata suricata-oinkmaster
S'actualitzaran els paquets següents:
 libgnutls-dane0 libgnutls30 libhogweed4 libnettle6
4 actualitzats, 9 nous a instal·lar, 0 a suprimir i 1633 no actualitzats.
S'ha d'obtenir 5207 kB/7409 kB d'arxius.
Després d'aquesta operació s'empraran 25,5 MB d'espai en disc addicional.
Voleu continuar? [S/n] 

```

Nom i Cognoms	Data
Arnau Subirós Puigarnau	

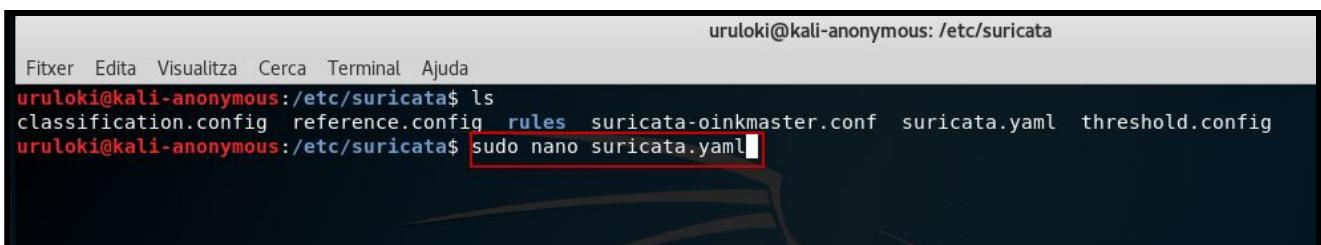
Un cop instal.lat reviso l'estat del servei, al comprovar que està inactiu l'activo i torno a confirmar l'estat



```
uruloki@kali-anonymous:~$ sudo systemctl status suricata
● suricata.service - Suricata IDS/IDP daemon
  Loaded: loaded (/lib/systemd/system/suricata.service; disabled; vendor preset: disabled)
  Active: inactive (dead)
    Docs: man:suricata(8)
           man:suricatas(8)
           https://suricata-ids.org/docs/
uruloki@kali-anonymous:~$ sudo systemctl start suricata
uruloki@kali-anonymous:~$ 
uruloki@kali-anonymous:~$ 
uruloki@kali-anonymous:~$ sudo systemctl status suricata
● suricata.service - Suricata IDS/IDP daemon
  Loaded: loaded (/lib/systemd/system/suricata.service; disabled; vendor preset: disabled)
  Active: active (running) since Fri 2019-01-18 12:15:27 CET; 9s ago
    Docs: man:suricata(8)
           man:suricatas(8)
           https://suricata-ids.org/docs/
Process: 4918 ExecStart=/usr/bin/suricata -D --af-packet -c /etc/suricata/suricata.yaml --pidfile /var/run/suricata.pid (code=exited, st
Main PID: 4919 (Suricata-Main)
  Tasks: 7 (limit: 2352)
 Memory: 48.1M
  CGroup: /system.slice/suricata.service
          └─4919 /usr/bin/suricata -D --af-packet -c /etc/suricata/suricata.yaml --pidfile /var/run/suricata.pid

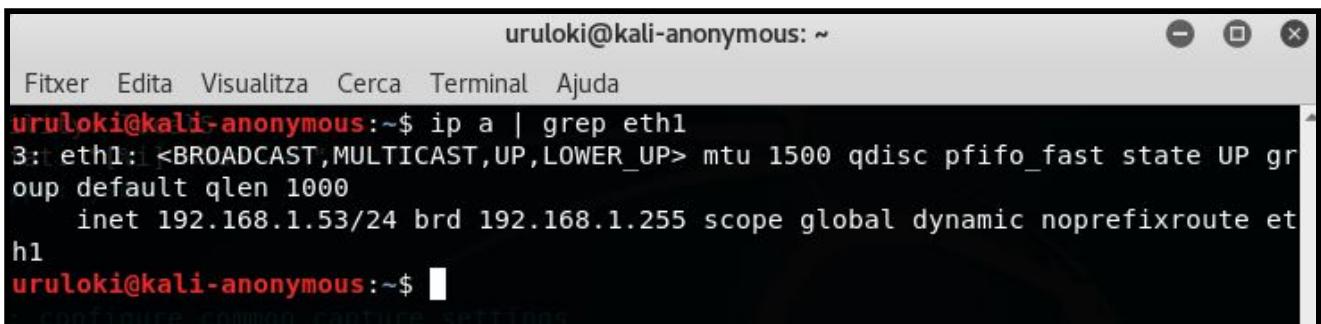
de gen. 18 12:15:27 kali-anonymous systemd[1]: Starting Suricata IDS/IDP daemon...
```

Ara hem de accedir a l'arxiu de configuració i modificar alguns paràmetres



