Snorter

Guia d'Instal·lació

Instal·la `Snort` + `Barnyard2` + `PulledPork` automàticament

@joan_bono

Què necessites?

- Un ordinador amb:
  - Debian
  - Kali Linux
  - Raspbian Jessie
- Oinkcode:
  - És GRATUÏT! 😉
  - Molt recomanable
  - Obtenir el teu aquí.
- Interfície de xarxa identificada:
  - `ip link show`
- Dependències prèvies:
  - `sudo apt-get install git`
- Paciència.

Primeres passes

- Clonar el repositori:

```
git clone https://github.com/joanbono/Snorter.git`
cd Snorter/src
bash Snorter.sh -h
```

- Recomanat: Executa el programa fent servir un oinkcode

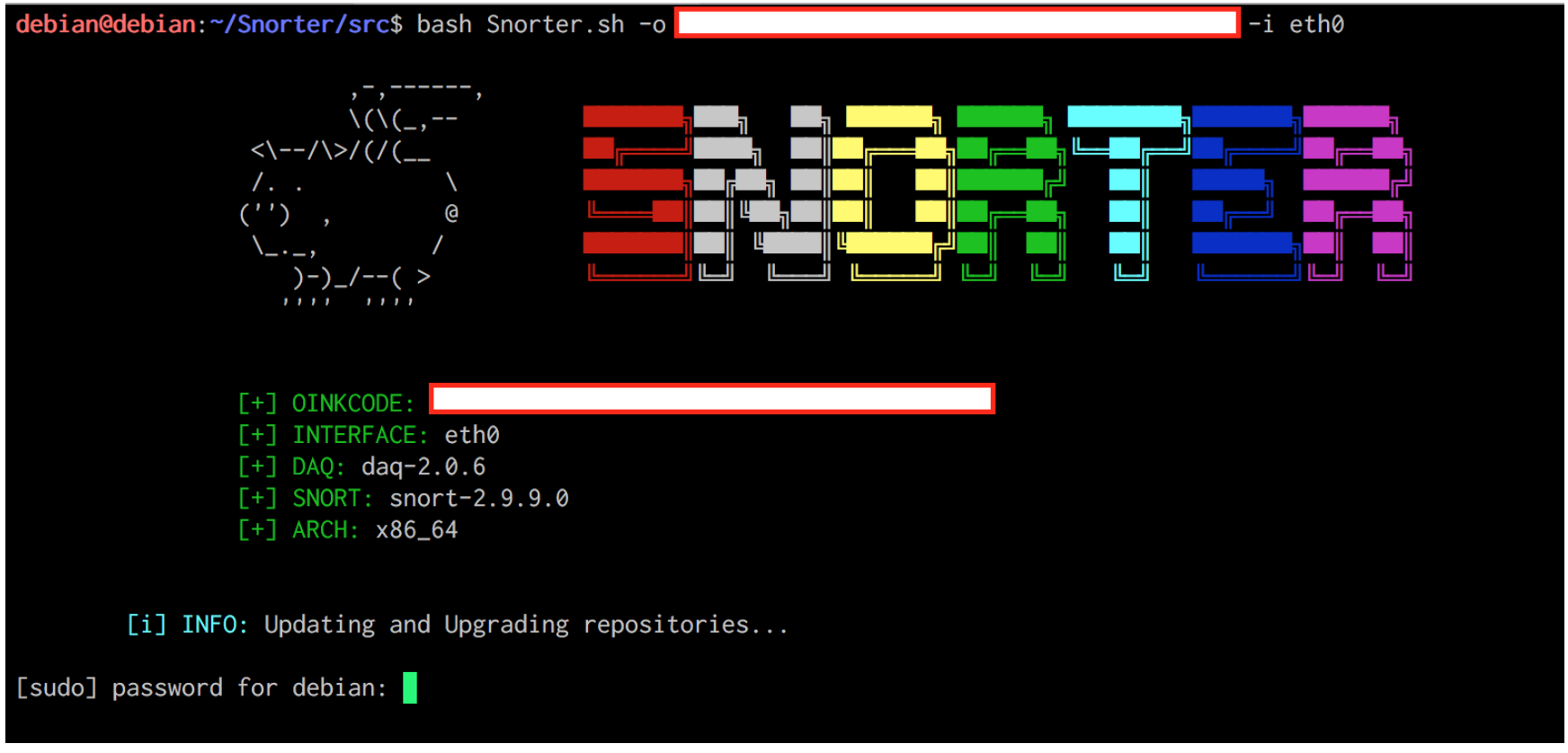
```
bash Snorter.sh -o <oinkcode> -i <interface>
Ex: bash Snorter.sh -o XXXXXXXXXXXXX -i eth0
```

- No Recomanat: Executa el programa sense cap oinkcode

```
bash Snorter.sh -i interface
bash Snorter.sh -i eth0
```

Instal·lació de `Snort`

- Contrassenya de superusuari, i esperar...



