JESUÏTES El Clot
Escola del Clot

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.)

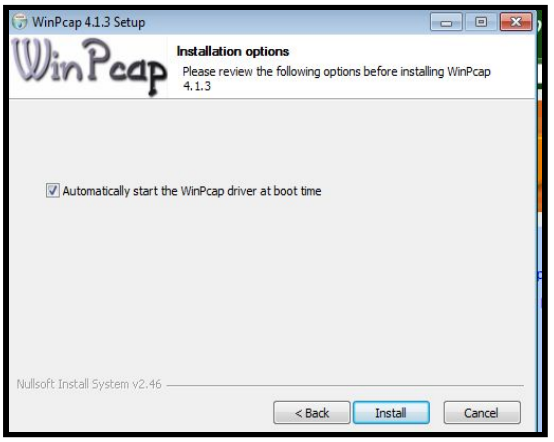
De les eines comentades una de les més significatives és el SNORT. Per tant, en un primer moment ens centrarem en aquesta.
Per fer-ho podem seguir el tutorial que s'adjunta en el següent link. Feu captures de pantalla del procés que aneu seguint. En aquest link trobareu com s'ha de realitzar la instal·lació 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

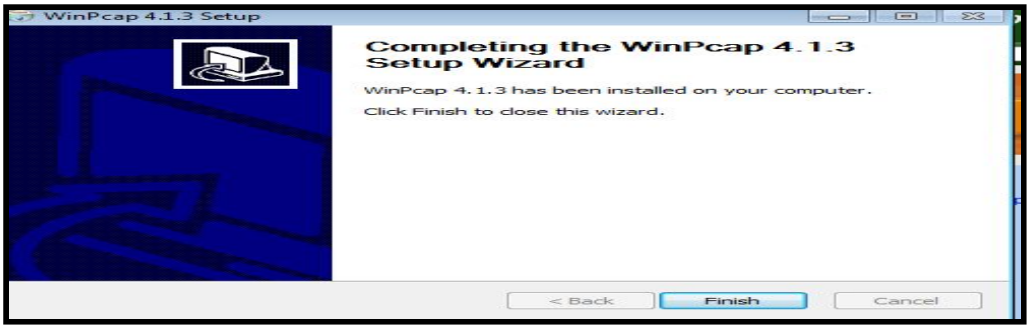
SNORT (Windows 7)

- En sistemes operatius Windows, primer de tot s'ha d'instal.lar **WinPcap (**www.winpcap.org**)**
  - **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

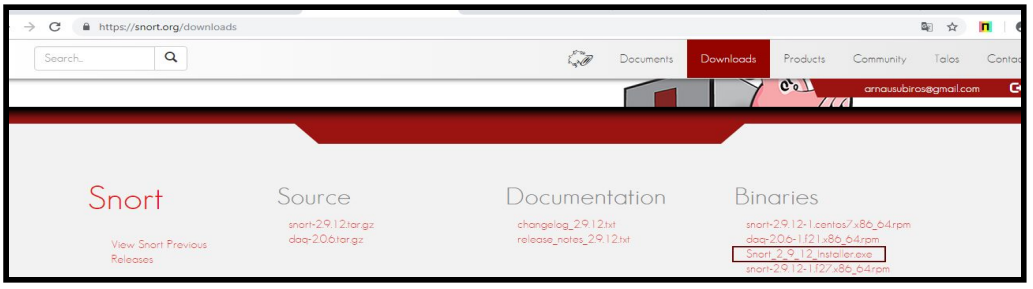


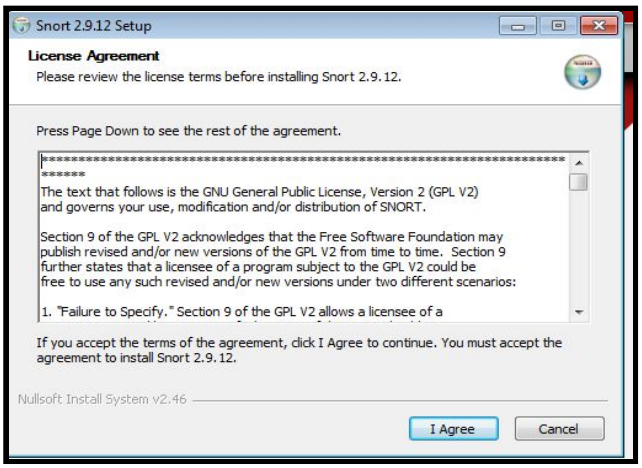


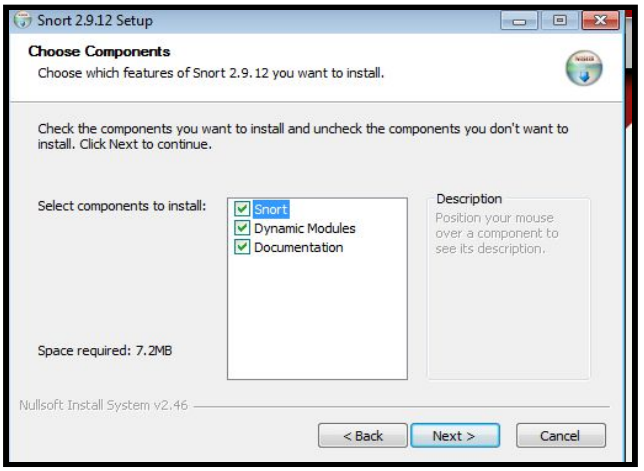
Nom i Cognoms **Data**

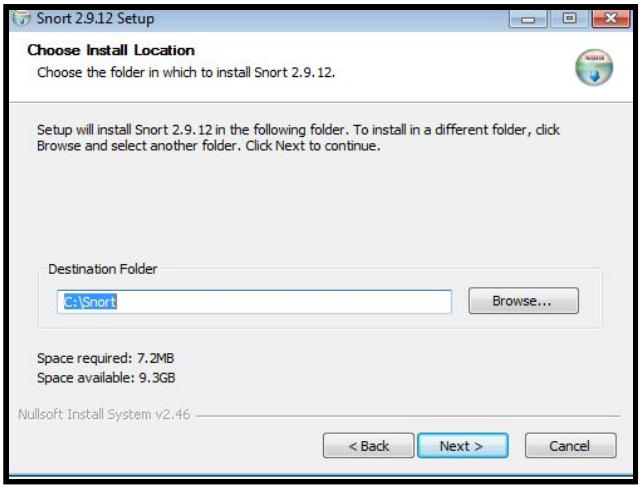
Arnau Subirós Puigarnau

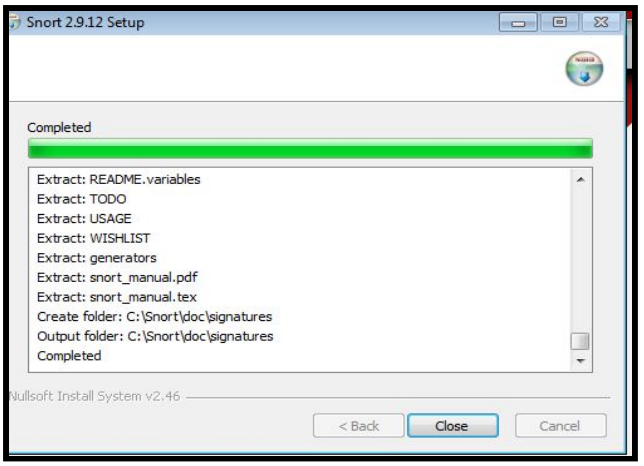
- Ens descarguem e instal.lem **SNORT** (www.snort.org)





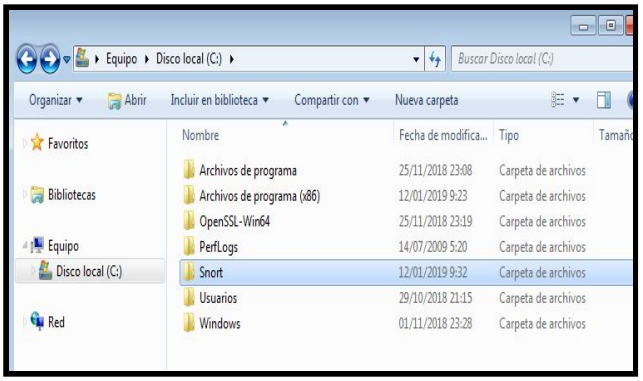


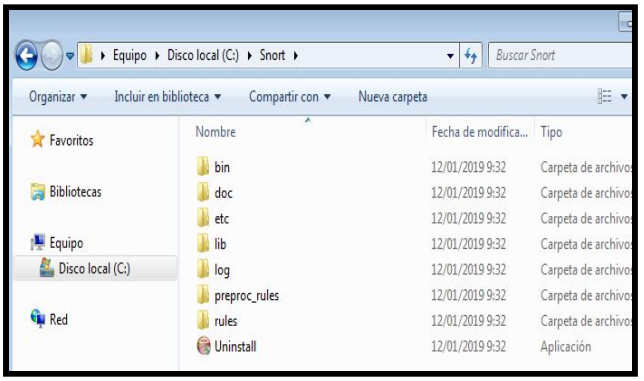




Nom i Cognoms **Data**

Arnau Subirós Puigarnau

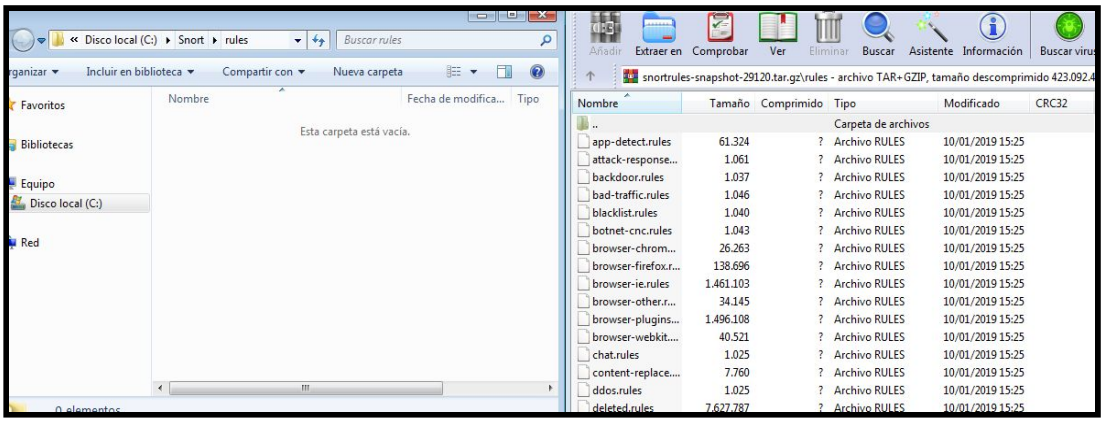




- Durant la instal·lació de Snort crea una estructura de directoris en C: \ Snort :
  - C: \snort \ bin directori on es troba l'executable de l'eina
  - C: \ snort \ contrib
  - C: \snort \ doc documentació de l'eina
  - C: \snort \ etc directori principal per als arxius de configuració
  - C: \snort \ log
  - C: \snort\ rules jocs de regles (al descargar SNORT la carpeta està buida, per això ens hem de descargar-les després)

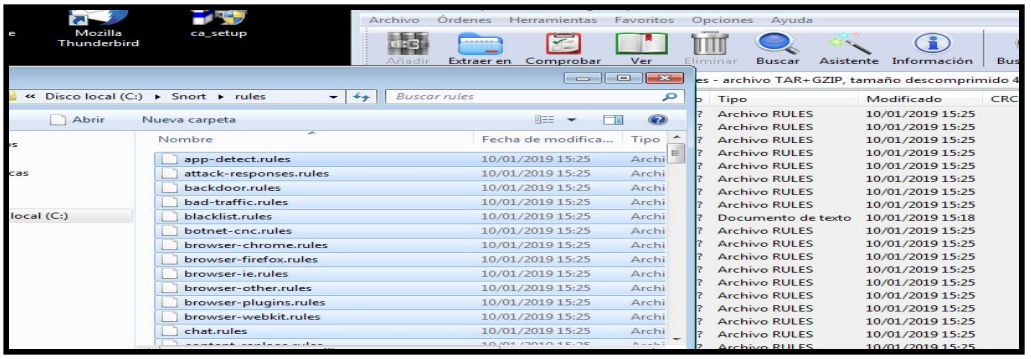
- El primer que hem de fer és accedir a la carpeta C:\Snort\etc en aquest directori trobarem un fitxer anomenat snort.conf,que és el fitxer de configuració que utilitzarem per a configurar Snort. Accedim al fitxer amb un editor de text que no corrompi el format original de l'arxiu (per ejemple notepad++)

- Ens hem de descargar les regles i hem de sobreescriure 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

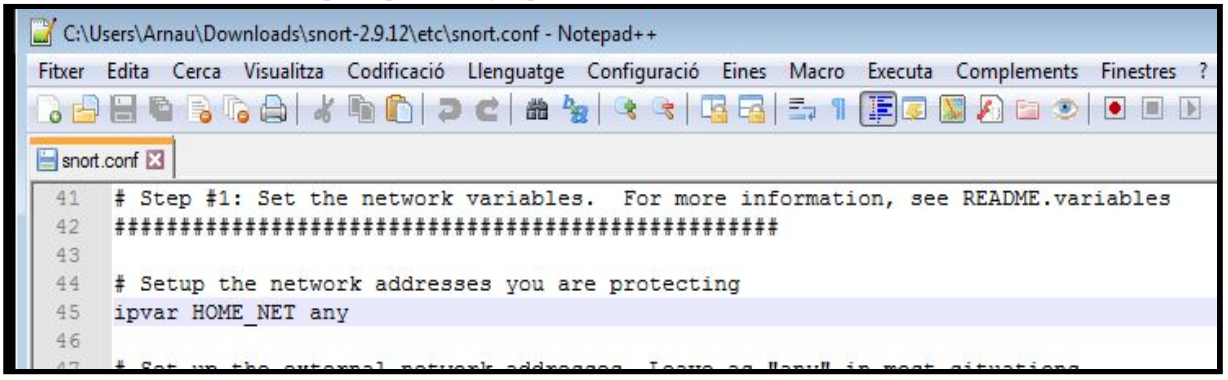


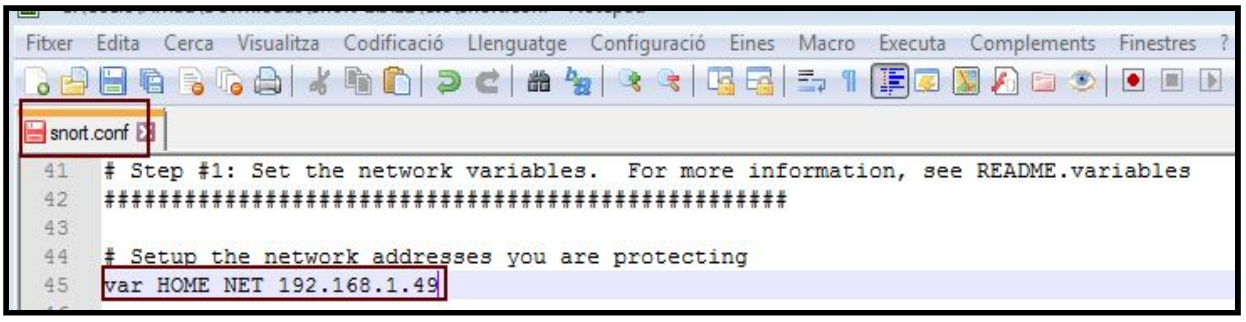
- Anirem al directori a on està instal.lat SNORT per editar l'arxiu de configuració amb notepad++ .E**n el meu cas c:\Snort\etc\snort.conf**

STEPS de l'arxiu SNORT.CONF

STEP 1

- Cambiem **ipvar** per **var** (ja que ivar s'utiliza 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
```

```
47  # Set up the external network addresses. Leave as "any" in most situations
48  var EXTERNAL_NET !$HOME_NET
49
```

➢ 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
```

```
snort.conf
183
184  # Configure default log directory for snort to log to.  For more informa
185  #
186
187  config logdir c:\snort\log
188
189
190  ##################################################
191  # Step #3: Configure the base detection engine.  For more information, s
```

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)

➢ Aqui es configuren algunes llibreries que Snort carga quan arranca

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

```
56  ##################################################
57  # Step #5: Configure preprocessors
58  # For more information, see the Snort Manual, Configuring Snort - Preproce
59  ##################################################
60
61  # GTP Control Channle Preprocessor. For more information, see README.GTP
62  # preprocessor gtp: ports { 2123 3386 2152 }
63
64  # Inline packet normalization. For more information, see README.normalize
65  # Does nothing in IDS mode
66  preprocessor normalize_ip4
67  preprocessor normalize_tcp: ips ecn stream
68  preprocessor normalize_icmp4
69  preprocessor normalize_ip6
70  preprocessor normalize_icmp6
71
72  # Target-based IP defragmentation.  For more inforation, see README.frag3
```

```
63
64  # Inline packet normalization. For more information, see README.normalize
65  # Does nothing in IDS mode
66  #preprocessor normalize_ip4
67  #preprocessor normalize_tcp: ips ecn stream
68  #preprocessor normalize_icmp4
69  #preprocessor normalize_ip6
70  #preprocessor normalize_icmp6
```

➢ Deixarem comentada una altre linea

```
preprocessor rpc_decode: 111

# Back Orifice detection.
preprocessor bo
```

```
334
335  # Back Orifice detection.
336  #preprocessor bo
337
```

Nom i Cognoms **Data**

Arnau Subirós Puigarnau

➢ S'activarà alerta escaneig de ports (la línea de codi estava comentada)

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

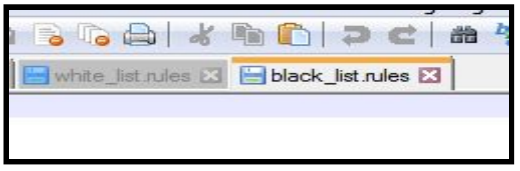
```
# Portscan detection.  For more information, see README.sfportscan
preprocessor sfportscan: proto  { all } memcap { 10000000 } sense_level { low }
```