```
uruloki@kali-anonymous: /etc/suricata
Fitxer Edita Visualitza Cerca Terminal Ajuda
uruloki@kali-anonymous: /etc/suricata$ ls
classification.config reference.config rules suricata-oinkmaster.conf suricata.yaml threshold.config
uruloki@kali-anonymous: /etc/suricata$ sudo nano suricata.yaml
```

Abans hem de revisar el nom de la nostra interfície i modificar-la a l'arxiu de configuració



```
uruloki@kali-anonymous: ~
Fitxer Edita Visualitza Cerca Terminal Ajuda
uruloki@kali-anonymous:~$ ip a | grep eth1
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    inet 192.168.1.53/24 brd 192.168.1.255 scope global dynamic noprefixroute eth1
uruloki@kali-anonymous:~$
```

Nom i Cognoms	Data
Arnau Subirós Puigarnau	

```
uruloki@kali-anonymous: /etc/suricata
Fitxer Edita Visualitza Cerca Terminal Ajuda
GNU nano 2.9.8 suricata.yaml

## See "Advanced Capture Options" below for more options, including NETMAP
## and PF_RING.
##
# Linux high speed capture support
af-packet:
- interface: eth1
  # Number of receive threads. "auto" uses the number of cores
  #threads: auto
```

Ens descarguem un conjunt de regles **Emerging Threats** comprimit

```
uruloki@kali-anonymous: /etc/suricata/rules
Fitxer Edita Visualitza Cerca Terminal Ajuda
uruloki@kali-anonymous: /etc/suricata$ cd rules
uruloki@kali-anonymous: /etc/suricata/rules$ ls
app-layer-events.rules dns-events.rules ipsec-events.rules nfs-events.rules smtp-events.rules
decoder-events.rules files.rules kerberos-events.rules ntp-events.rules stream-events.rules
dnp3-events.rules http-events.rules modbus-events.rules smb-events.rules tls-events.rules
uruloki@kali-anonymous: /etc/suricata/rules$ sudo wget http://rules.emergingthreats.net/open/suricata/emerging.rules.tar.gz
--2019-01-18 16:19:42-- http://rules.emergingthreats.net/open/suricata/emerging.rules.tar.gz
S'està resolent rules.emergingthreats.net (rules.emergingthreats.net)... 204.12.217.19, 96.43.137.99
S'està connectant a rules.emergingthreats.net (rules.emergingthreats.net)|204.12.217.19|:80... connectat.
HTTP: s'ha enviat la petició, s'està esperant una resposta... 200 OK
Mida: 2334156 (2,2M) [application/x-gzip]
S'està desant a: «emerging.rules.tar.gz»

emerging.rules.tar.gz 100%[=====] 2,23M 571KB/s

2019-01-18 16:19:47 (466 KB/s) - s'ha desat «emerging.rules.tar.gz» [2334156/2334156]
uruloki@kali-anonymous: /etc/suricata/rules$
```

Descomprimint les regles en format tar

```
uruloki@kali-anonymous: /etc/suricata/rules
Fitxer Edita Visualitza Cerca Terminal Ajuda
uruloki@kali-anonymous: /etc/suricata/rules$ ls
app-layer-events.rules dns-events.rules http-events.rules modbus-events.rules smb-events.rules tls-events.rules
decoder-events.rules emerging.rules.tar.gz ipsec-events.rules nfs-events.rules smtp-events.rules
dnp3-events.rules files.rules kerberos-events.rules ntp-events.rules stream-events.rules
uruloki@kali-anonymous: /etc/suricata/rules$ sudo tar xzvf emerging.rules.tar.gz
rules/
rules/emerging-mobile_malware.rules
rules/botcc.rules
rules/botcc.portgrouped.rules
rules/dshield.rules
rules/tor.rules
rules/emerging-tftp.rules
rules/emerging-chat.rules
rules/emerging-current_events.rules
rules/emerging-web_server.rules
rules/emerging-policy.rules
rules/LICENSE
rules/emerging-scada.rules
rules/emerging-pop3.rules
rules/drop.rules
rules/american_attack_responses.rules
```

Nom i Cognoms	Data
Arnau Subirós Puigarnau	

Crearem un alerta per fer proves