- `Snort` i `daq` s'han instal·lat.

```
      [+] INFO: snort-2.9.9.0 installed successfully.

      [i] INFO: Adding user and group SNORT.

      [i] INFO: /var/log/snort and /etc/snort created and configurated.

 ,,_     -*> Snort! <*-
o"  )~   Version 2.9.9.0 GRE (Build 56)
 ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
         Copyright (C) 2014-2016 Cisco and/or its affiliates. All rights reserved.
         Copyright (C) 1998-2013 Sourcefire, Inc., et al.
         Using libpcap version 1.6.2
         Using PCRE version: 8.35 2014-04-04
         Using ZLIB version: 1.2.8

      [+] INFO: SNORT is successfully installed and configurated!
```

- Ara toca afegir la `HOME_NET` i la `EXTERNAL_NET`.

```
[!] INFO: Now it's time to edit the SNORT configuration file.


[i] INFO: Add your HOME_NET address [Ex: 192.168.1.0/24]
[!] WARNING: Press ENTER to continue.
```

- Prémer `Intro` per continuar. Obrirà `vim`:
  - Prémer `A` per anar al final de la línia.
  - Afegeix l'adreça i la màscara de la xarxa a protegir.
  - Prémer `Esc` i després `:wq!` per desar canvis.

```
39
40 ###################################################
41 # Step #1: Set the network variables.  For more information, see README.variables
42 ###################################################
43
44 # Setup the network addresses you are protecting
45 ipvar HOME_NET 172.16.77.0/24
46
```

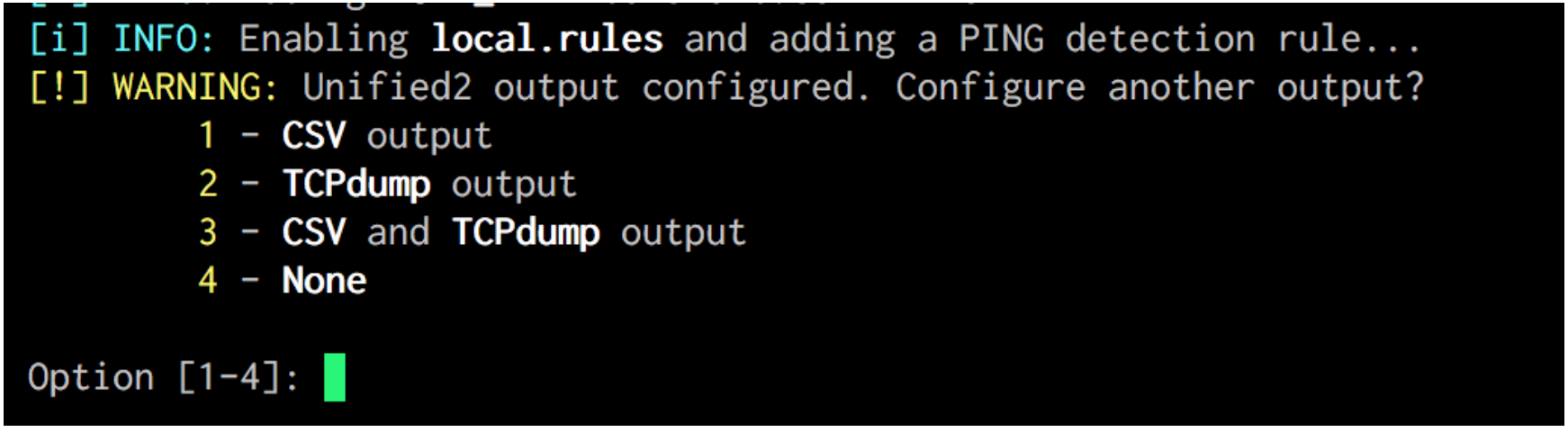
- Fes el mateix per a la `EXTERNAL_NET`:

```
[i] INFO: Add your EXTERNAL_NET address [Ex: !$HOME_NET]
[!] WARNING: Press ENTER to continue.
```

- Prémer `Intro` per continuar. Obrirà `vim`:
  - Prémer `A` per anar al final de la línia.
  - Afegir l'adreça *atacant*. Recomanat: `!$HOME_NET`.
  - Prémer `Esc` i després `:wq!` per desar canvis.