➢ 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
```

```
05    check_crc
06
07  # Reputation preprocessor. For more information see README.reputation
08  preprocessor reputation: \
09     memcap 500, \
10     priority whitelist, \
11     nested_ip inner, \
12     whitelist $WHITE_LIST_PATH\white_list, \
13     blacklist $BLACK_LIST_PATH\black_list
14
```

- Tindrem que crear l' arxius(black_list.rules and white_list.rules a c:\Snort\rules



Nom i Cognoms **Data**

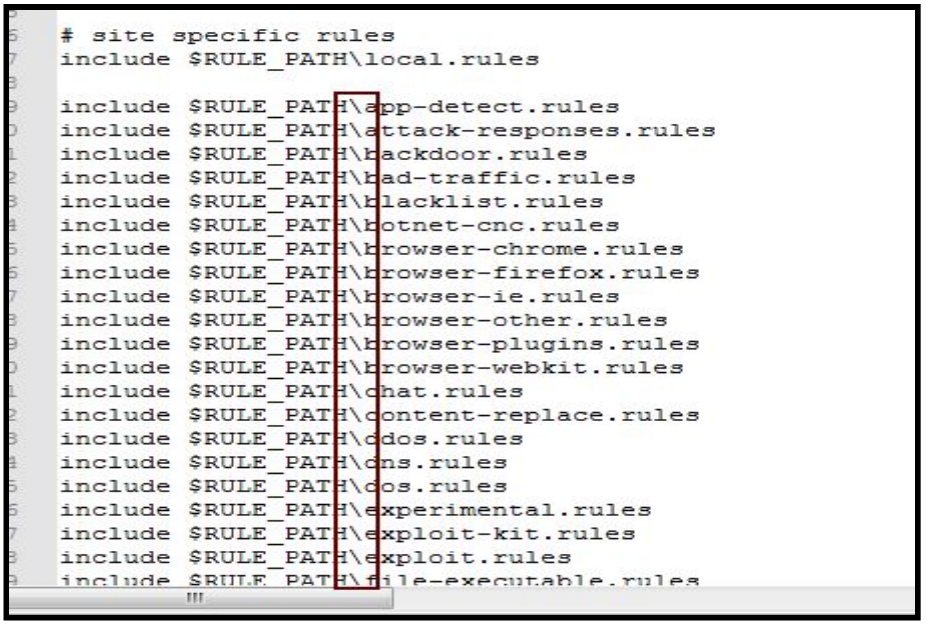
Arnau Subirós Puigarnau

STEP 6 (no fer res, només per Linux)

STEP 7

- Descomentarem les línes per activar les regles
- si uses 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
```



```
6   # site specific rules
7   include $RULE_PATH\local.rules
8
9   include $RULE_PATH\app-detect.rules
0   include $RULE_PATH\attack-responses.rules
1   include $RULE_PATH\backdoor.rules
2   include $RULE_PATH\bad-traffic.rules
3   include $RULE_PATH\blacklist.rules
4   include $RULE_PATH\botnet-cnc.rules
5   include $RULE_PATH\browser-chrome.rules
6   include $RULE_PATH\browser-firefox.rules
7   include $RULE_PATH\browser-ie.rules
8   include $RULE_PATH\browser-other.rules
9   include $RULE_PATH\browser-plugins.rules
0   include $RULE_PATH\browser-webkit.rules
1   include $RULE_PATH\chat.rules
2   include $RULE_PATH\content-replace.rules
3   include $RULE_PATH\ddos.rules
4   include $RULE_PATH\dns.rules
5   include $RULE_PATH\dos.rules
6   include $RULE_PATH\experimental.rules
7   include $RULE_PATH\exploit-kit.rules
8   include $RULE_PATH\exploit.rules
9   include $RULE_PATH\file-executable.rules
```