```
uruloki@kali-anonymous: /etc/suricata/rules
Fitxer Edita Visualitza Cerca Terminal Ajuda
uruloki@kali-anonymous:/etc/suricata$ cd rules
uruloki@kali-anonymous:/etc/suricata/rules$ sudo gedit local.rules
local.rules
/etc/suricata/rules
Desa
alert icmp any any -> any any (msg:"ALERTA paquet ICMP detectat";)
```

Ja tenim la regla instal.lada ,ara la afegirem a l'arxiu de configuració

```
uruloki@kali-anonymous: /etc/suricata
Fitxer Edita Visualitza Cerca Terminal Ajuda
uruloki@kali-anonymous:/etc/suricata$ sudo gedit suricata.yaml
uruloki@kali-anonymous: ~
```

```
## Configure Suricata to load Suricata-Update managed rules.
##
## If this section is completely commented out move down to the "Advanced rule
## file configuration".
##

#default-rule-path: /etc/suricata/rules
#rule-files:
# - suricata.rules

##
## Advanced rule file configuration.
##
## If this section is completely commented out then your configuration
## is setup for suricata-update as it was most likely bundled and
## installed with Suricata.
##

default-rule-path: /etc/suricata/rules

rule-files:
- botcc.rules
# - botcc.portgrouped.rules
- ciarmy.rules
- compromised.rules
- drop.rules
- tor.rules
# - decoder-events.rules # available in suricata sources under rules dir
# - stream-events.rules # available in suricata sources under rules dir
- http-events.rules # available in suricata sources under rules dir
- smtp-events.rules # available in suricata sources under rules dir
- dns-events.rules # available in suricata sources under rules dir
- tls-events.rules # available in suricata sources under rules dir
# - modbus-events.rules # available in suricata sources under rules dir
# - app-layer-events.rules # available in suricata sources under rules dir
# - dnp3-events.rules # available in suricata sources under rules dir
# - ntp-events.rules # available in suricata sources under rules dir
# - ipsec-events.rules # available in suricata sources under rules dir
# - kerberos-events.rules # available in suricata sources under rules dir
- local.rules # les regles que creare jo

##
## Auxiliary configuration files.
##
```

Nom i Cognoms	Data
Arnau Subirós Puigarnau	

un cop guardat els canvis, hem de reiniciar el servei suricata.

```
uruloki@kali-anonymous: /etc/suricata
Fitxer Edita Visualitza Cerca Terminal Ajuda
uruloki@kali-anonymous:/etc/suricata$ sudo systemctl restart suricata
uruloki@kali-anonymous:/etc/suricata$ sudo systemctl status suricata
● suricata.service - Suricata IDS/IDP daemon
   Loaded: loaded (/lib/systemd/system/suricata.service; disabled; vendor preset: disabled)
   Active: active (running) since Fri 2019-01-18 17:05:18 CET; 8s ago
     Docs: man:suricata(8)
           man:suricatasc(8)
           https://suricata-ids.org/docs/
   Process: 9253 ExecStop=/usr/bin/suricatasc -c shutdown (code=exited, status=0/SUCCESS)
   Process: 9254 ExecStart=/usr/bin/suricata -D --af-packet -c /etc/suricata/suricata.yaml --p
 Main PID: 9255 (Suricata-Main)
    Tasks: 1 (limit: 2352)
   Memory: 185.3M
      CGroup: /system.slice/suricata.service
```

procedim a l'execució de **SURICATA**, on s'utiliza l'arxiu binari /usr/bin/suricata , l'arxiu de configuració /etc/suricata/suricata.yaml i la intereficie de xarxa ( en el meu cas eth1).

**sudo /usr/bin/suricata -c /etc/suricata/suricata.yaml -i -eth1**