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

- Ara la sortida. Per defecte, s'habilita el format de sortida `unified2`, però pots habilitar més d'una sortida. Vaig a habilitar la sortida en CSV i format TCPdump.



- Ara `SNORT` arrancarà en mode `consola`. Mana un `PING` des d'altra màquina per comprovar el funcionament.

```
       [!] WARNING: Attempting to test ICMP rule in eth0. Send a PING to your SNORT machine. Press Ctrl+C once and wait few seconds to stop the process...

       [!] WARNING: Press ENTER to continue.
01/09-12:39:29.229291  [**] [1:10000001:1] Atac per PINGs [**] [Priority: 0] {ICMP} 172.16.77.1 -> 172.16.77.137
01/09-12:39:29.229320  [**] [1:10000001:1] Atac per PINGs [**] [Priority: 0] {ICMP} 172.16.77.137 -> 172.16.77.1
01/09-12:39:30.229230  [**] [1:10000001:1] Atac per PINGs [**] [Priority: 0] {ICMP} 172.16.77.1 -> 172.16.77.137
01/09-12:39:30.229294  [**] [1:10000001:1] Atac per PINGs [**] [Priority: 0] {ICMP} 172.16.77.137 -> 172.16.77.1
01/09-12:39:31.230473  [**] [1:10000001:1] Atac per PINGs [**] [Priority: 0] {ICMP} 172.16.77.1 -> 172.16.77.137
01/09-12:39:31.230526  [**] [1:10000001:1] Atac per PINGs [**] [Priority: 0] {ICMP} 172.16.77.137 -> 172.16.77.1
01/09-12:39:32.231436  [**] [1:10000001:1] Atac per PINGs [**] [Priority: 0] {ICMP} 172.16.77.1 -> 172.16.77.137
01/09-12:39:32.231553  [**] [1:10000001:1] Atac per PINGs [**] [Priority: 0] {ICMP} 172.16.77.137 -> 172.16.77.1
01/09-12:39:33.236303  [**] [1:10000001:1] Atac per PINGs [**] [Priority: 0] {ICMP} 172.16.77.1 -> 172.16.77.137
01/09-12:39:33.236387  [**] [1:10000001:1] Atac per PINGs [**] [Priority: 0] {ICMP} 172.16.77.137 -> 172.16.77.1
01/09-12:39:34.241661  [**] [1:10000001:1] Atac per PINGs [**] [Priority: 0] {ICMP} 172.16.77.1 -> 172.16.77.137
01/09-12:39:34.241796  [**] [1:10000001:1] Atac per PINGs [**] [Priority: 0] {ICMP} 172.16.77.137 -> 172.16.77.1
^C*** Caught Int-Signal
snort: no process found
```

- Mostrarà una alerta de `PING`. Prémer `Ctrl+C` una vegada, i continua la instal·lació.

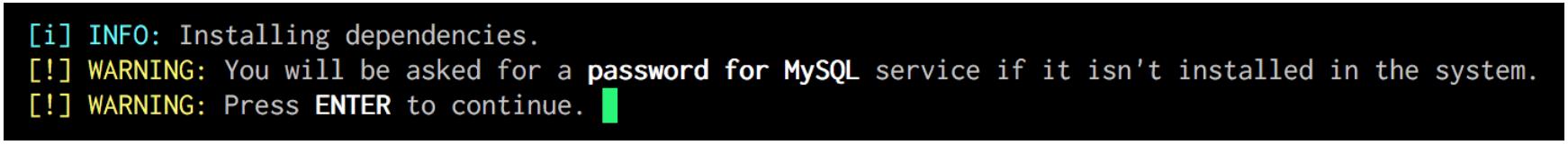
Instalació de `Barnyard2`

- Ara toca instal·lar `BARNYARD2` si vols.
- Es demana inserir una contrassenya per la base de dades de `SNORT` que es va a crear. En l'exemple utilitzo `SNORTSQL`.