Nom i Cognoms **Data**

Arnau Subirós Puigarnau

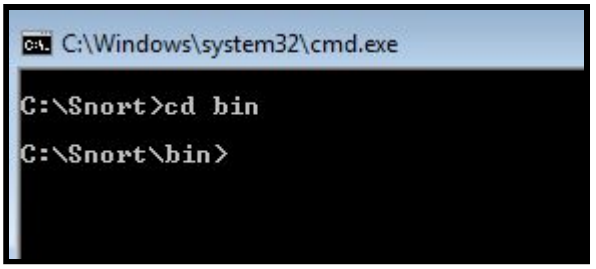
STEP 8

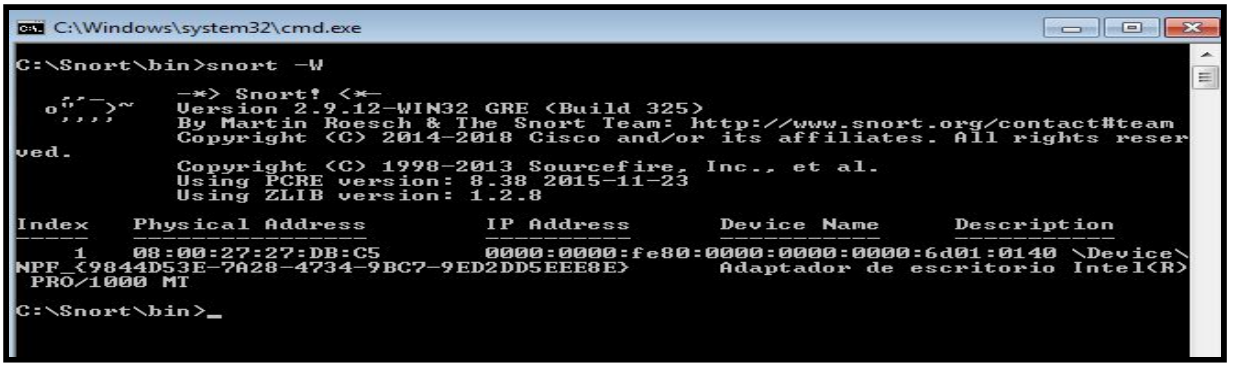
➢ s'activaran els següents preprocessors

```
653
654  ##################################################
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

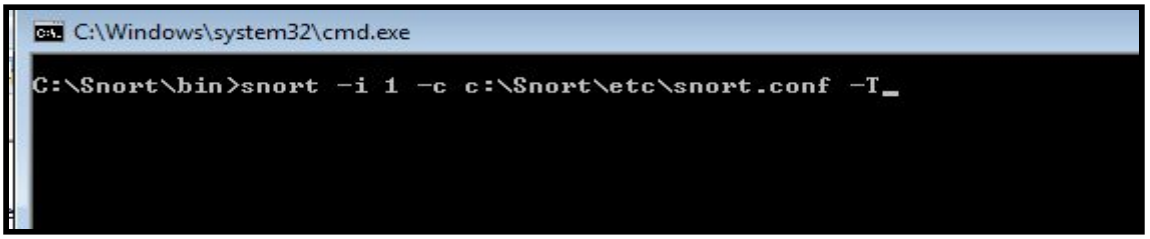


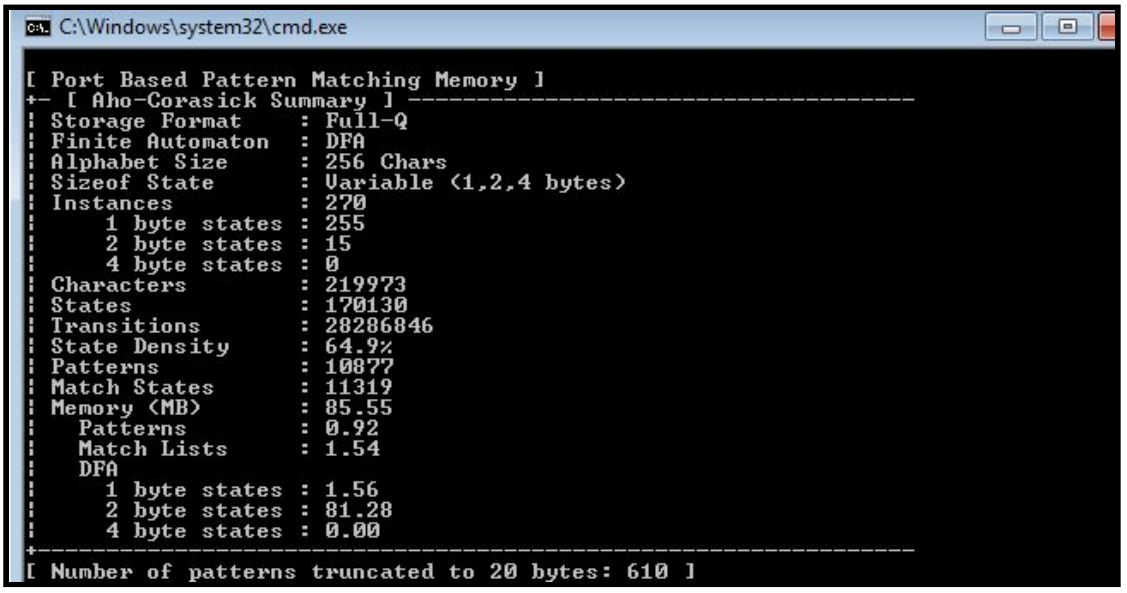


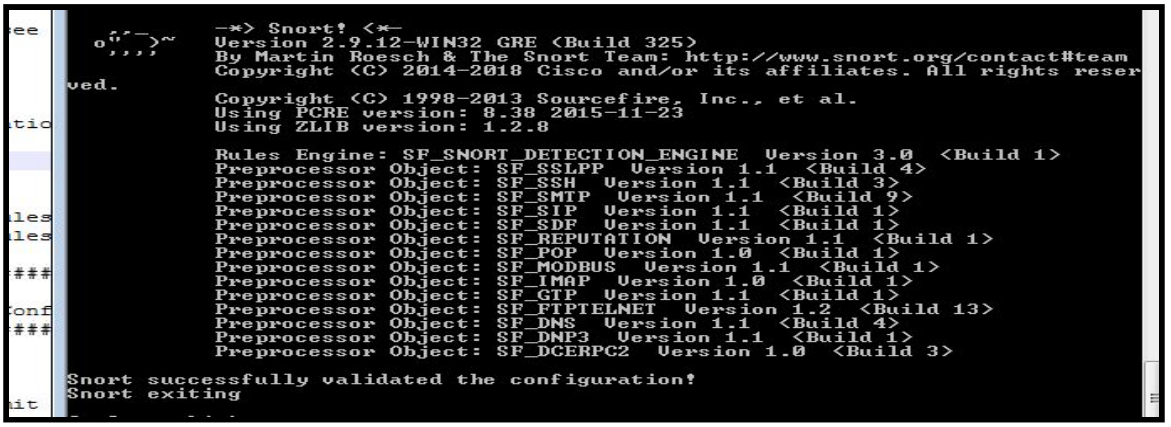
Nom i Cognoms **Data**

Arnau Subirós Puigarnau

- Ara hem de verificar que tenim un configuració red válida





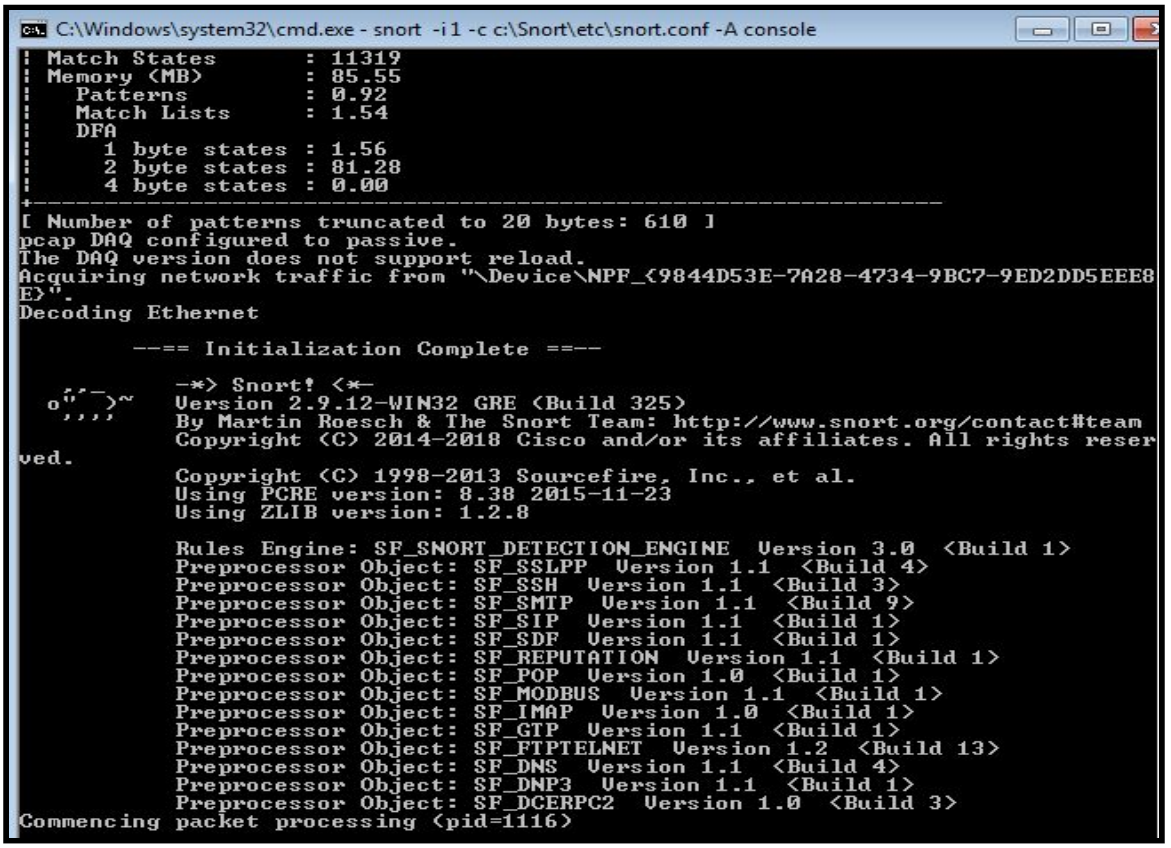


Nom i Cognoms **Data**

Arnau Subirós Puigarnau

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

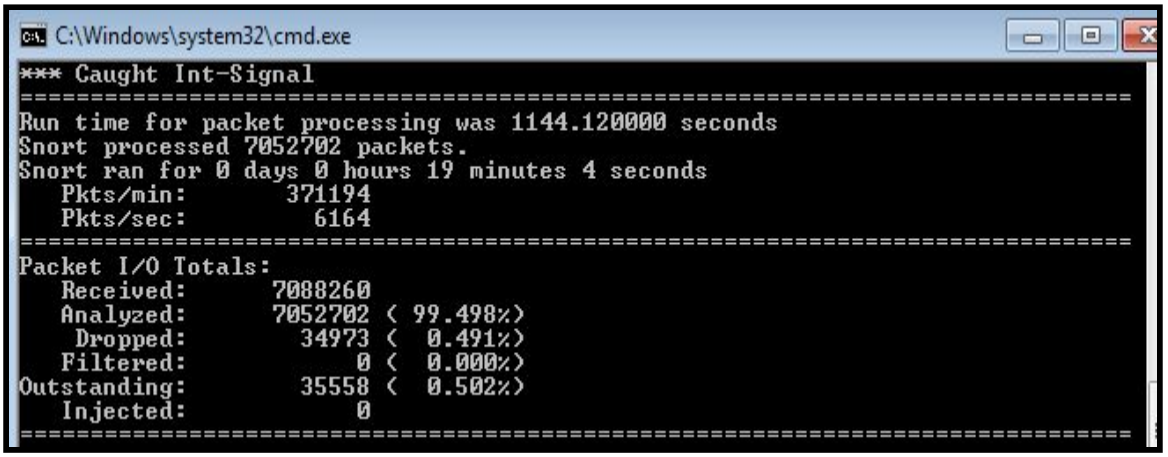
  ➢ C:\Snort\bin> **snort -i 1 -c c:\Snort\etc\snort.conf -A console**

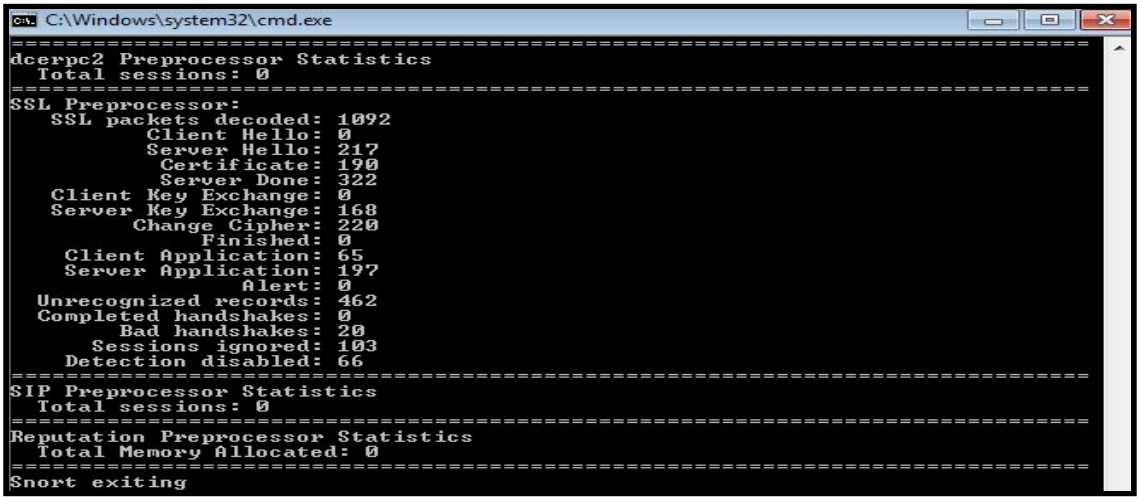


Nom i Cognoms **Data**

Arnau Subirós Puigarnau

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



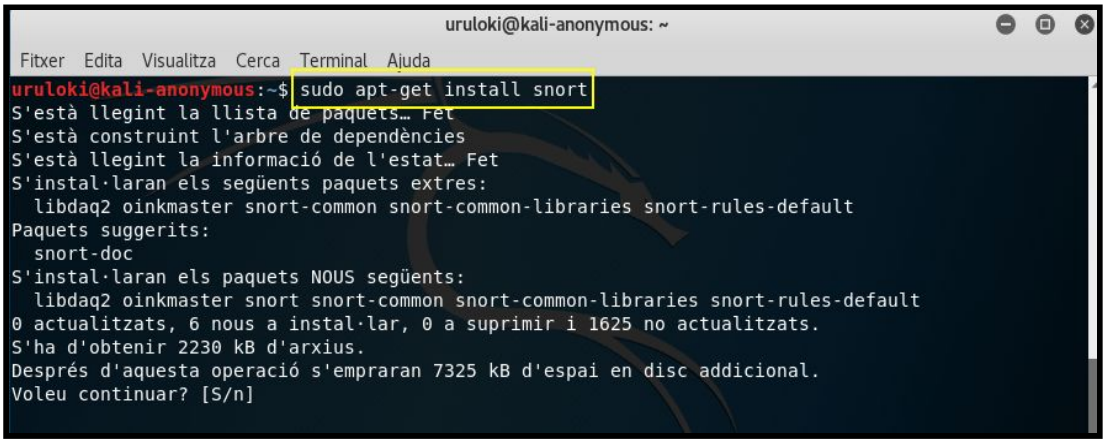


Nom i Cognoms **Data**

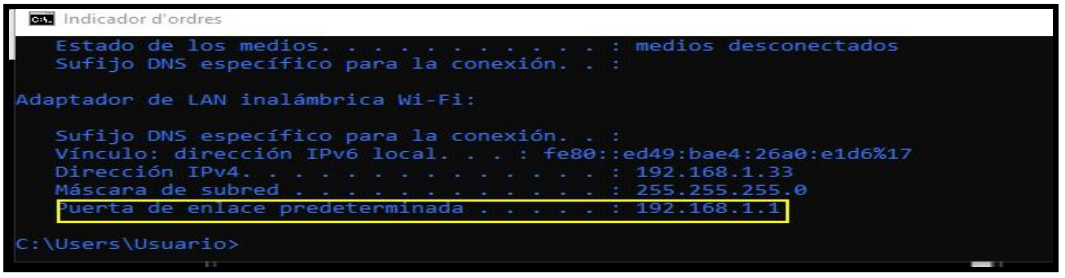
Arnau Subirós Puigarnau

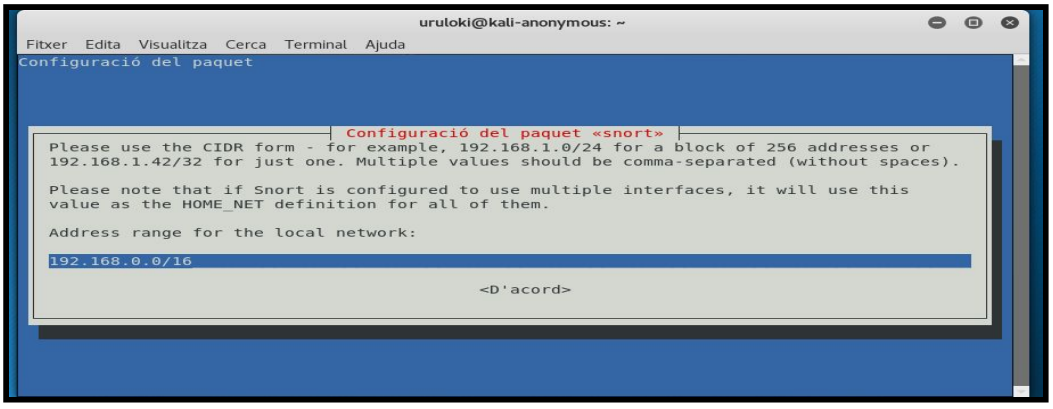
SNORT (Kali Linux)

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 varies modificaciones adiccionals i instal.lar un altre software.



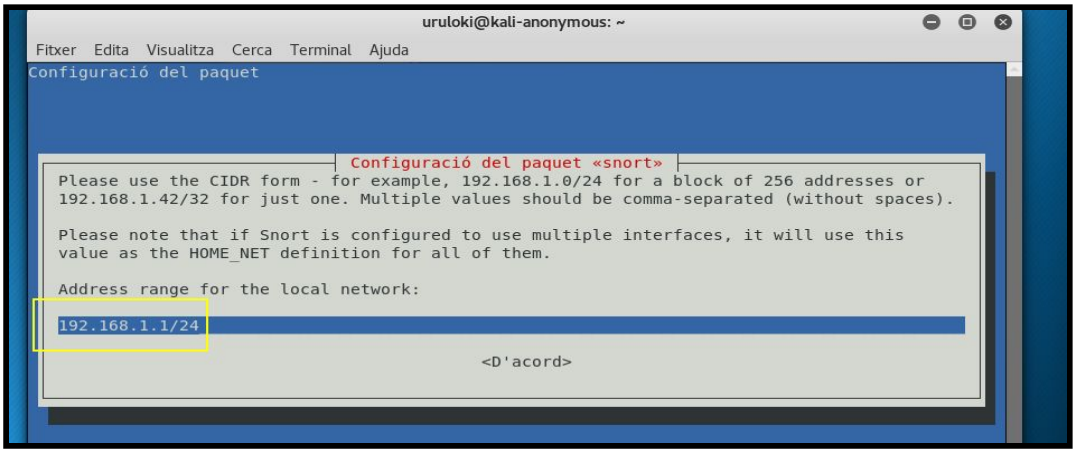
Revisem la IP de la gateway de l'ordinador físic

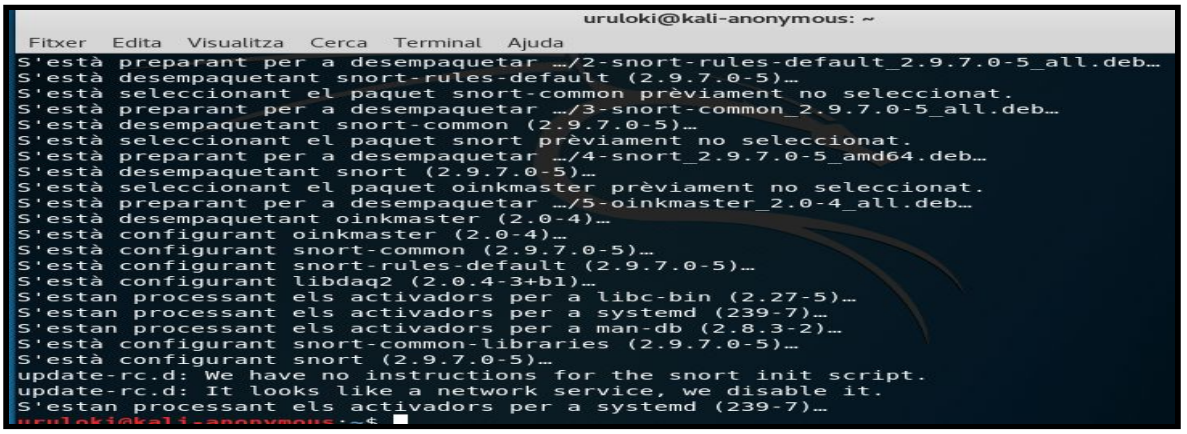




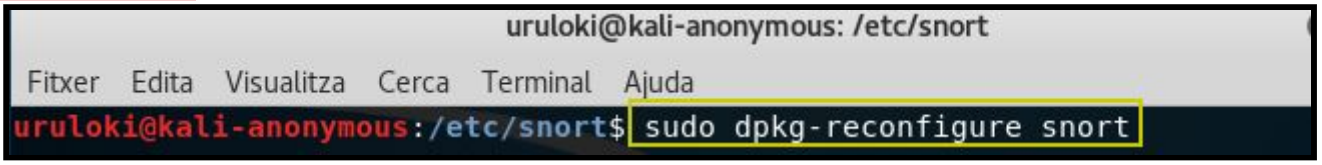
Nom i Cognoms **Data**

Arnau Subirós Puigarnau





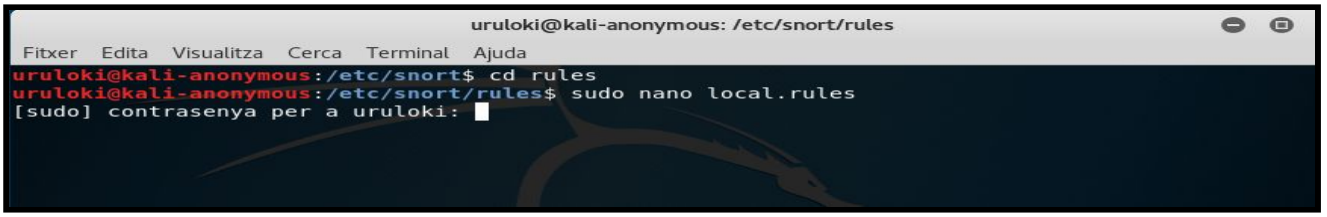
IMPORTANT!!! la instal.lació s'ha fet a la red de casa on la gateway es 192.168.1.1. Un cop instal.lat i donat el cas que estic a una altre red(la de l'escola on la seva gateway és 172.20.23.254, hauriem de reconfigurar amb el comando

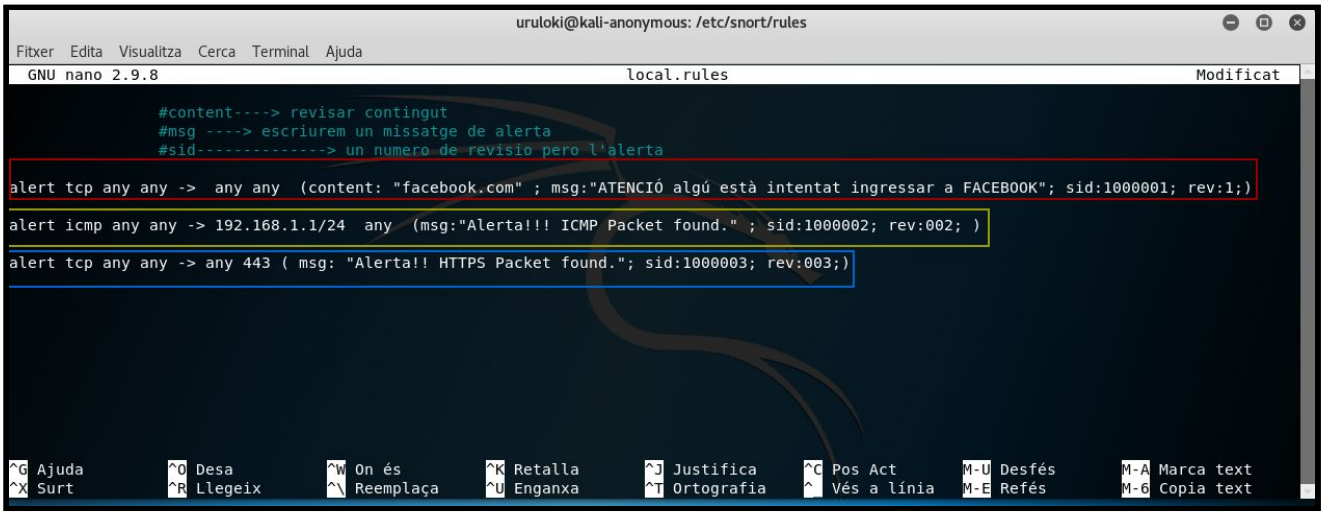


Nom i Cognoms **Data**

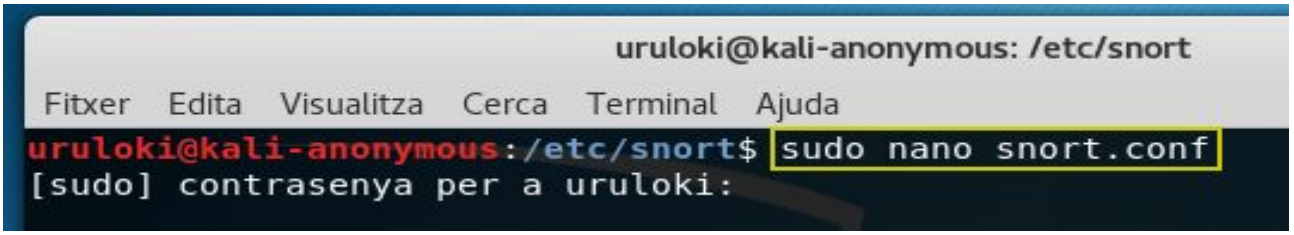
Arnau Subirós Puigarnau

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



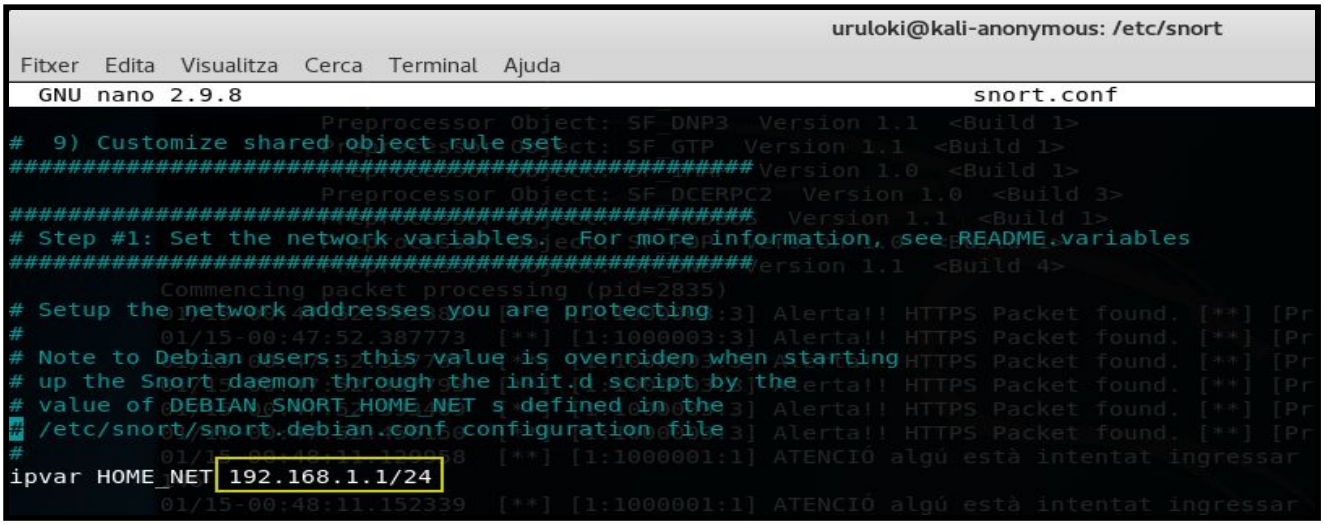


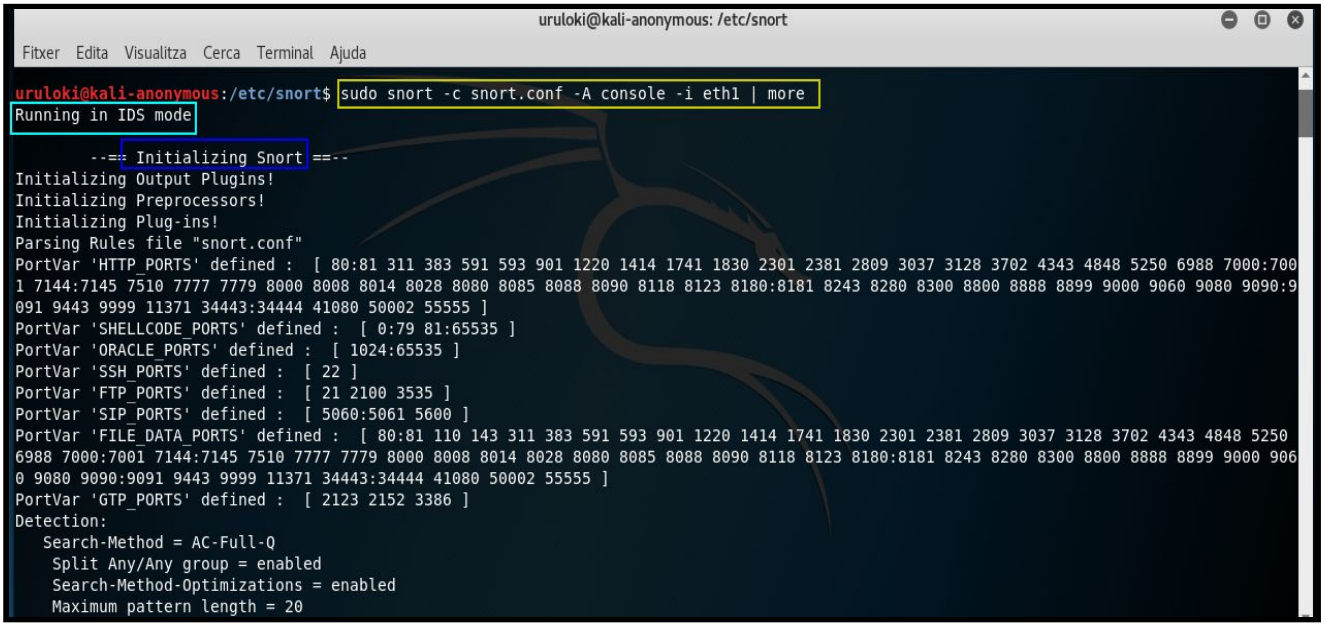
Accedirem a l'arxiu de configuració de Snort, **snort.conf** on afegirem la **IP del nostre gateway**



Nom i Cognoms **Data**

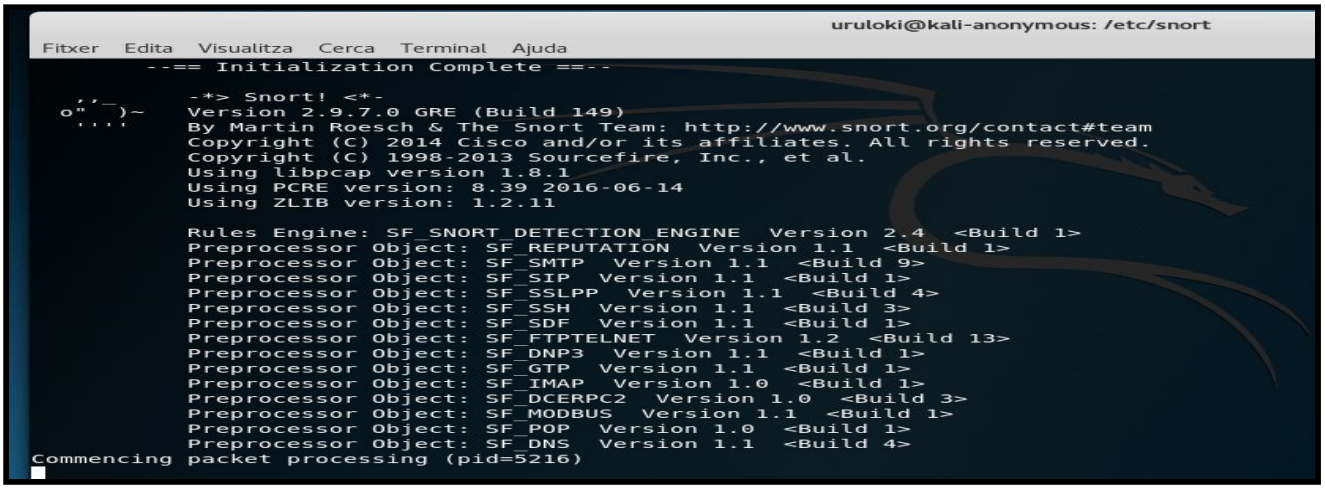
Arnau Subirós Puigarnau





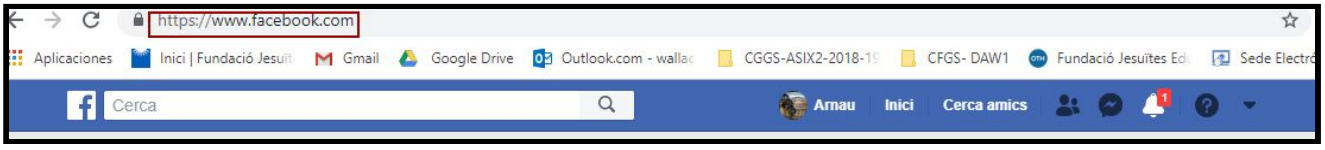
Nom i Cognoms **Data**

Arnau Subirós Puigarnau

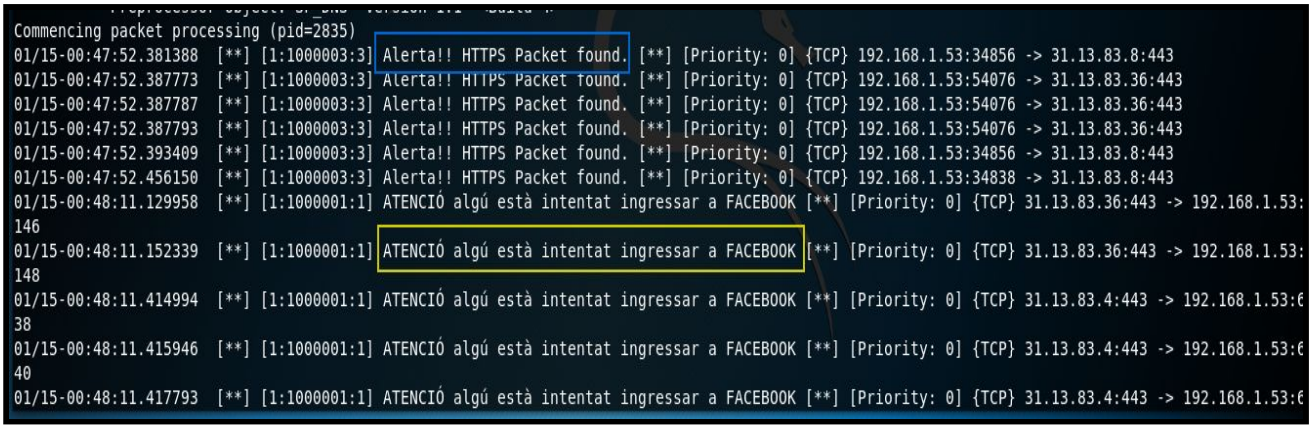


PROVES amb l'IDS SNORT

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



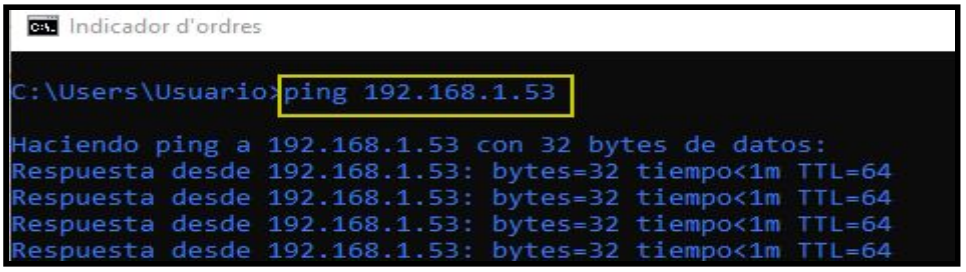
S'han activat 2 alertes : que estàn accedint a una conexio https(port 443) i s' està ingressant al facebook