```
uruloki@kali-anonymous: /etc/suricata
Fitxer Edita Visualitza Cerca Terminal Ajuda
uruloki@kali-anonymous:/etc/suricata$ clear
uruloki@kali-anonymous:/etc/suricata$ sudo /usr/bin/suricata -c /etc/suricata/suricata.yaml -i eth1
18/1/2019 -- 17:17:06 - <Notice> - This is Suricata version 4.1.2 RELEASE
18/1/2019 -- 17:17:12 - <Warning> - [ERRCODE: SC_WARN_FLOWBIT(306)] - flowbit 'HTTP.UncompressedFlash' is checked but not set. Checked in 201 other sigs
18/1/2019 -- 17:17:12 - <Warning> - [ERRCODE: SC_WARN_FLOWBIT(306)] - flowbit 'ET.pdf.in.http' is checked but not set. Checked in 201 other sigs
18/1/2019 -- 17:17:12 - <Warning> - [ERRCODE: SC_WARN_FLOWBIT(306)] - flowbit 'ET.JS.Obfus.Func' is checked but not set. Checked in 1 other sigs
18/1/2019 -- 17:17:12 - <Warning> - [ERRCODE: SC_WARN_FLOWBIT(306)] - flowbit 'et.http.PK' is checked but not set. Checked in 201983 other sigs
18/1/2019 -- 17:17:12 - <Warning> - [ERRCODE: SC_WARN_FLOWBIT(306)] - flowbit 'et.JavaArchiveOrClass' is checked but not set. Checked in 15 other sigs
```

Nom i Cognoms	Data
Arnau Subirós Puigarnau	

## 2. OSSEC

És un software de codi lliure de sistema de detecció d'intrusions basat en host (HIDS)

- ❑ Realitza anàlisi de registre , comprovació d'integritat, supervisió de registre de Windows , detecció de rootkits , alertes basades en el temps i resposta activa.
- ❑ Proporciona detecció d'intrusions per a la majoria dels sistemes operatius, inclosos *Linux* , *OpenBSD* , *FreeBSD* , *US X* , *Solaris* i *Windows*
- ❑ OSSEC consisteix en una aplicació principal, un agent i una interfície web
- ❑ En aquest cas, aprofitem la maquina on tenim instal.lat **SECURE ONION** ja que ja està inclòs el software OSSEC(actua com a servidor)

```
Terminal - arsupu@M011-SecureOnion: ~
File Edit View Terminal Tabs Help

arsupu@M011-SecureOnion:~$ sudo systemctl status ossec-hids-server.service
● ossec-hids-server.service - LSB: ossec-hids-server
   Loaded: loaded (/etc/init.d/ossec-hids-server; bad; vendor preset: enabled)
   Active: active (running) since Fri 2019-01-18 17:01:56 UTC; 1h 8min ago
     Docs: man:systemd-sysv-generator(8)
  Process: 930 ExecStart=/etc/init.d/ossec-hids-server start (code=exited, status=0/SUCCESS)
    Tasks: 52
   Memory: 996.0M
      CPU: 53.586s
     CGroup: /system.slice/ossec-hids-server.service
             └─1544 /var/ossec/bin/wazuh-db
                 ├─1548 /var/ossec/bin/ossec-execd
                 ├─1553 /var/ossec/bin/ossec-analysisd
                 ├─1557 /var/ossec/bin/ossec-syscheckd
                 ├─1566 /var/ossec/bin/ossec-logcollector
                 ├─1571 /var/ossec/bin/ossec-monitord
                 └─1577 /var/ossec/bin/wazuh-modulesd

Jan 18 17:01:51 M011-SecureOnion ossec-hids-server[930]: Started wazuh-db...
Jan 18 17:01:51 M011-SecureOnion ossec-hids-server[930]: Started ossec-execd...
Jan 18 17:01:51 M011-SecureOnion ossec-hids-server[930]: Started ossec-analysisd...
Jan 18 17:01:51 M011-SecureOnion ossec-hids-server[930]: Started ossec-syscheckd...
```

Nom i Cognoms	Data
Arnau Subirós Puigarnau	

```
Terminal - root@M011-SecureOnion: /var/ossec

File Edit View Terminal Tabs Help
root@M011-SecureOnion:/var/ossec# ls
active-response bin framework lib queue rules.backup.20190110 stats var
agentless etc integrations logs rules ruleset
root@M011-SecureOnion:/var/ossec# 
```

## 2.1. Sguil

El component principal de Sguil és una GUI intuïtiva que brinda accés a esdeveniments en temps real, dades de sessió i captura de paquets sense processar. Sguil facilita la pràctica del monitoratge de seguretat de xarxa i l'anàlisi dirigida per esdeveniments. El client Sguili pot executar-se en qualsevol sistema operatiu que admeti tcl / tk(inclusos Linux, \* BSD, Solaris, MacOS i Win32).

- **Agent OSSEC per a Sguil**, que rep les alertes de `/var/*ossec/*logs/*alerts/*alerts.log` i les envia a Sguil.