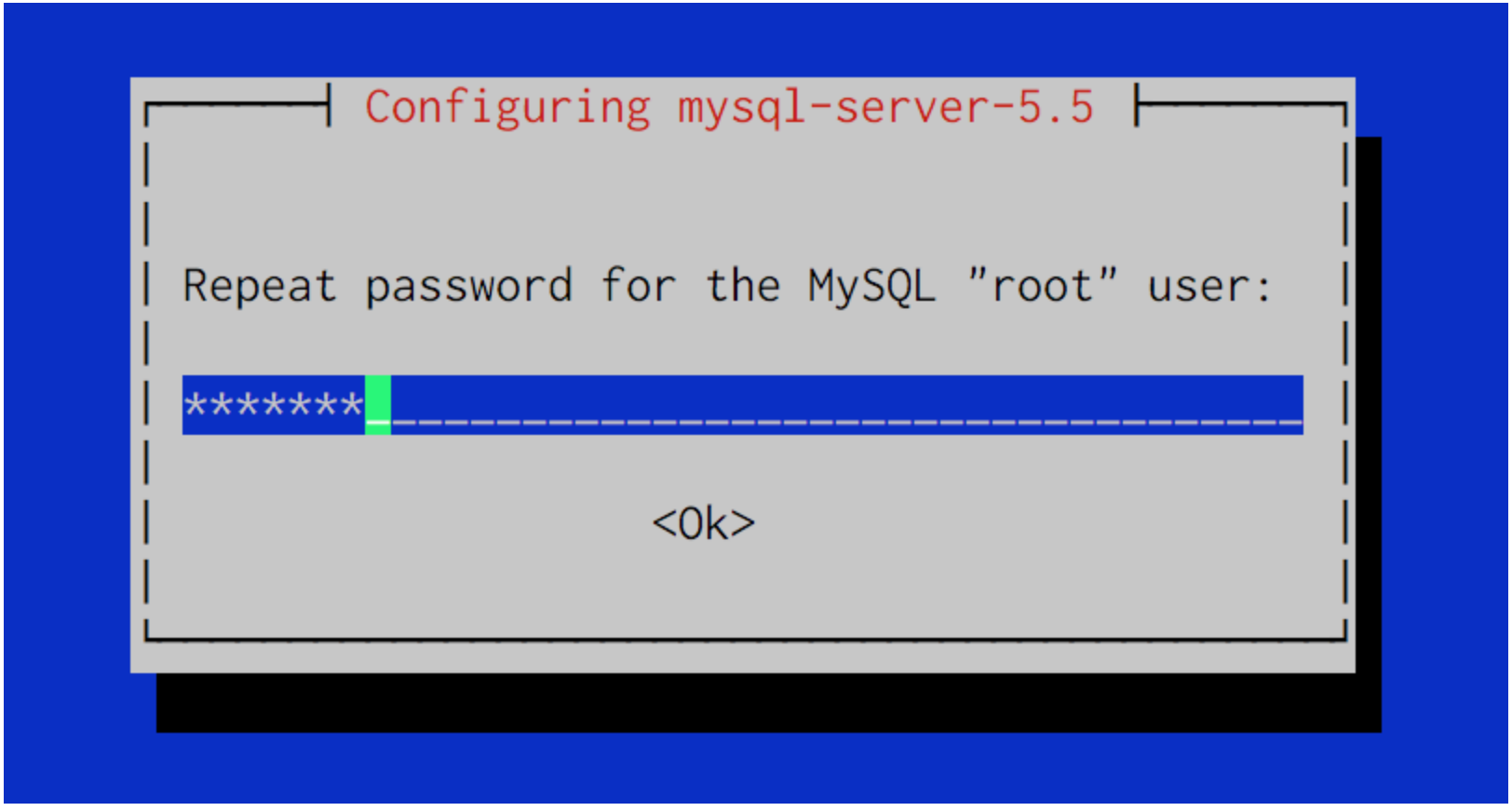
```
[!] IMPORTANT: Would you like to install BARNYARD2? [Y/n] Y

[!] WARNING: Insert new SNORT Database Password: SNORTSQL
```