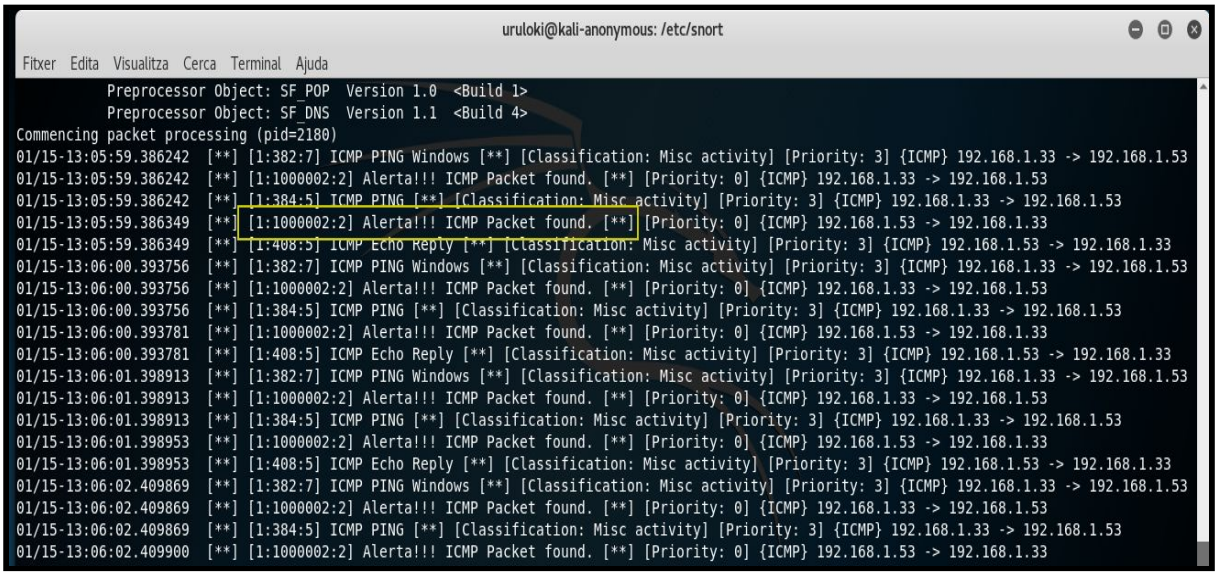


Nom i Cognoms **Data**

Arnau Subirós Puigarnau

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





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 sguil (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

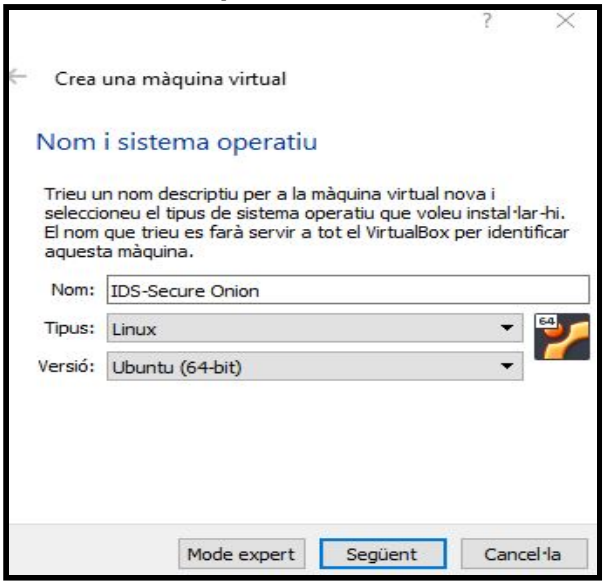
Procés d'instal.lació de Secure Onion

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 defecte 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).

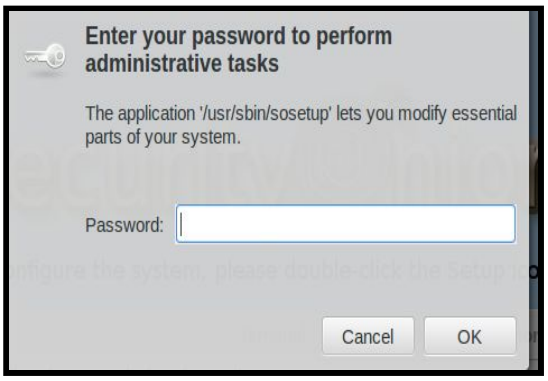
A continuació procedim a instal.lar la màquina virtual

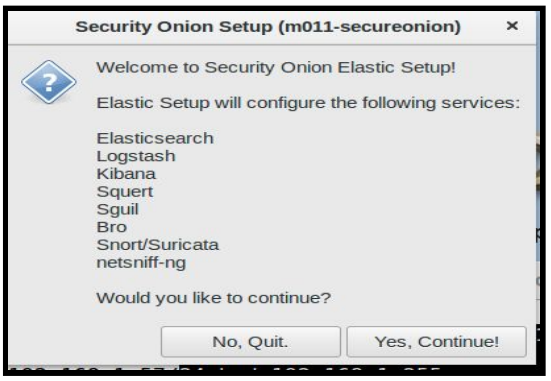


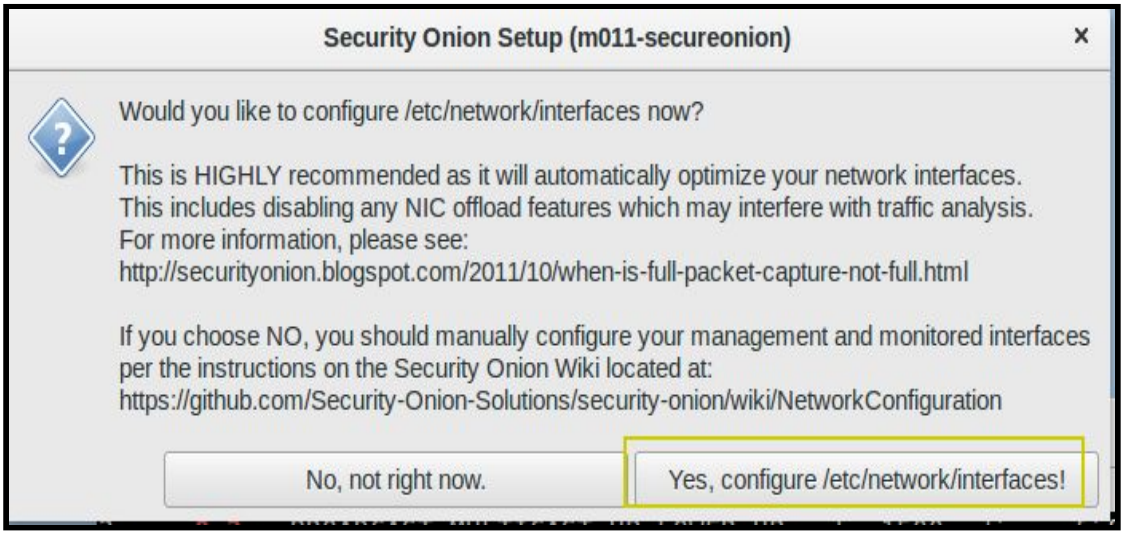
Nom i Cognoms **Data**

Arnau Subirós Puigarnau

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



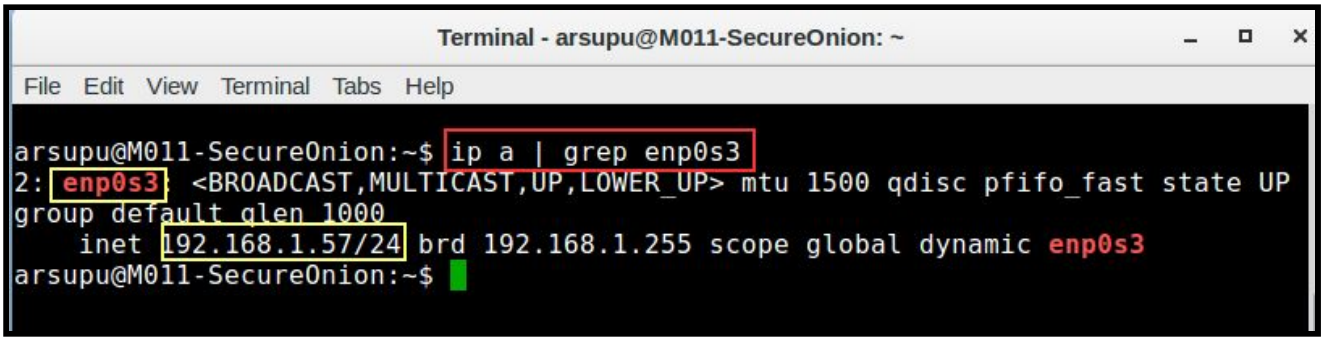




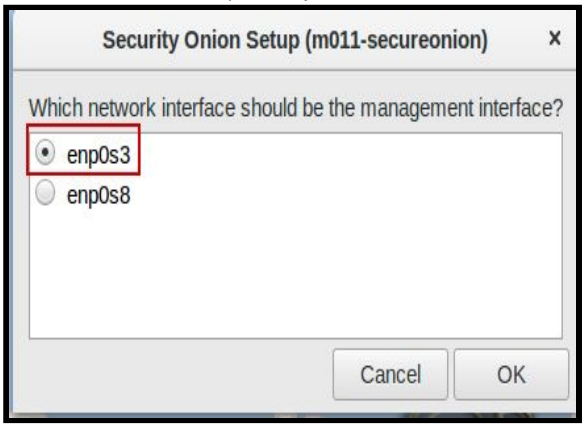
Nom i Cognoms **Data**

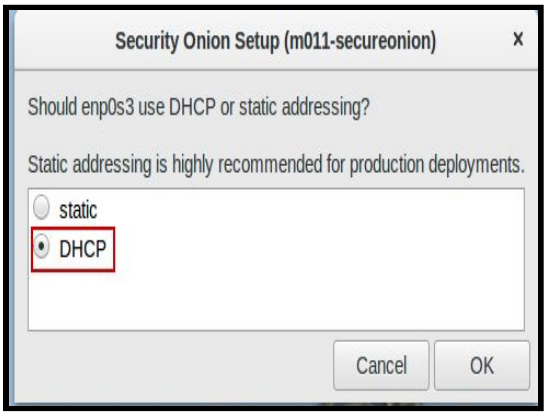
Arnau Subirós Puigarnau

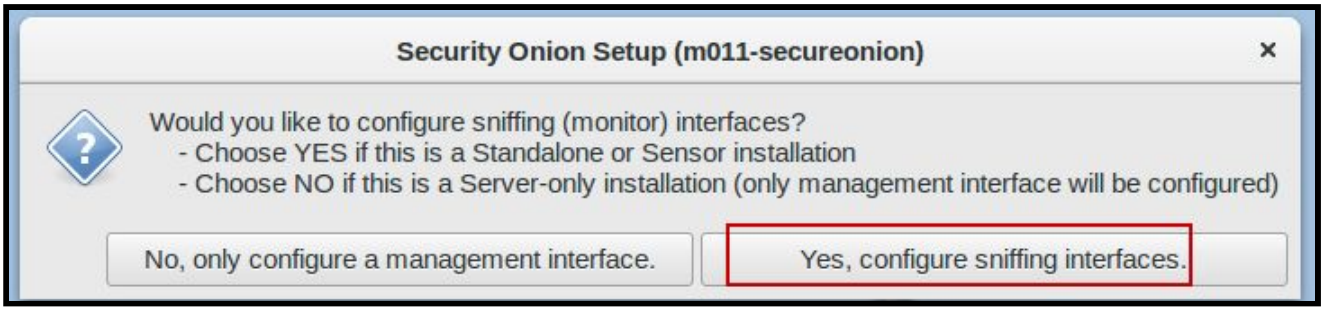
Abans de continuar, obriré el terminal per saber la interfície i la meva IP privada



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



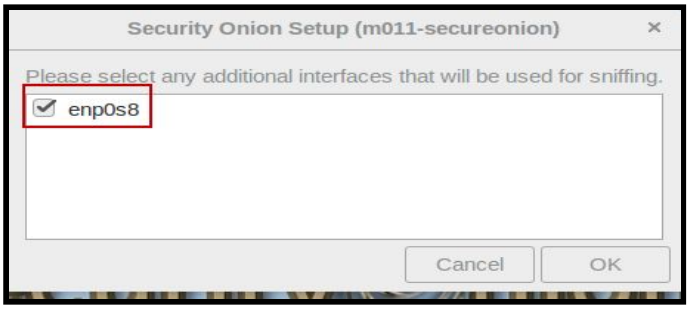


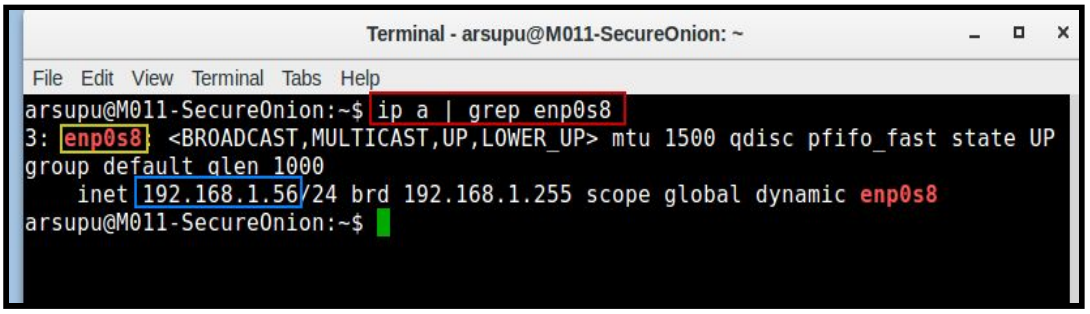


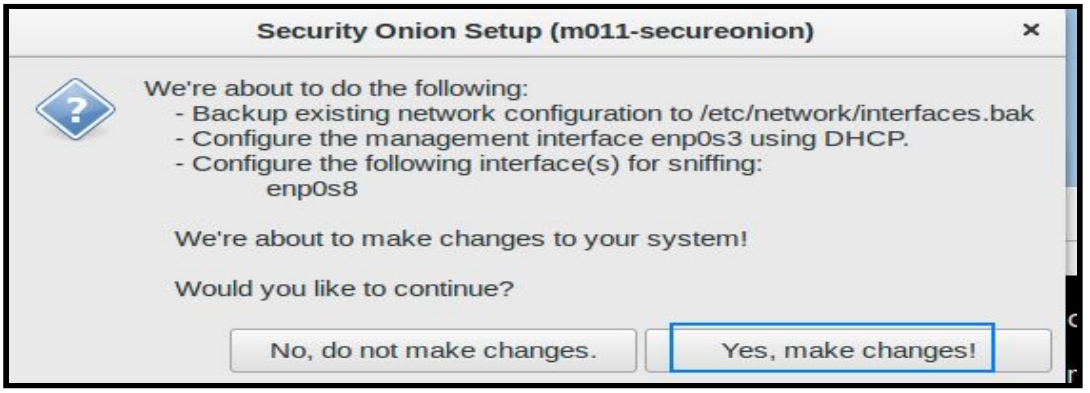
Nom i Cognoms **Data**

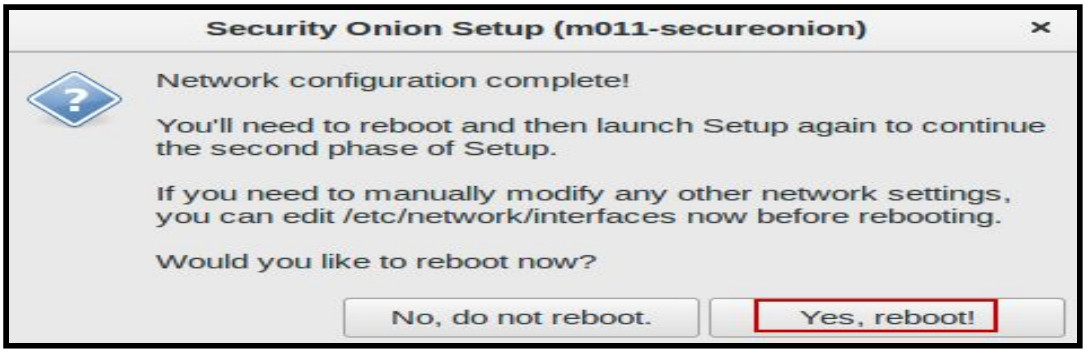
Arnau Subirós Puigarnau

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





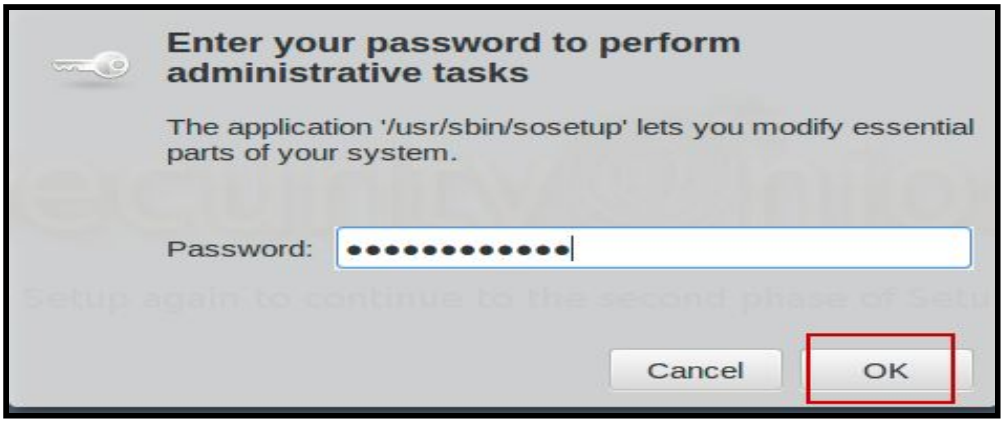




Nom i Cognoms **Data**

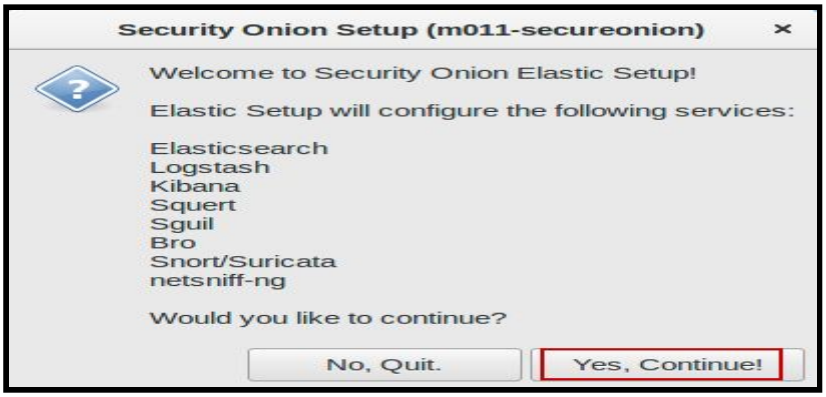
Arnau Subirós Puigarnau

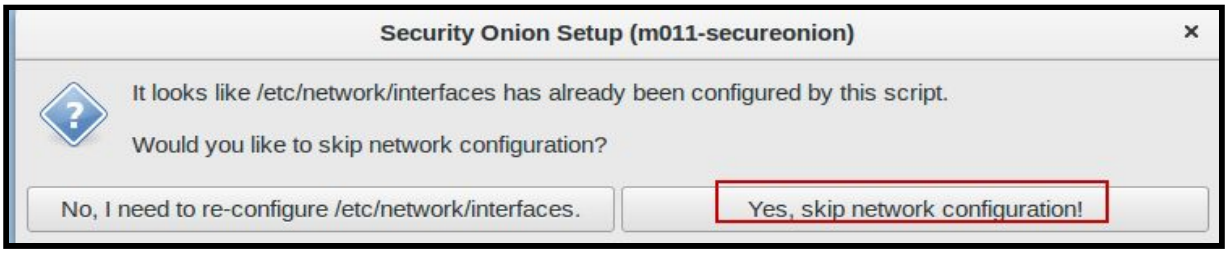
Després de reiniciar , en el fons de pantalla em demana que torni a utilitzar setup per la 2 fase la configuració



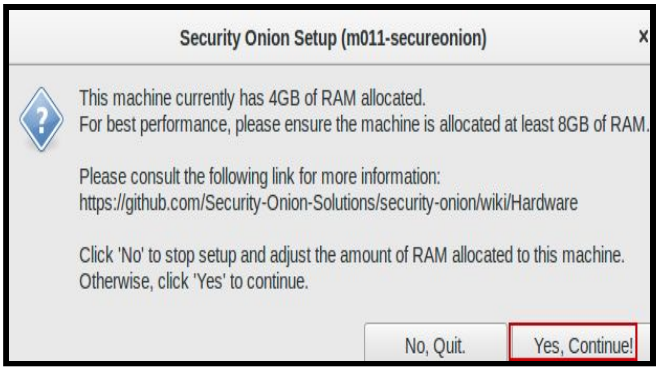
Nom i Cognoms **Data**

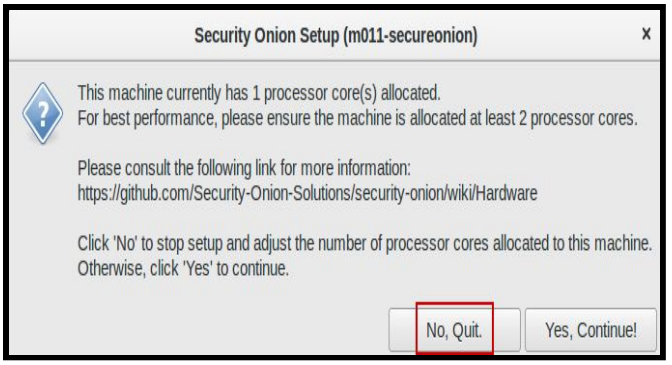
Arnau Subirós Puigarnau





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 configuracio per ampliar la memoria de la màquina, per evitar problemes posteriors.

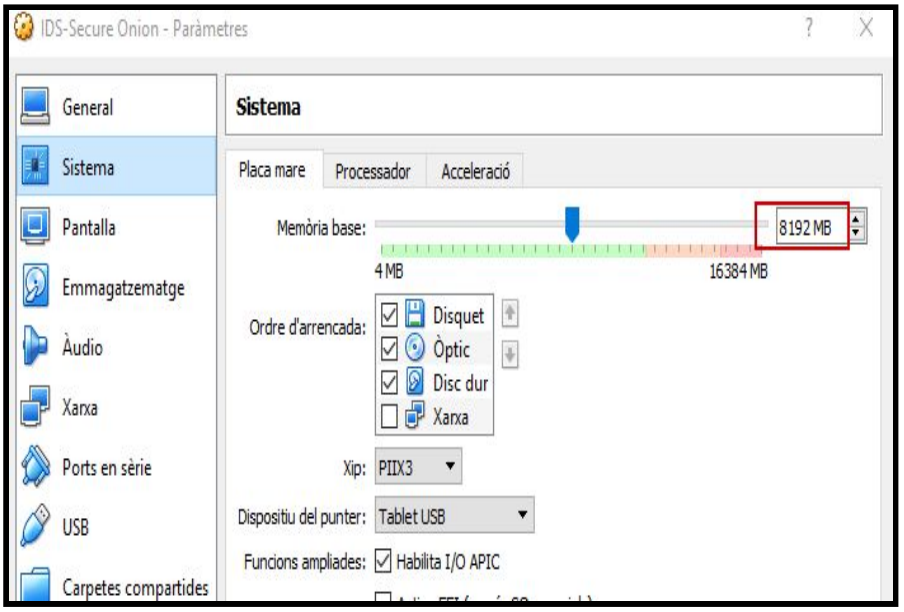




Nom i Cognoms **Data**

Arnau Subirós Puigarnau

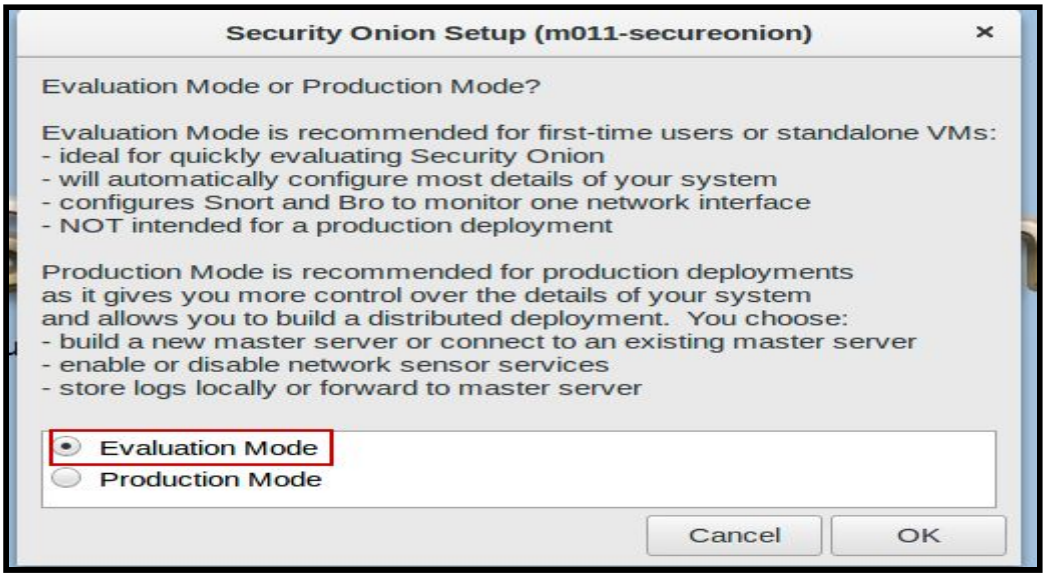
Un cop afegit 4 gb més de memoria ram i 1 processador més, torno a engegar la màquina i seguiré amb l'instal.lació(2 fase).

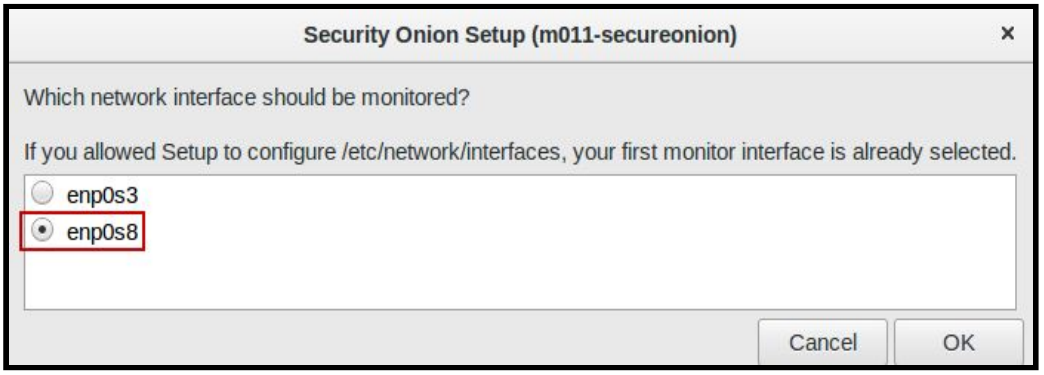


Nom i Cognoms **Data**

Arnau Subirós Puigarnau

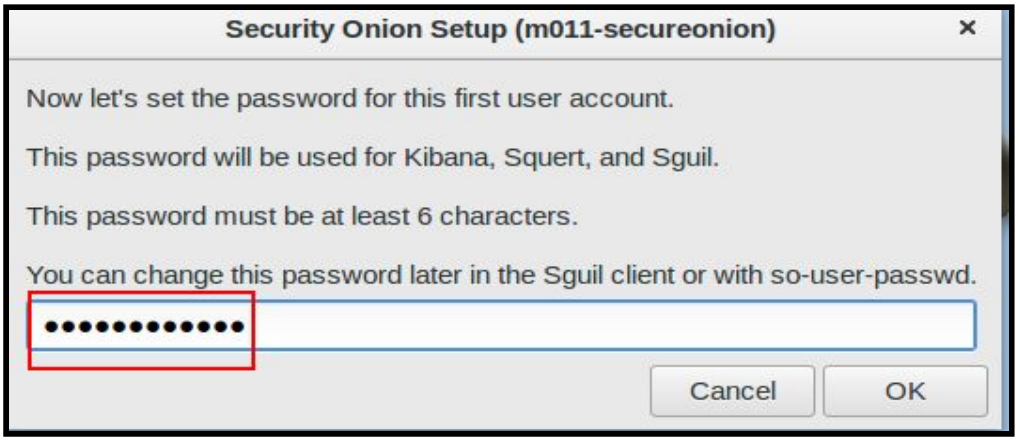
A continuació mostraré desde a partir del **"No, Quit",** en la cancel.lació de la configuració(per evitar fer captures repetides)

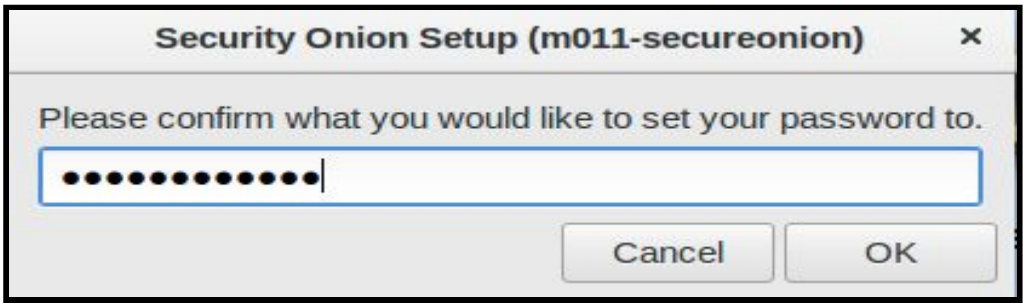