```
root@M011-SecureOnion: /var/ossec/logs/alerts

File Edit View Search Terminal Help
** Alert 1547801257.0: - ossec,rootcheck,gdpr_IV_30.1.g,
2019 Jan 18 03:47:37 M011-SecureOnion->rootcheck
Rule: 516 (level 3) -> 'System Audit event.'
System Audit: SSH Hardening - 1: Port 22 {PCI_DSS: 2.2.4}. File: /etc/ssh/sshd_config. Reference: 1 .
title: SSH Hardening - 1: Port 22
file: /etc/ssh/sshd_config

** Alert 1547801257.315: - ossec,rootcheck,gdpr_IV_30.1.g,
2019 Jan 18 03:47:37 M011-SecureOnion->rootcheck
Rule: 516 (level 3) -> 'System Audit event.'
System Audit: SSH Hardening - 3: Root can log in. File: /etc/ssh/sshd_config. Reference: 3 .
title: SSH Hardening - 3: Root can log in.
file: /etc/ssh/sshd_config

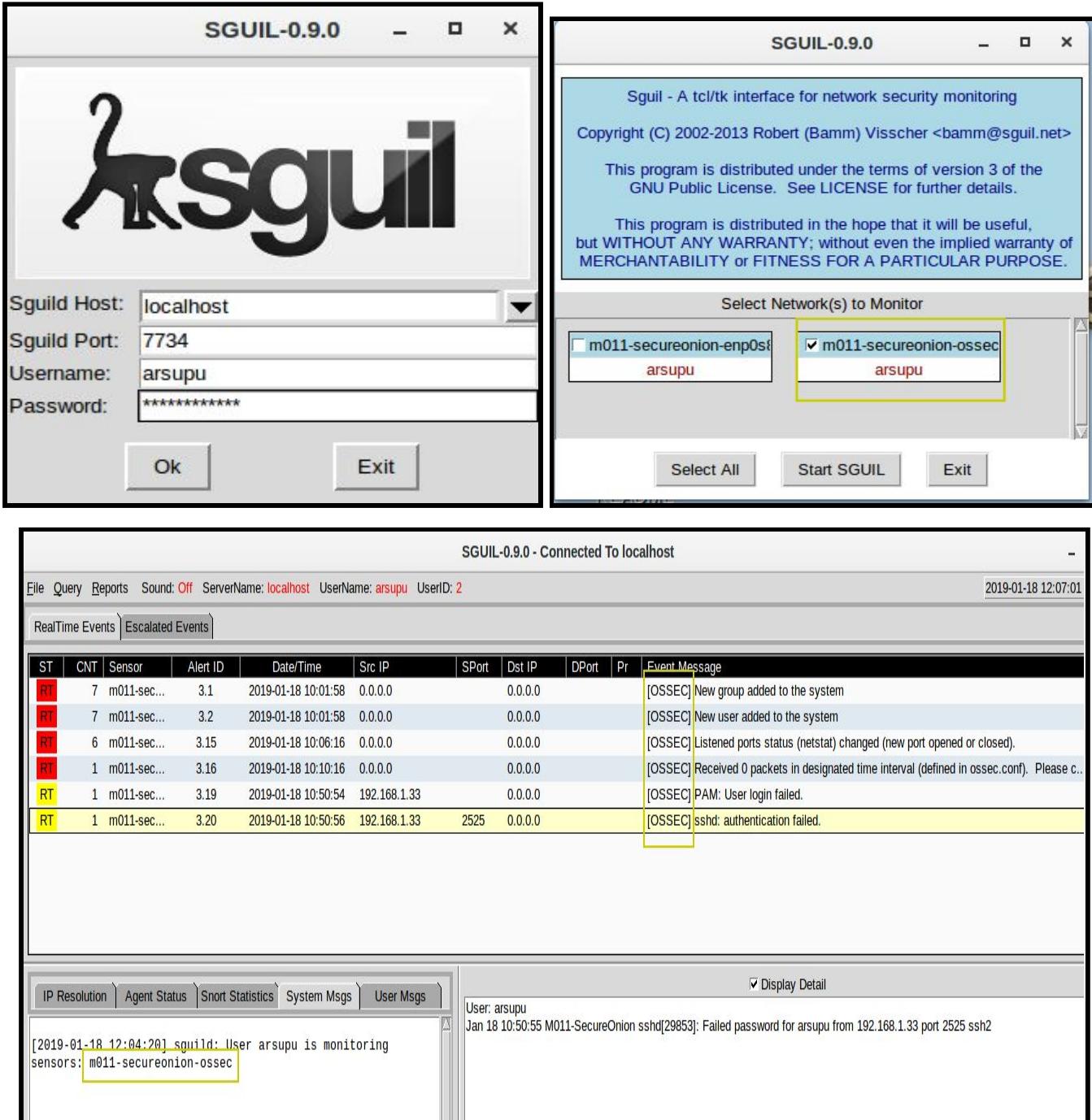
** Alert 1547801257.632: - ossec,rootcheck,gdpr_IV_30.1.g,
2019 Jan 18 03:47:37 M011-SecureOnion->rootcheck
Rule: 516 (level 3) -> 'System Audit event.'
System Audit: SSH Hardening - 5: Password Authentication {PCI_DSS: 2.2.4}. File: /etc/ssh/sshd_config. Reference: 5 .
title: SSH Hardening - 5: Password Authentication
file: /etc/ssh/sshd_config