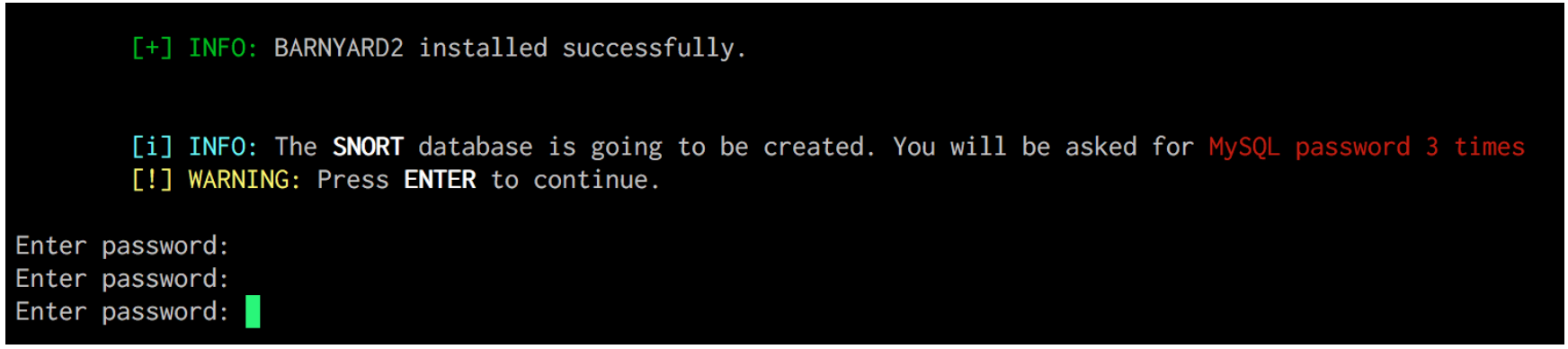
- Ara el programa instal·larà algunes dependències.
- Instal·larà `MySQL`, si no està instal·lat prèviament, hauràs d' introduïr una contrassenya de `root`. En l'ejemplo, poso `ROOTSQL`.



- I la contrassenya del servei `MySQL`.



- Ara el programa pregunta la contrassenya de `MySQL` 3 vegades
- Tenir en compte: contrassenya **`root`** de **`MySQL`** 3 vegades.



Instal·lació de `PulledPork`

- Ara toca instal·lar `PulledPork` si vols.

```
[!] IMPORTANT: Would you like to install PULLEDPORK? [Y/n] Y
```

```
        [i] INFO: Downloading PULLEDPORK.

Cloning into 'pulledpork'...
remote: Counting objects: 1207, done.
remote: Total 1207 (delta 0), reused 0 (delta 0), pack-reused 1207
Receiving objects: 100% (1207/1207), 249.49 KiB | 0 bytes/s, done.
Resolving deltas: 100% (814/814), done.
Checking connectivity... done.

        [i] INFO: Adding PULLEDPORK to crontab. [Everyday at 4:15 AM].

PulledPork v0.7.3 - Making signature updates great again!


        [+] INFO: PULLEDPORK is successfully installed and configured!
```

Crear un `servei`

- Crear un `servei` del sistema:

```
[!] IMPORTANT: Would you like to create a service snort? [Y/n] Y

[i] INFO: Now you can run sudo systemctl {start|stop|status} snort .
```

Descarregar i instal·lar noves regles

- Pots descarregar i instal·lar noves regles quan tot estiga instal·lat i configurat.

Habilitar regles **`Emerging Threats`** i **`Community`**

- Habilitar automàticamente al `snort.conf` les regles d'`Emerging Threats` i `Community`

```
[!] IMPORTANT: Would you like to enable Emerging Threats and Community rules for detection? [Y/n] Y

[+] SUCCESS: Emerging Threats and Community rules enabled
```

WebSnort

- Instal·lar WebSnort per analitzar `PCAPs`

```
[!] IMPORTANT: Would you like to install WEBSNORT for PCAP Analysis? [Y/n] Y

[i] INFO: Installing dependencies.


[i] INFO: running WEBSNORT on http://localhost:80.


[!] IMPORTANT: Would you like to start WEBSNORT with the system? [Y/n] Y

[+] INFO: WEBSNORT is successfully installed and configured!
```

Reiniciar

- Reiniciar el sistema.

```
[!] IMPORTANT: Would you like to REBOOT now? [Y/n] Y

[i] INFO: Rebooting...
```