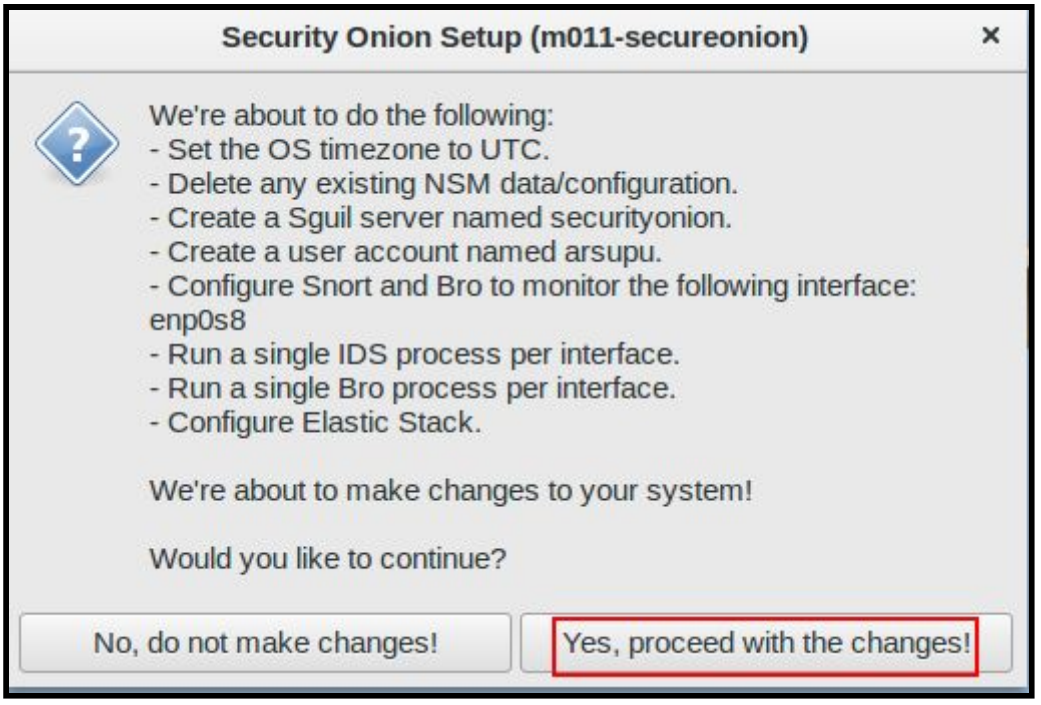


Nom i Cognoms **Data**

Arnau Subirós Puigarnau

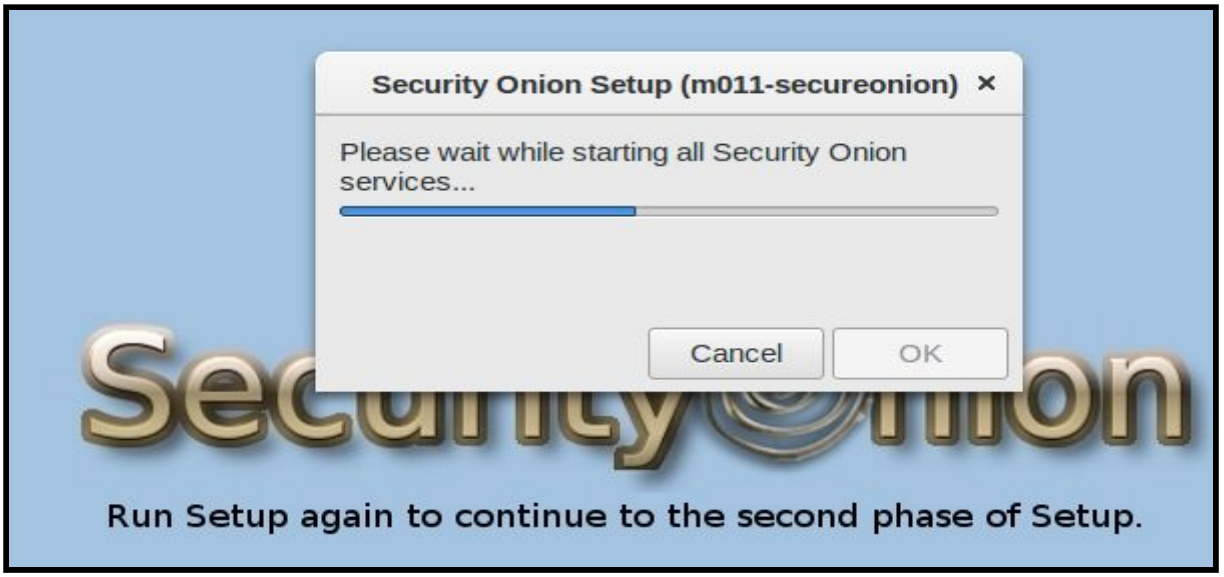




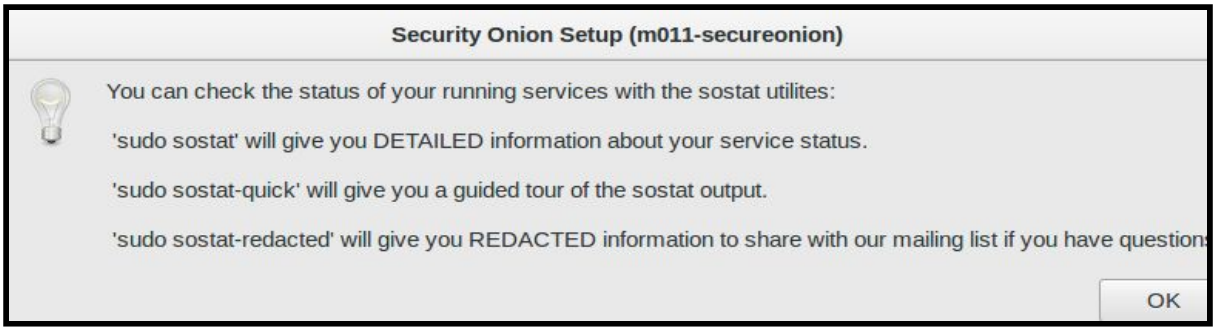


Nom i Cognoms **Data**

Arnau Subirós Puigarnau

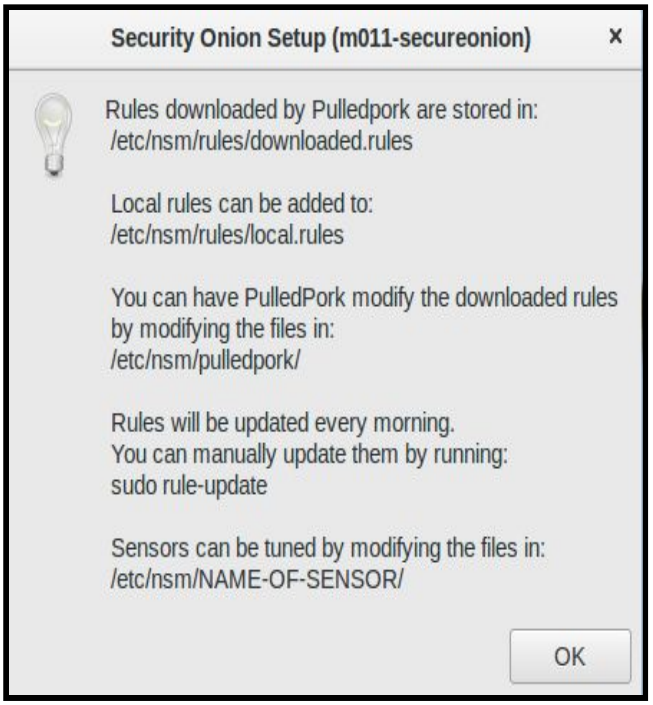


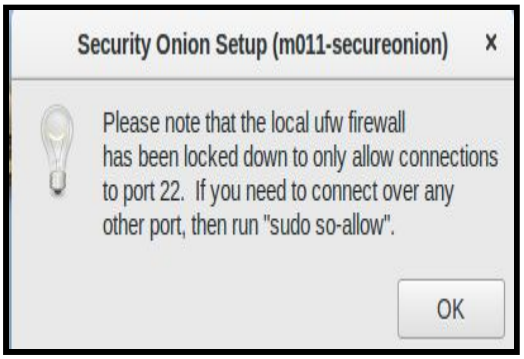
Abans d'acabar es mostren varis missatges d'ajuda i recomenacions (per veure ,status, regles, el port i informació de links per suport comercial)



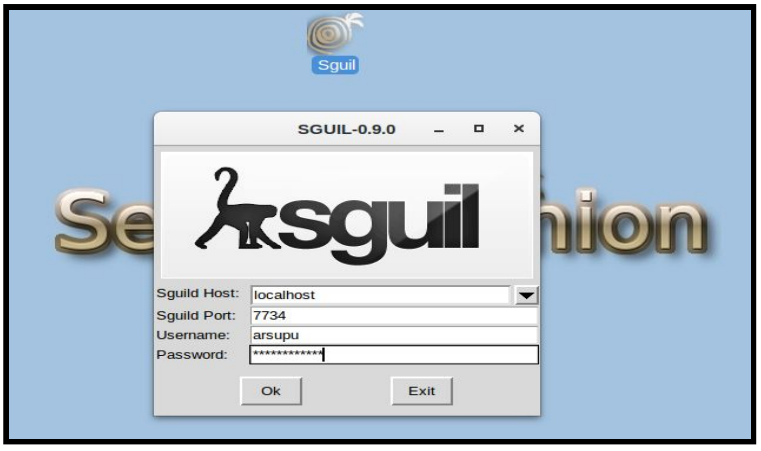
Nom i Cognoms **Data**

Arnau Subirós Puigarnau



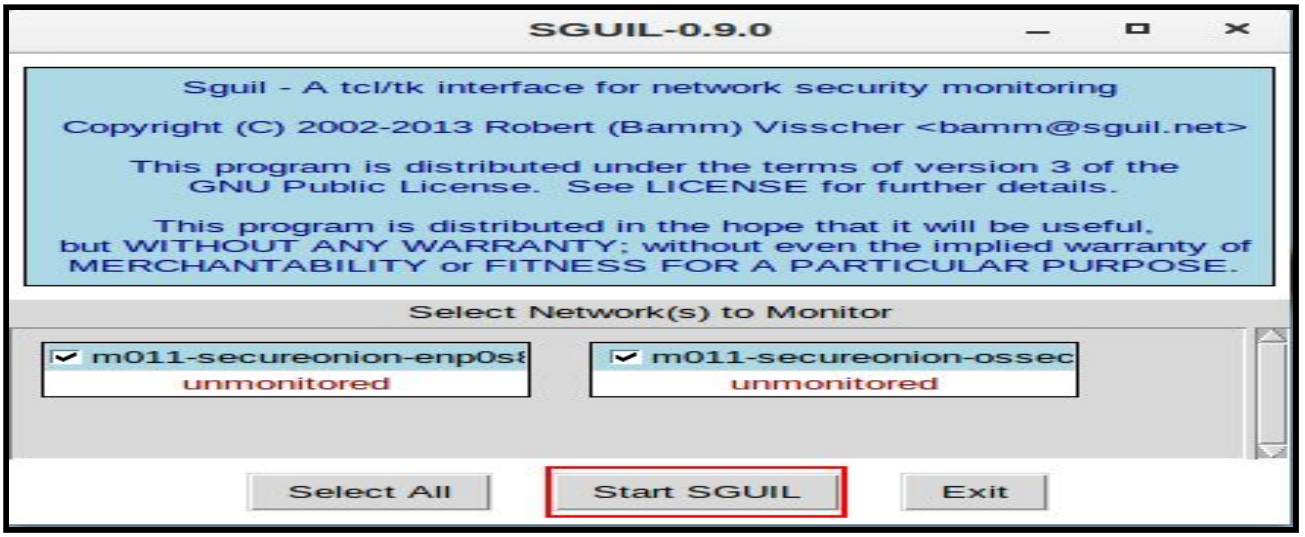


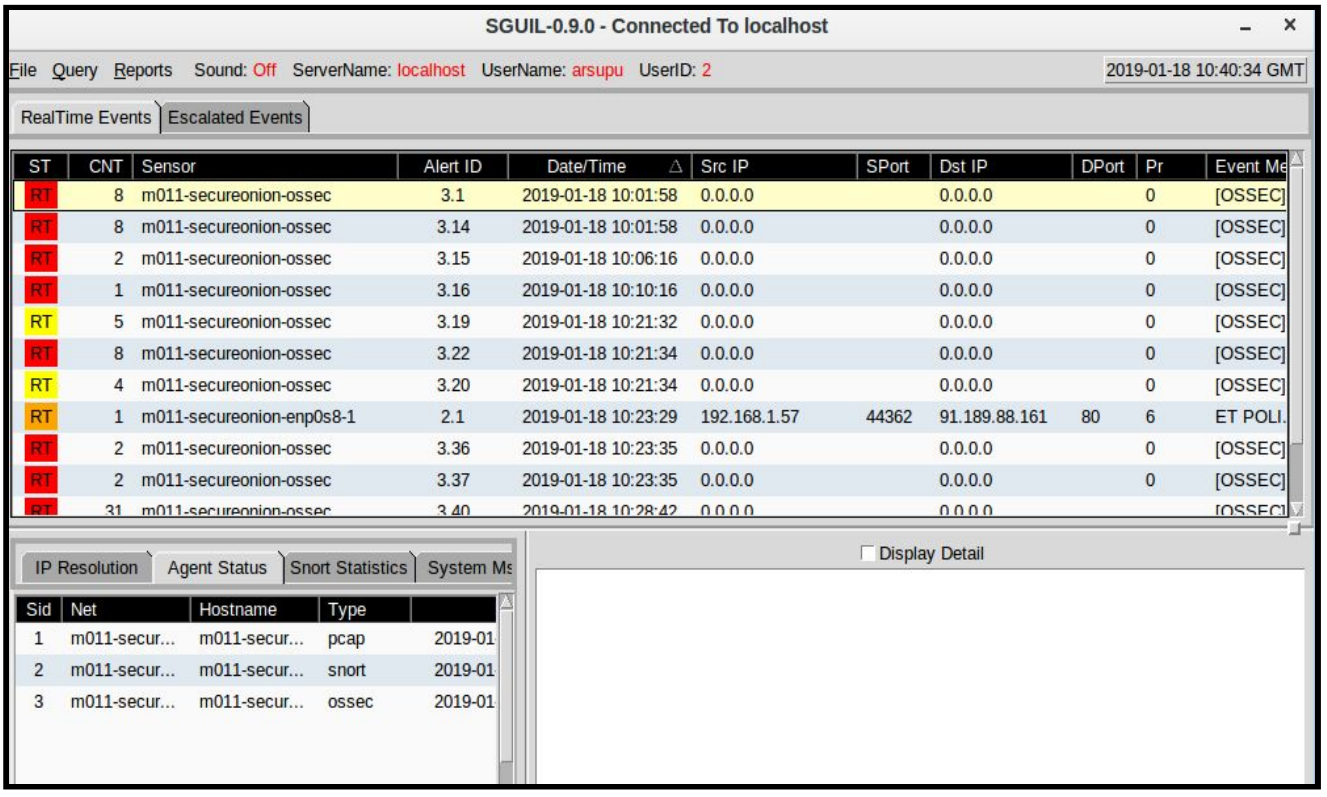
Un cop instal.lat SECURE ONION obrim el SGUIL que és un software per monitoritzar la seguretat a la red (NSM) i l'anàlisis de l'alertes IDS



Nom i Cognoms **Data**

Arnau Subirós Puigarnau





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.

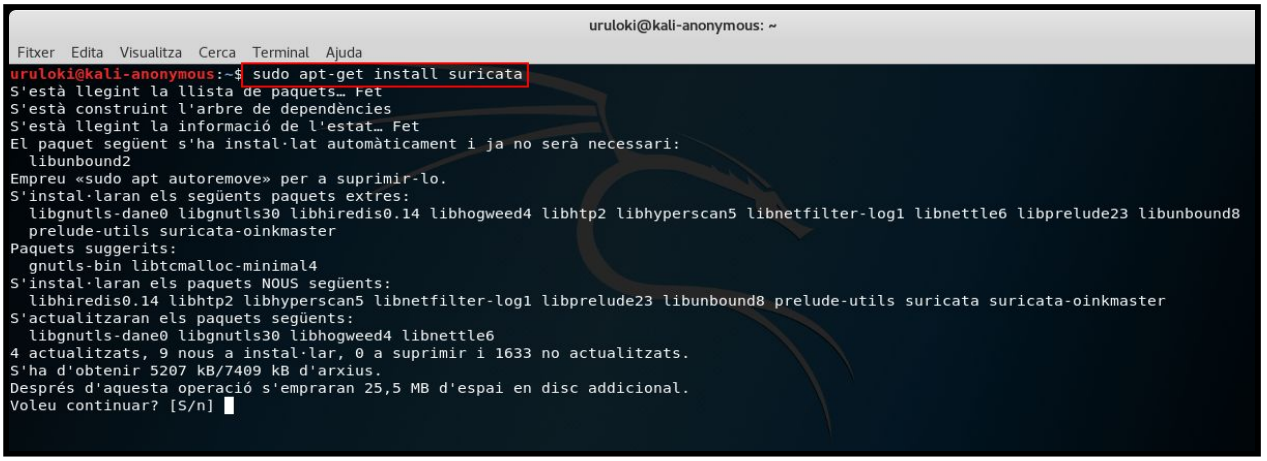
  El motor Suricata és capaç de:
  - detecció d'intrusió en temps real (IDS)
  - prevenció d'intrusió en línia (IPS)
  - monitoratge de seguretat de xarxa (NSM)
  - processament de pcap fos de línia. per a anàlisi forense).

- 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.

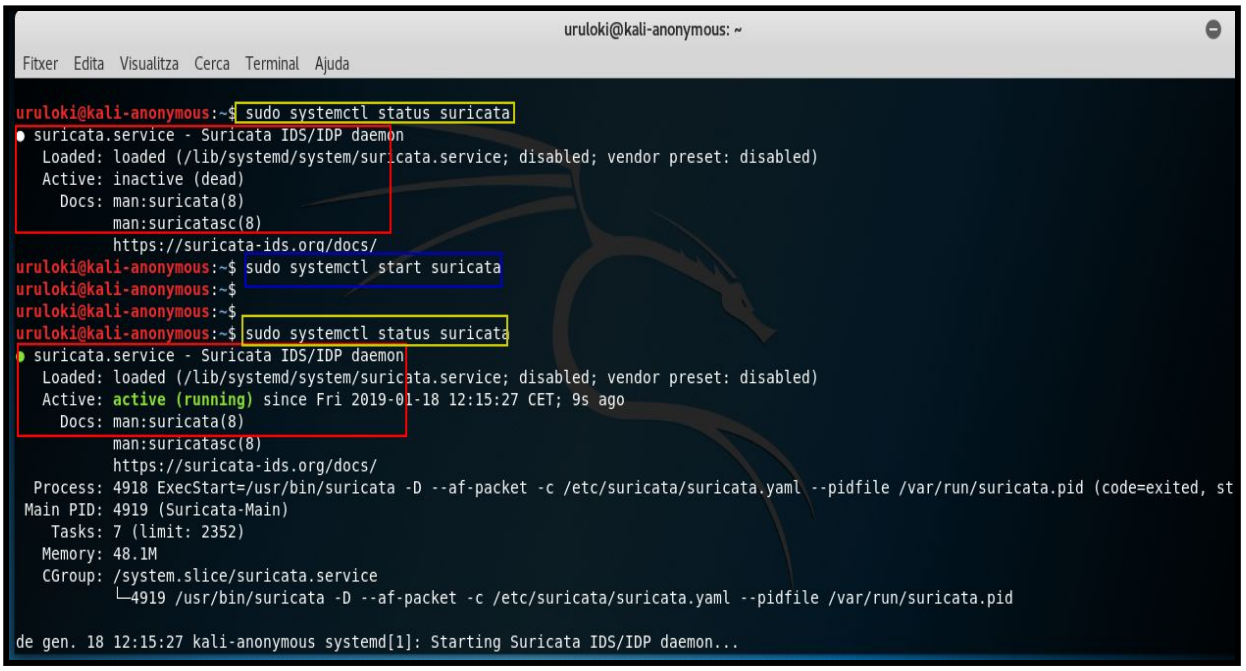
- El projecte i el codi de Suricata són propietat i estan recolzats per la **Open InformationSecurity Foundation** (OISF), una fundació sense finalitats de lucre compromesa a garantir el desenvolupament i l'èxit sostingut de Suricata com un projecte de codi obert.
  - ➔ En aquest cas instal.larem el software en la màquina virtual Kali Linux



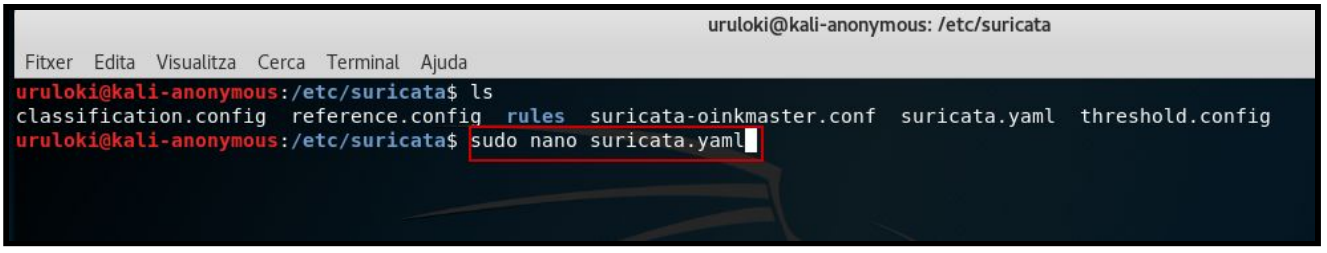
Nom i Cognoms **Data**

Arnau Subirós Puigarnau

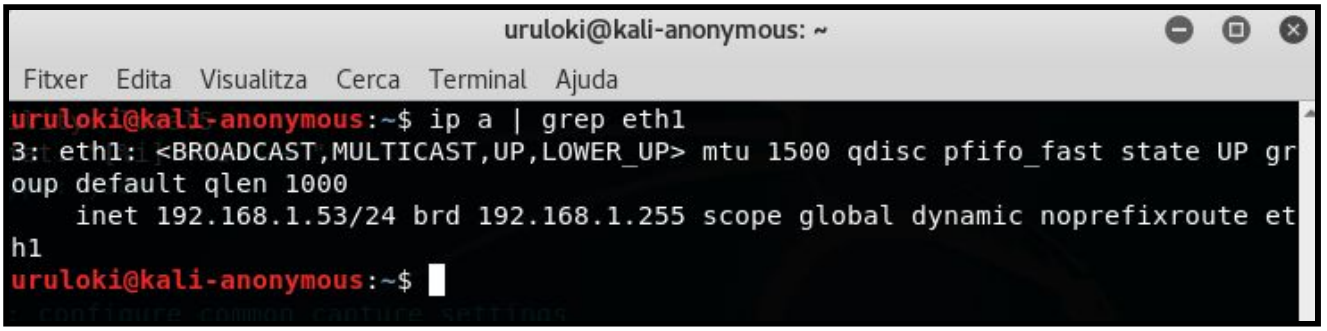
Un cop instal.lat reviso l'estat del servei, al comprovar que està inactiu l'activo i torno a confirmar l'estat



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

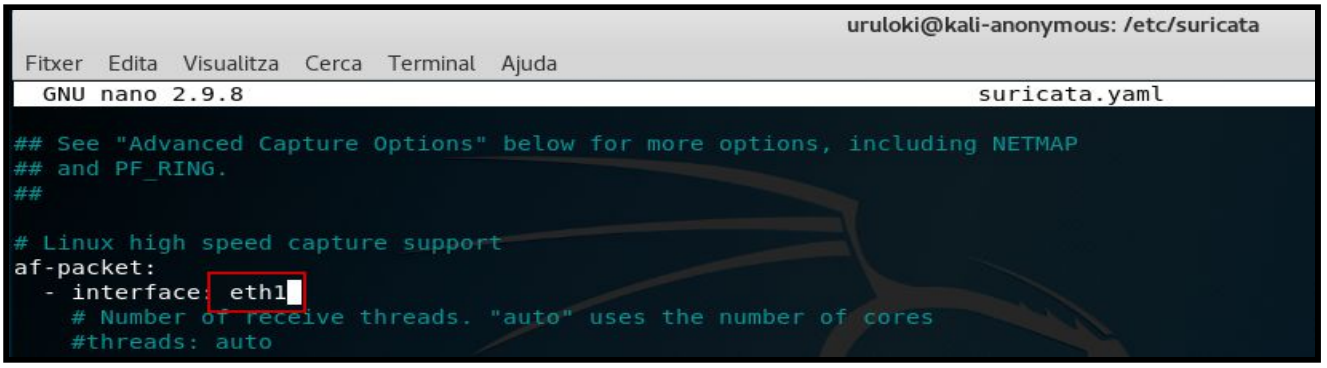


Abans hem de revisar el nom de la nostra interfície i modificar-la a l'arxiu de configuració

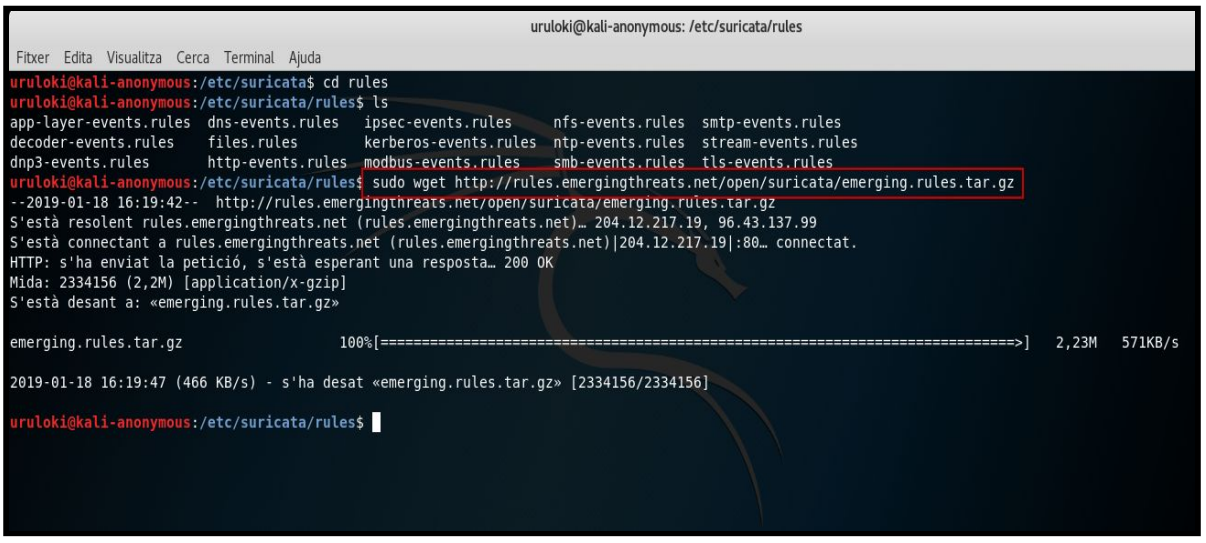


Nom i Cognoms **Data**

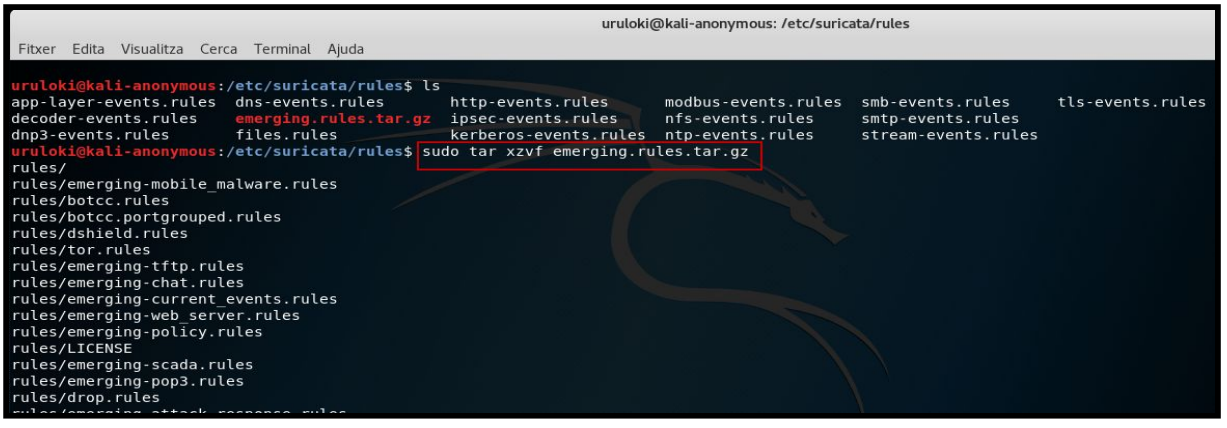
Arnau Subirós Puigarnau



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



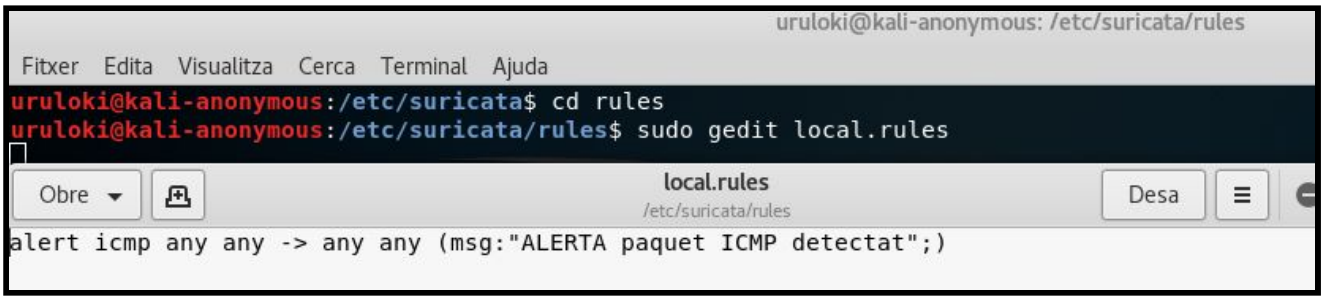
Descomprimint les regles en format tar



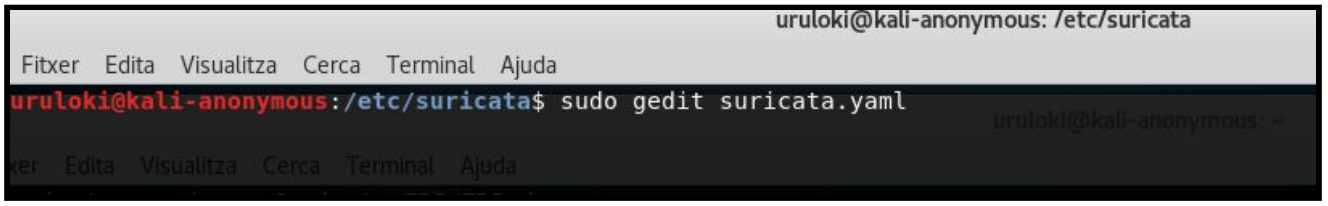
Nom i Cognoms **Data**

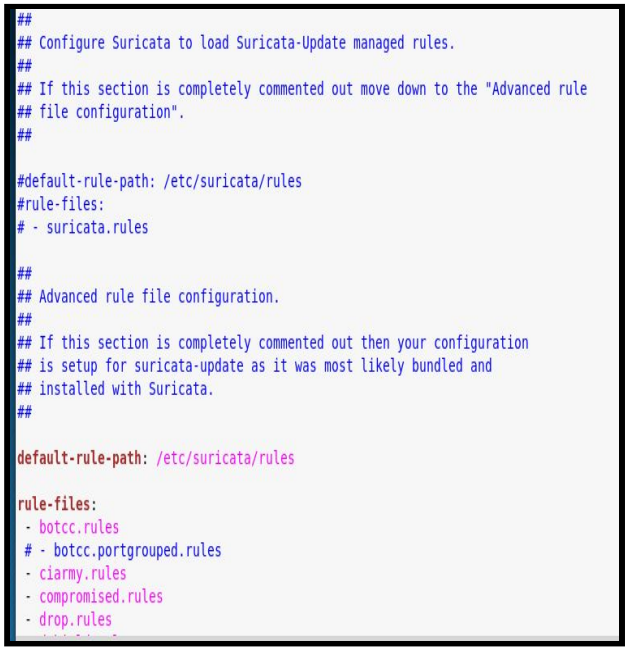
Arnau Subirós Puigarnau

Crearem un alerta per fer proves

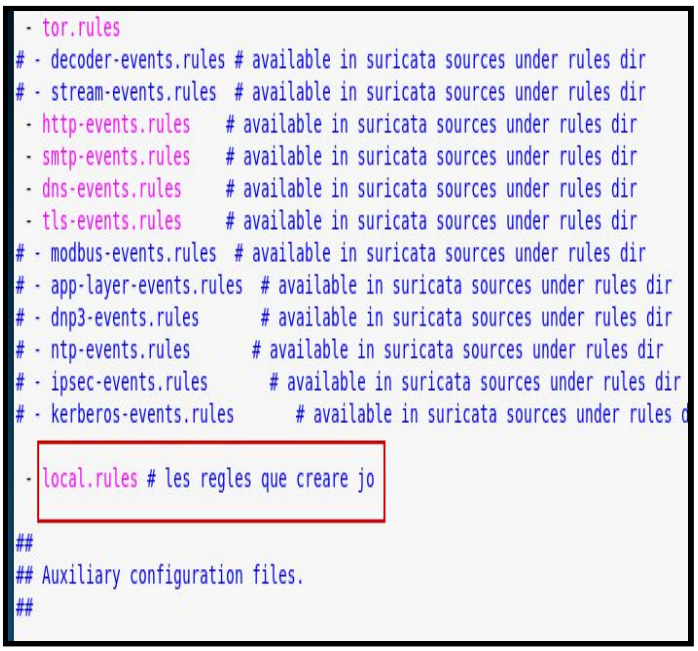


Ja tenim la regla instal.lada ,ara la afegirem a l'arxiu de configuració