** Alert 1547801257.981: - ossec,rootcheck,gdpr_IV_30.1.g,
2019 Jan 18 03:47:37 M011-SecureOnion->rootcheck
Rule: 516 (level 3) -> 'System Audit event.'
System Audit: SSH Hardening - 8: Wrong Grace Time {PCI_DSS: 2.2.4}. File: /etc/ssh/sshd_config. Reference: 8 .
title: SSH Hardening - 8: Wrong Grace Time
file: /etc/ssh/sshd_config

--More--
```

Nom i Cognoms	Data
Arnau Subirós Puigarnau	

Anteriorment ja s'ha mostrat però aquest cop només selecciono m011-secureonion-ossec(host)



**SGUIL-0.9.0**

Sguild Host: localhost  
 Sguild Port: 7734  
 Username: arsupu  
 Password: \*\*\*\*\*

**SGUIL-0.9.0**

SgUIL - A tcl/tk interface for network security monitoring  
 Copyright (C) 2002-2013 Robert (Bamm) Visscher <bamm@sguil.net>  
 This program is distributed under the terms of version 3 of the  
 GNU Public License. See LICENSE for further details.  
 This program is distributed in the hope that it will be useful,  
 but WITHOUT ANY WARRANTY; without even the implied warranty of  
 MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

Select Network(s) to Monitor

<input type="checkbox"/> m011-secureonion-emp0s1 arsupu	<input checked="" type="checkbox"/> m011-secureonion-ossec arsupu
--	--

Ok      Exit

Select All      Start SGUIL      Exit

**SGUIL-0.9.0 - Connected To localhost**

File Query Reports Sound: Off ServerName: localhost UserName: arsupu UserID: 2 2019-01-18 12:07:01

RealTime Events Escalated Events

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	7	m011-sec...	3.1	2019-01-18 10:01:58	0.0.0		0.0.0			[OSSEC] New group added to the system
RT	7	m011-sec...	3.2	2019-01-18 10:01:58	0.0.0		0.0.0			[OSSEC] New user added to the system
RT	6	m011-sec...	3.15	2019-01-18 10:06:16	0.0.0		0.0.0			[OSSEC] Listened ports status (netstat) changed (new port opened or closed).
RT	1	m011-sec...	3.16	2019-01-18 10:10:16	0.0.0		0.0.0			[OSSEC] Received 0 packets in designated time interval (defined in ossec.conf). Please c...
RT	1	m011-sec...	3.19	2019-01-18 10:50:54	192.168.1.33		0.0.0			[OSSEC] PAM: User login failed.
RT	1	m011-sec...	3.20	2019-01-18 10:50:56	192.168.1.33	2525	0.0.0			[OSSEC] sshd: authentication failed.

IP Resolution Agent Status Snort Statistics System Msgs User Msgs

Display Detail

User: arsupu  
 Jan 18 10:50:55 M011-SecureOnion sshd[29853]: Failed password for arsupu from 192.168.1.33 port 2525 ssh2

[2019-01-18 12:04:20] sguild: User arsupu is monitoring sensors: m011-secureonion-ossec

Nom i Cognoms	Data
Arnau Subirós Puigarnau	

## BroIDS

- ❑ BRO és una eina open-source per a l'anàlisi de trànsit de xarxa l'objectiu de la qual és reconèixer activitats sospitoses per Unix/Linux
- ❑ L'anàlisi de xarxa reporta diversos tipus de registres dividits segons el protocol i característiques com pot ser HTTP, DNS, SSL, FTP, sessions IRC, SMTP, etc.
- ❑ Per a la captura de paquets utilitzà libpcap. És capaç d'analitzar i detectar túnels (incloent Ayiya, Teredo, GTPv1) a més de desencapsular-los per a després analitzar el seu contingut.
- ❑ Ja el tenim instal.lat a la màquina virtual que utilitza **SECURE ONION**

### 1. Arquitectura de BroIDS

Es basa en dos components:

- ❖ Motor d'esdeveniments (event engine): Redueix el flux de paquets, organitzant-los per a ser portats a un nivell superior.
- ❖ Interpret de Scripts (policy script interpreter): accions a prendre quan es detecta una activitat determinada.

### 2. BroControl

BroControl és una shell interactiva per al maneig de BRO que té dues maneres d'operació:

- stand alone: per a administrar BRO de forma habitual (un node).
- clúster mode: múltiples nodes actuants en conjunt per a aconseguir balanceig de la càrrega

#### 2.1. Execució de Brotcl

La primera vegada que s'usa **broctl** és recomanable usar el comando **deploy** (chequea la configuració de BRO: **broctl.cfg**, **node.cfg** i **networks.cfg**). La resta de vegades es pot usar el comando **start**, però si els fitxers de configuració nomenats abans es modifiquen, s'haurà d'usar **deploy**.

Nom i Cognoms	Data
Arnau Subirós Puigarnau	

Terminal - arsupu@M011-SecureOnion: /opt/bro/bin

```

File Edit View Terminal Tabs Help
arsupu@M011-SecureOnion:/opt/bro/bin$ ls
adtrace bifcl binpac bro bro-config broctl bro-cut capstats rst trace-summary
arsupu@M011-SecureOnion:/opt/bro/bin$ sudo ./broctl

Welcome to BroControl 1.9-2

Type "help" for help.

[BroControl] > [deploy]
checking configurations ...
installing ...
removing old policies in /nsm/bro/spool/installed-scripts-do-not-touch/site ...
removing old policies in /nsm/bro/spool/installed-scripts-do-not-touch/auto ...
creating policy directories ...
installing site policies ...
generating standalone-layout.bro ...
generating local-networks.bro ...
generating broctl-config.bro ...
generating broctl-config.sh ...
stopping ...
stopping bro ...
starting ...
starting bro ...
[BroControl] >

```

Comando **estatus** per a veure l'estat de BRO

```

starting ...
starting bro ...
[BroControl] > [status]
Name      Type      Host      Status      Pid      Started
bro      standalone localhost  running    27539  18 Jan 10:42:36
[BroControl] >

```

Per veure els **scripts**.

Terminal - arsupu@M011-SecureOnion: /opt/bro/bin