```
##
## 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
```

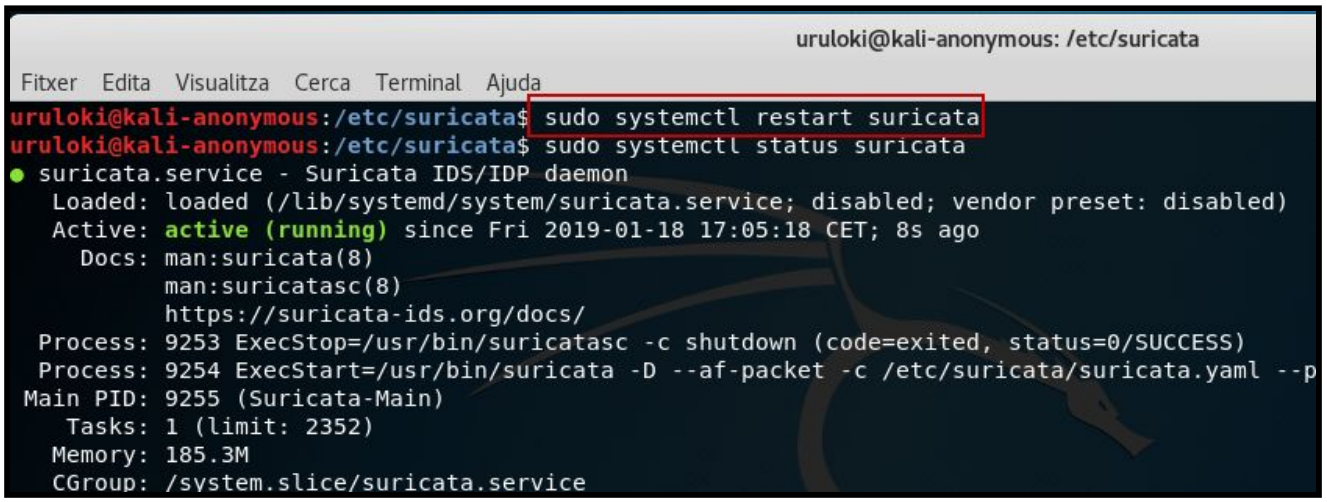