```

File Edit View Terminal Tabs Help
[BroControl] >
[BroControl] > [scripts]
bro scripts are ok.
received termination signal
{"name": "/opt/bro/share/bro/base/init-bare.bro"}
{"name": "/opt/bro/share/bro/base/bif/const.bif.bro"}
{"name": "/opt/bro/share/bro/base/bif/types.bif.bro"}
{"name": "/opt/bro/share/bro/base/bif/bro.bif.bro"}
{"name": "/opt/bro/share/bro/base/bif/stats.bif.bro"}
{"name": "/opt/bro/share/bro/base/bif/reporter.bif.bro"}
{"name": "/opt/bro/share/bro/base/bif/strings.bif.bro"}
 {"name": "/opt/bro/share/bro/base/bif/option.bif.bro"}
 {"name": "/opt/bro/share/bro/base/bif/plugins/Bro_SNMP.types.bif.bro"}
 {"name": "/opt/bro/share/bro/base/bif/plugins/Bro_KRB.types.bif.bro"}
 {"name": "/opt/bro/share/bro/base/bif/event.bif.bro"}
 {"name": "/opt/bro/share/bro/base/init-frameworks-and-bifs.bro"}
 {"name": "/opt/bro/share/bro/base/frameworks/logging/_load_.bro"}
 {"name": "/opt/bro/share/bro/base/frameworks/logging/main.bro"}

```

Nom i Cognoms	Data
Arnau Subirós Puigarnau	

Veure les estadístiques de la red

```
[BroControl] > capstats
Interface          kpps      mbps      (10s average)
-----
localhost/enp0s8   0.0       0.0
[BroControl] >
```

Mostrar la configuració

```
File Edit View Terminal Tabs Help
Terminal - arsupu@M011-SecureOnion: ~
[BroControl] > config
bindir = /opt/bro/bin
bro = /opt/bro/bin/bro
bro-crashed = False
bro-expect-running = True
bro-host = localhost
bro-pid = 27539
bro-port = 47760
broargs =
brobase = /opt/bro
broctlconfigdir = /nsm/bro/spool
broport = 47760
broscriptdir = /opt/bro/share/bro
broversion = 2.6.1
capstatspath = /opt/bro/bin/capstats
cfgdir = /opt/bro/etc
commandtimeout = 60
commtimeout = 10
compresscmd = gzip -9
compressextension = gz
compresslogs = 1
configchksum = 3957e56c43adc613c65de4a52a184bb30c6a6391
confignodechksum = b47443f8b2cd8a20ad59175ed418fabaa981a975
controltopic = bro/control
crashexpireinterval = 0
croncmd =
```

Els registres de Bro s'emmagatzemen a /nsm/bro/logs

```
File Edit View Terminal Tabs Help
Terminal - arsupu@M011-SecureOnion: /nsm/bro/logs/2019-01-18
arsupu@M011-SecureOnion:/nsm/bro$ cd logs
arsupu@M011-SecureOnion:/nsm/bro/logs$ ls
2019-01-18 current stats
arsupu@M011-SecureOnion:/nsm/bro/logs$ cd 2019-01-18
arsupu@M011-SecureOnion:/nsm/bro/logs/2019-01-18$ ls
capture_loss.10:16:30-10:42:34.log      files.10:01:51-10:42:34.log
capture_loss.10:42:35-10:42:36.log.gz  ftp.10:03:35-10:42:34.log.gz
capture_loss.10:57:37-11:00:00.log.gz  http.10:04:42-10:42:34.log.gz
conn.10:01:56-10:42:34.log.gz        known_hosts.10:01:51-10:42:34.log.gz
conn.10:42:35-10:42:36.log.gz        loaded_scripts.10:01:30-10:42:34.log.gz
conn.10:44:47-11:00:00.log.gz        loaded_scripts.10:42:37-11:00:00.log.gz
conn-summary.10:01:56-10:42:34.log.gz notice.10:03:24-10:42:34.log.gz
conn-summary.10:42:35-10:42:36.log.gz packet_filter.10:01:30-10:42:34.log.gz
conn-summary.10:44:47-11:00:00.log.gz packet_filter.10:42:37-11:00:00.log.gz
software.10:04:41-10:42:34.log.gz
ssl.10:01:51-10:42:34.log.gz
stats.10:01:30-10:42:34.log.gz
stats.10:42:37-11:00:00.log.gz
stderr.10:01:27-10:42:36.log.gz
stdout.10:01:27-10:42:36.log.gz
weird.10:01:36-10:42:34.log.gz
weird.10:42:46-11:00:00.log.gz
x509.10:01:51-10:42:34.log.gz
```

Nom i Cognoms	Data
Arnau Subirós Puigarnau	

### 3. [Kibana](#)

Kibana pot connectar-se directament a les dades de Elasticsearch i proporcionar visualitzacions potents per a guanyar context entorn dels registres de Bro.(ja que no ens serveix tenir moltes dades si no les sabem utilitzar)