```
 - tor.rules
# - decoder-events.rules # available in suricata sources under rules dir
# - stream-events.rules  # available in suricata sources under rules dir
 - http-events.rules    # available in suricata sources under rules dir
 - smtp-events.rules    # available in suricata sources under rules 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 d

 - 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.



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

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

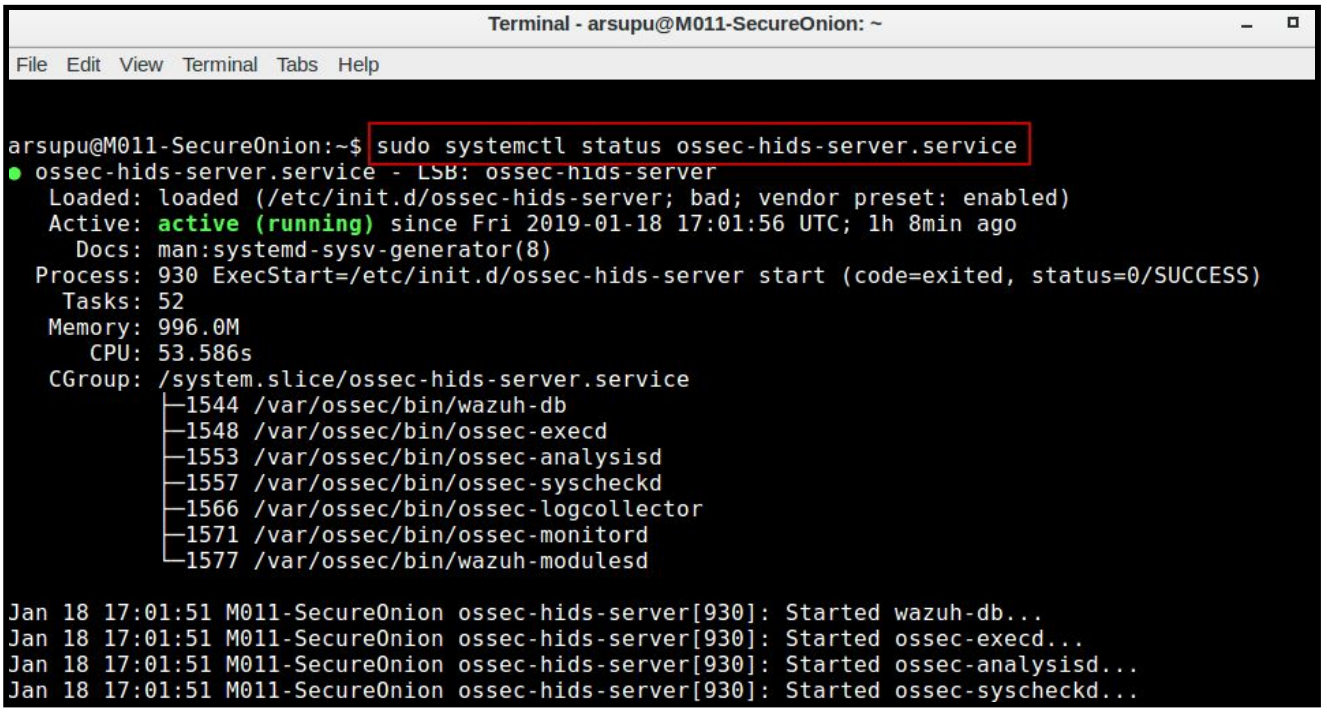
Nom i Cognoms **Data**

Arnau Subirós Puigarnau

2. OSSEC

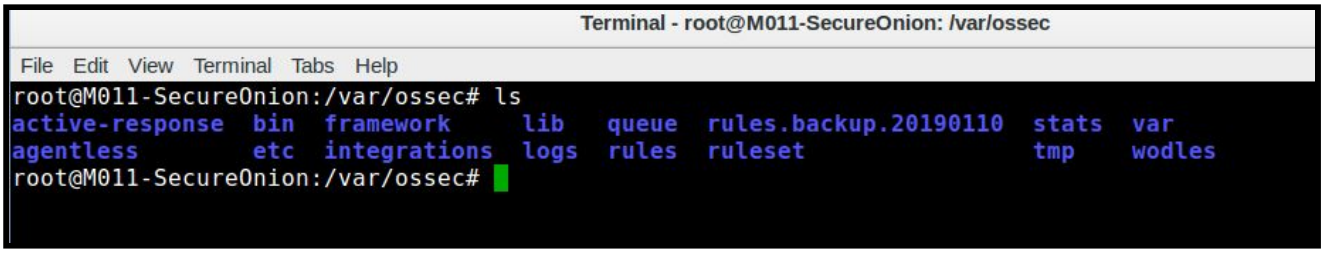
És un software de codi lliure de sistema de detecció d'intrusions basat en host (HIDS)

- 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(actúa com a servidor)



Nom i Cognoms **Data**

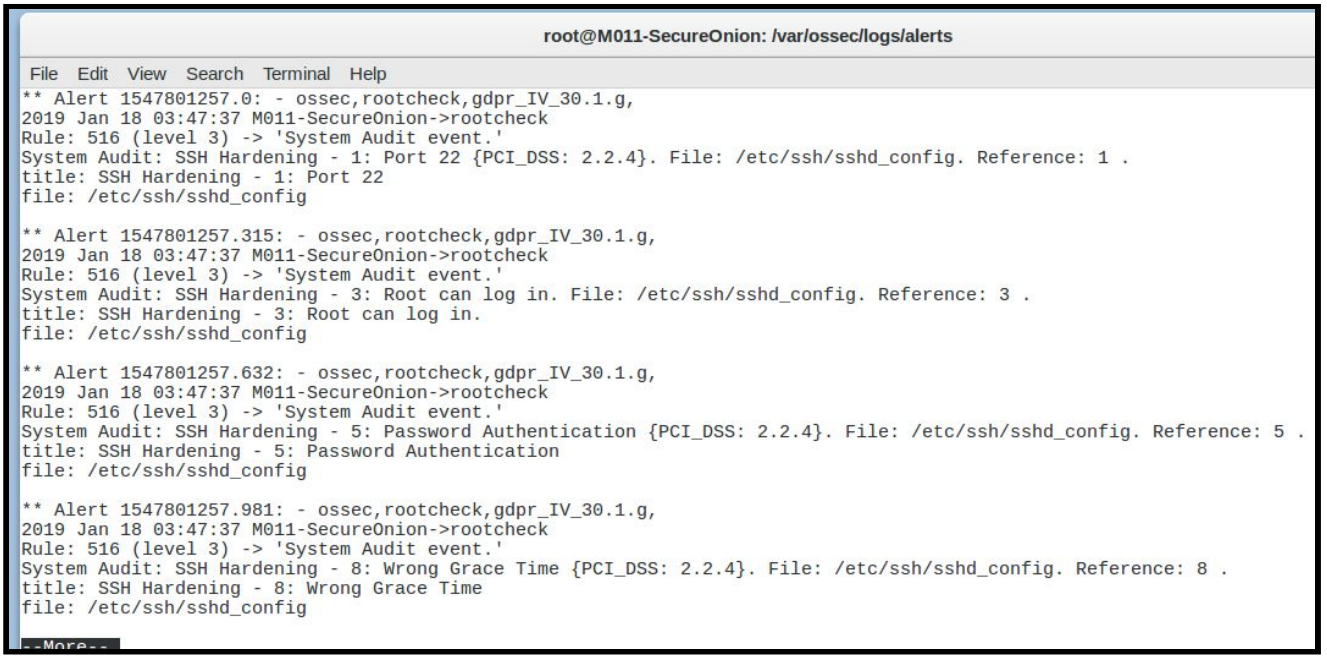
Arnau Subirós Puigarnau



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(inclosos Linux, * BSD, Solaris, MacOS i Win32).

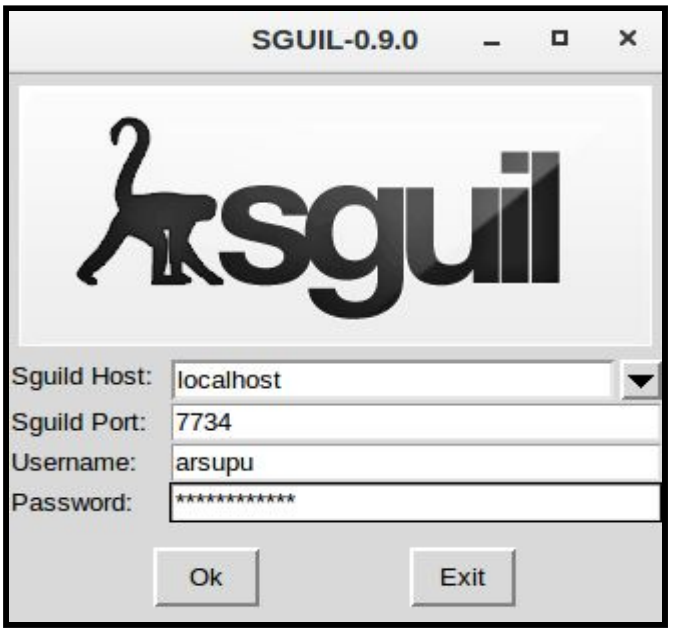
- **Agent OSSEC per a Sguil** , que rep les alertes de **/var/*ossec/*logs/*alerts/*alerts.log** i les envia a **Sguil.**

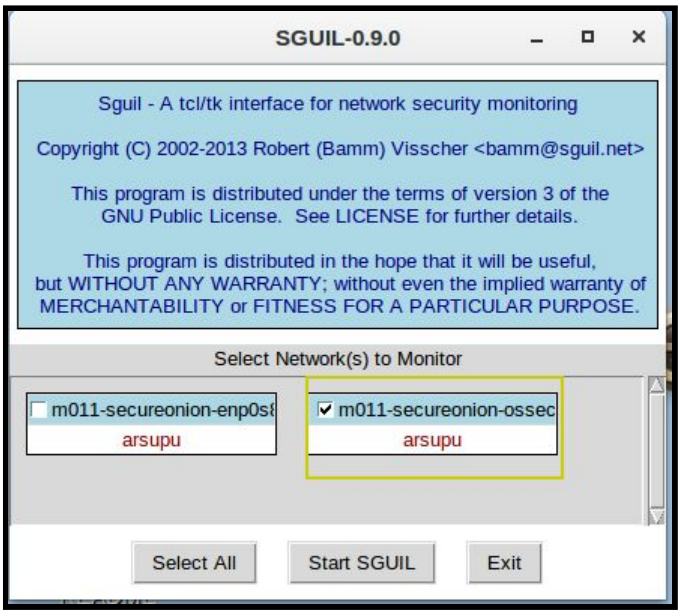


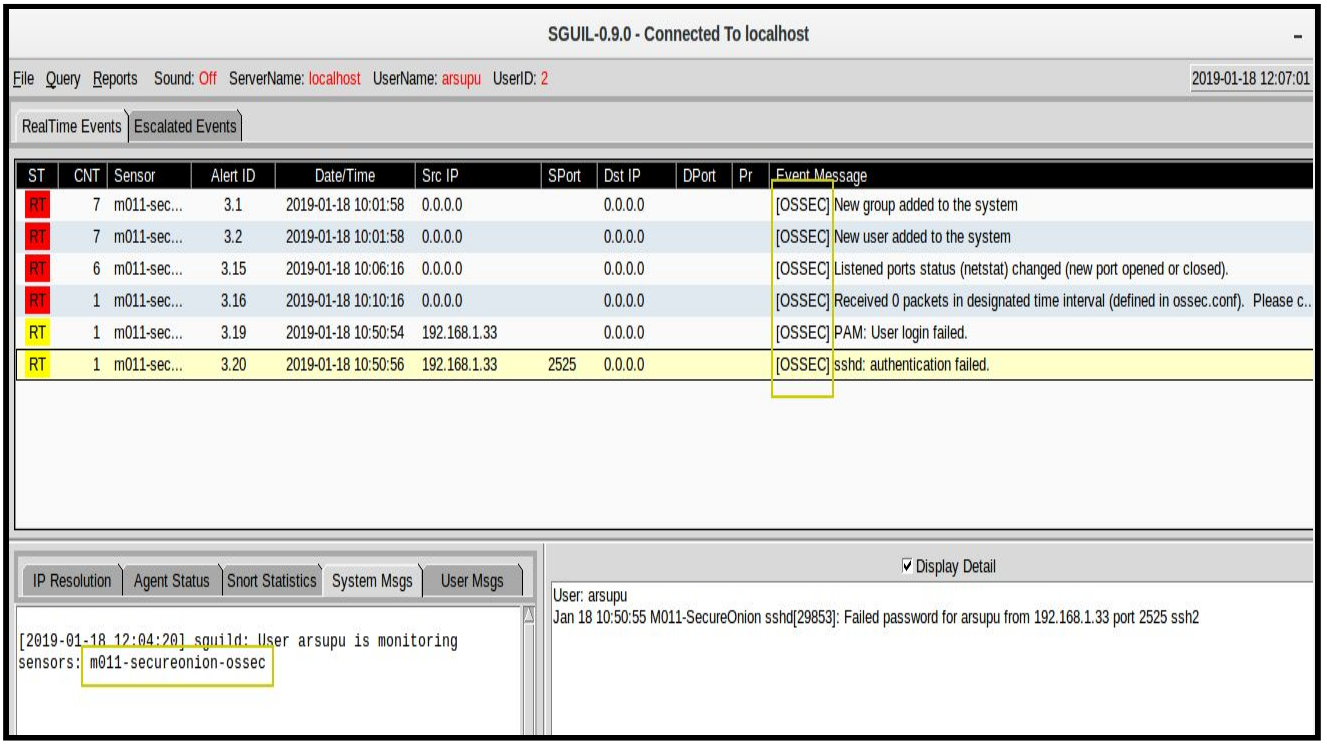
Nom i Cognoms **Data**

Arnau Subirós Puigarnau

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







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 utilitza 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:

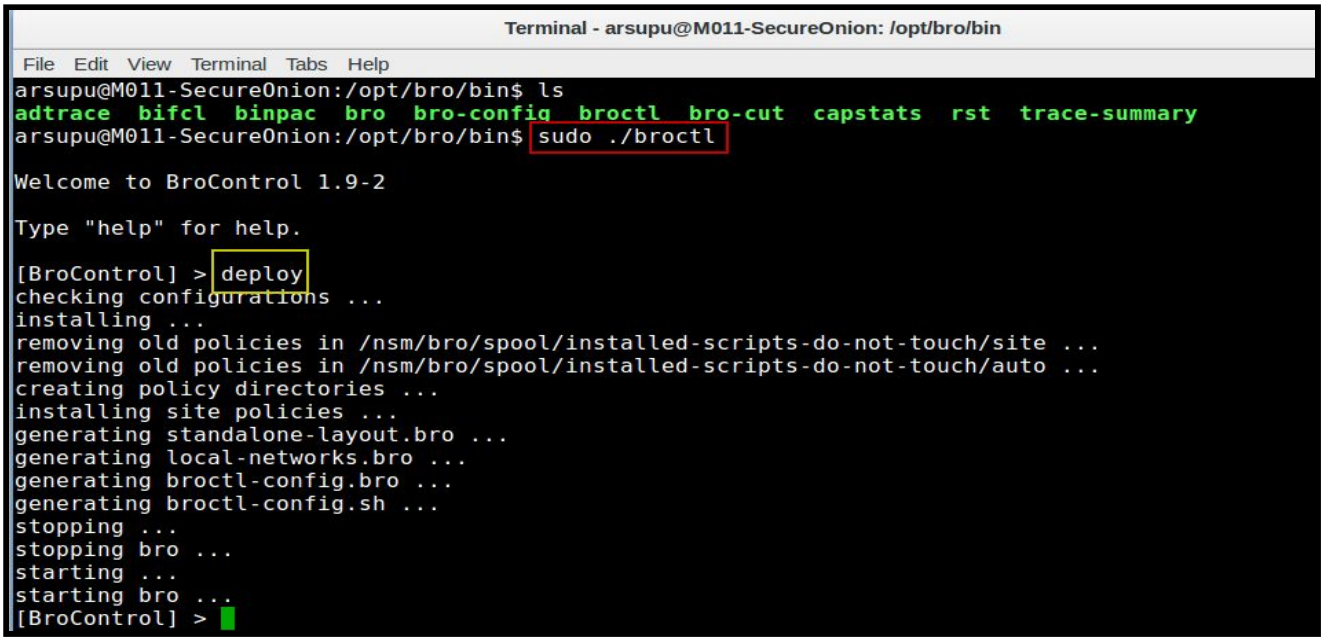
- stand alone: per a administrar BRO de forma habitual (un node).
- clúster mode: múltiples nodes actuant en conjunt per a aconseguir balanceig de la càrrega

2.1. Execució de Brotcl

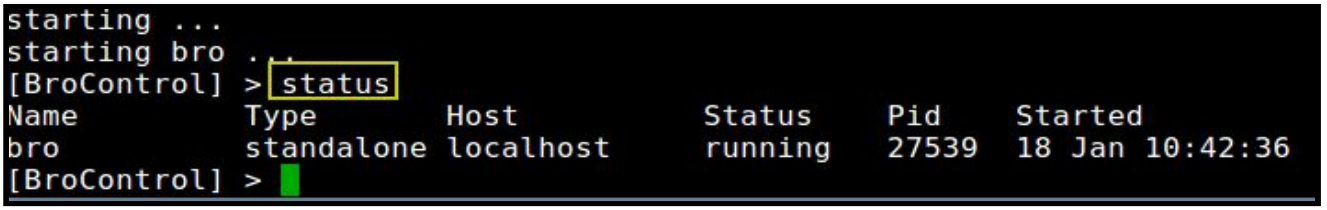
La primera vegada que s'usa **broctl** és recomanable usar el comando **deploy** (chequea la configuració de BRO: *broctl.cfg, node.cfg i networks.cfg*). La resta de vegades es pot usar el comando start, però si els fitxers de configuració nomenats abans es modifiquen, s'haurà d'usar deploy.

Nom i Cognoms **Data**

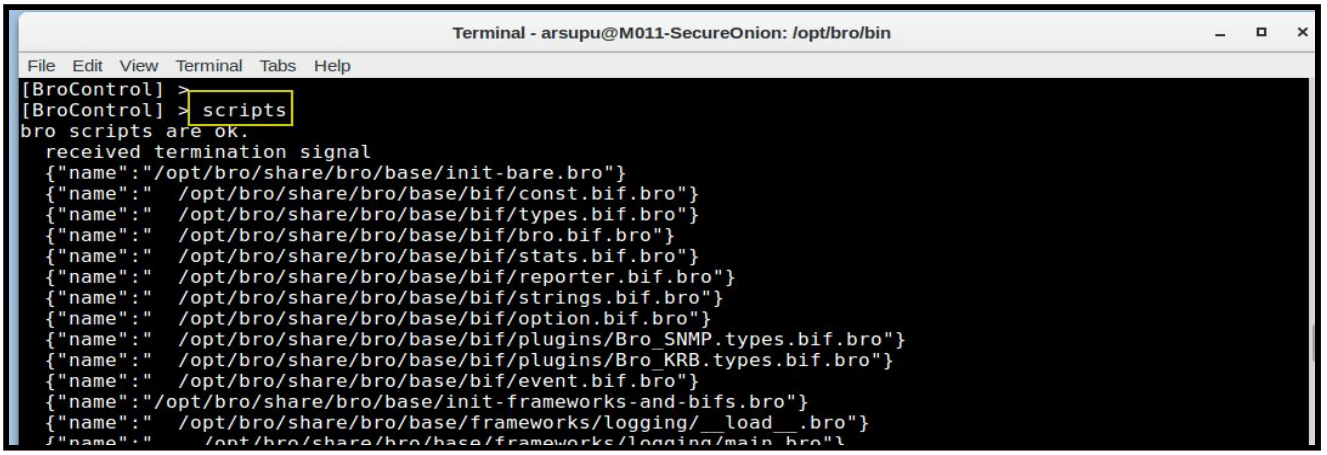
Arnau Subirós Puigarnau



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



Per veure els **scripts.**



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**

```
Terminal - arsupu@M011-SecureOnion:
File  Edit  View  Terminal  Tabs  Help
[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
configpodechksum = b47443f8b2cd8a20ad59175ed418fabaa981a975
controltopic = bro/control
crashexpireinterval = 0
croncmd =
```

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

```
Terminal - arsupu@M011-SecureOnion: /nsm/bro/logs/2019-01-18
File  Edit  View  Terminal  Tabs  Help
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            software.10:04:41-10:42:34.log.gz
capture_loss.10:42:35-10:42:36.log.gz  ftp.10:03:35-10:42:34.log.gz           ssl.10:01:51-10:42:34.log.gz
capture_loss.10:57:37-11:00:00.log.gz  http.10:04:42-10:42:34.log.gz          stats.10:01:30-10:42:34.log.gz
conn.10:01:56-10:42:34.log.gz          known_hosts.10:01:51-10:42:34.log.gz   stats.10:42:37-11:00:00.log.gz
conn.10:42:35-10:42:36.log.gz          loaded_scripts.10:01:30-10:42:34.log.gz stderr.10:01:27-10:42:36.log.gz
conn.10:44:47-11:00:00.log.gz          loaded_scripts.10:42:37-11:00:00.log.gz stdout.10:01:27-10:42:36.log.gz
conn-summary.10:01:56-10:42:34.log.gz  notice.10:03:24-10:42:34.log.gz        weird.10:01:36-10:42:34.log.gz
conn-summary.10:42:35-10:42:36.log.gz  packet_filter.10:01:30-10:42:34.log.gz weird.10:42:46-11:00:00.log.gz
conn-summary.10:44:47-11:00:00.log.gz  packet_filter.10:42:37-11:00:00.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 serveis tenir moltes dades si no les sabem utilitzar