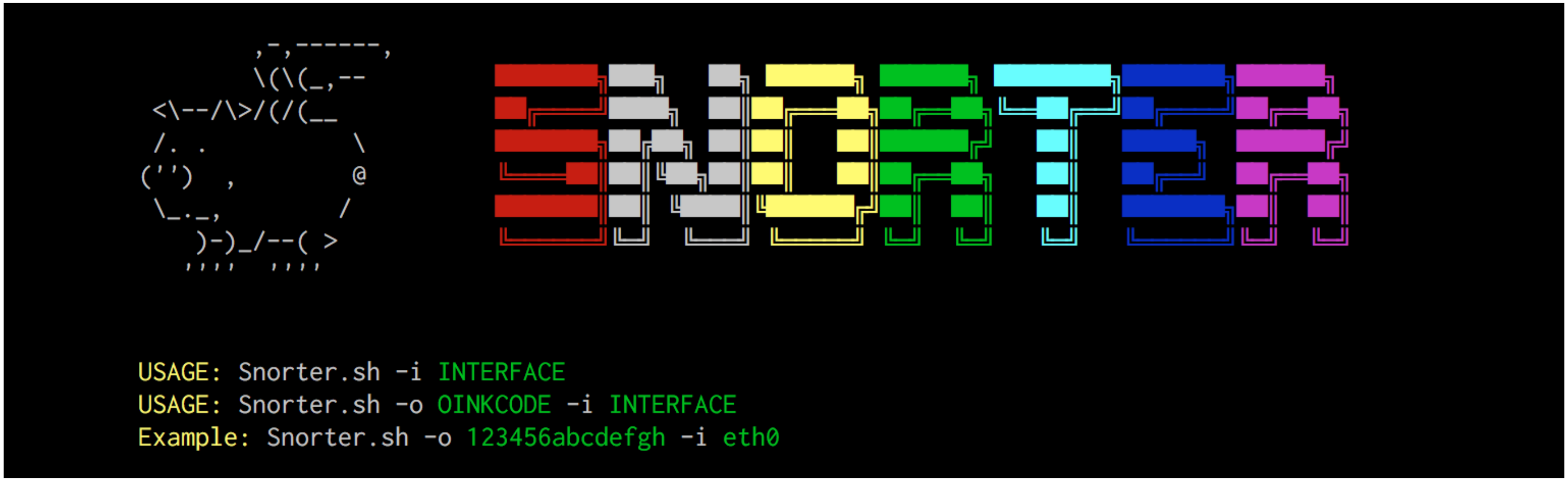


```
        ,-,------,
        \(\(_,--
 <\--/\>/(/(__
 /. .          \
('')  ,        @
 \_._,        /
    )-)_/--( >
   ,,,,  ,,,,
```

```
USAGE: Snorter.sh -i INTERFACE
USAGE: Snorter.sh -o OINKCODE -i INTERFACE
Example: Snorter.sh -o 123456abcdefgh -i eth0
```

Snorter

Guía de Instalación

Instala `Snort` + `Barnyard2` + `PulledPork` automáticamente

@joan_bono

¿Qué necesitas?

- Un ordenador con:
    - Debian
    - Kali Linux
    - Raspbian Jessie
- Oinkcode:
    - Es GRATIS! 😉
    - Muy recomendable
    - Obtén el tuyo aquí.
- Interfaz de red identificada:

    -
      ```
      ip link show
      ```
- Dependencias previas:

    -
      ```
      sudo apt-get install git
      ```
- Paciencia.

Primeros pasos

- Clonar el repositorio:

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

- Recomendado: Ejecuta el programa usando un oinkcode

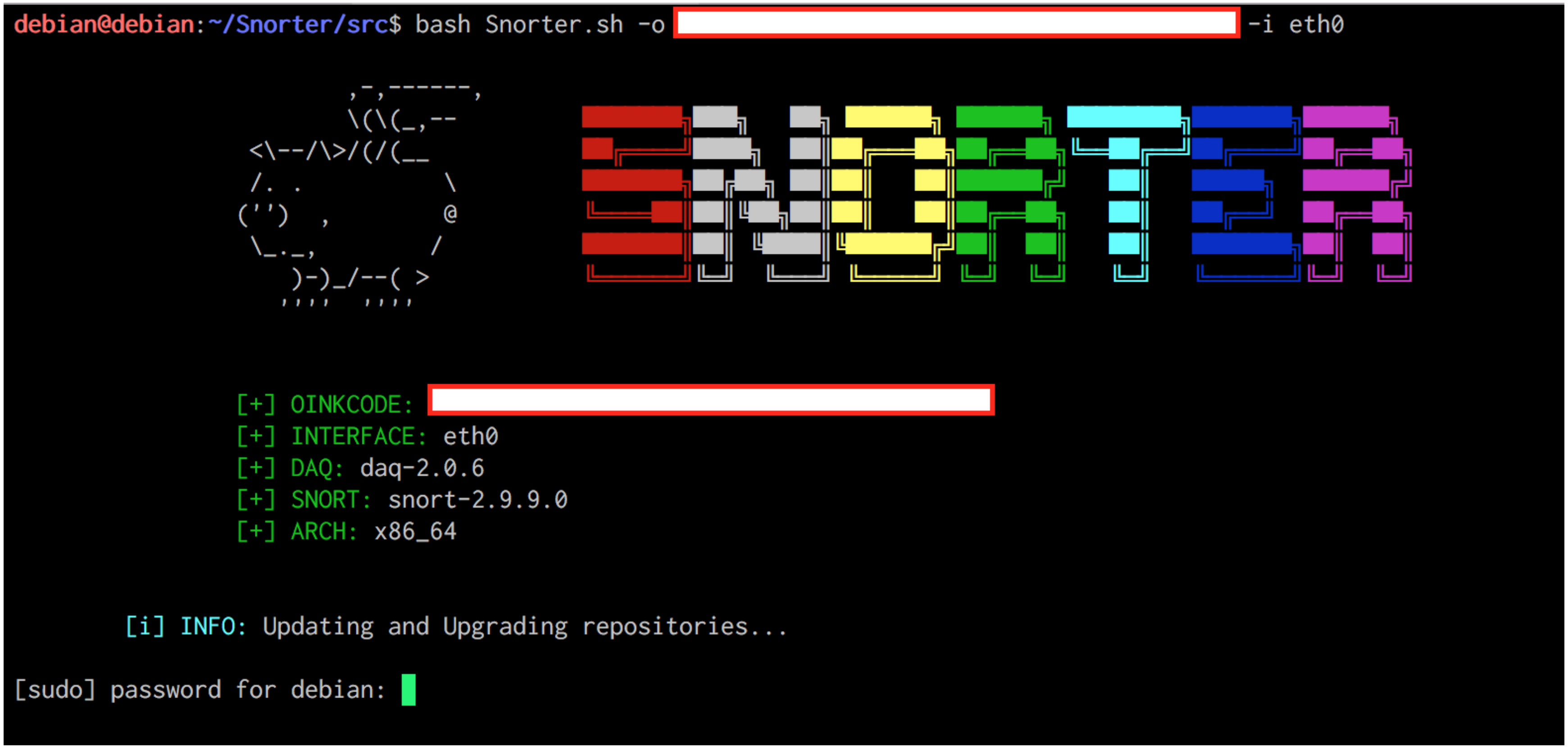
```
bash Snorter.sh -o <oinkcode> -i <interface>
Ex: bash Snorter.sh -o XXXXXXXXXXXXX -i eth0
```

- No Recomendado: Ejecuta el programa sin un oinkcode

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

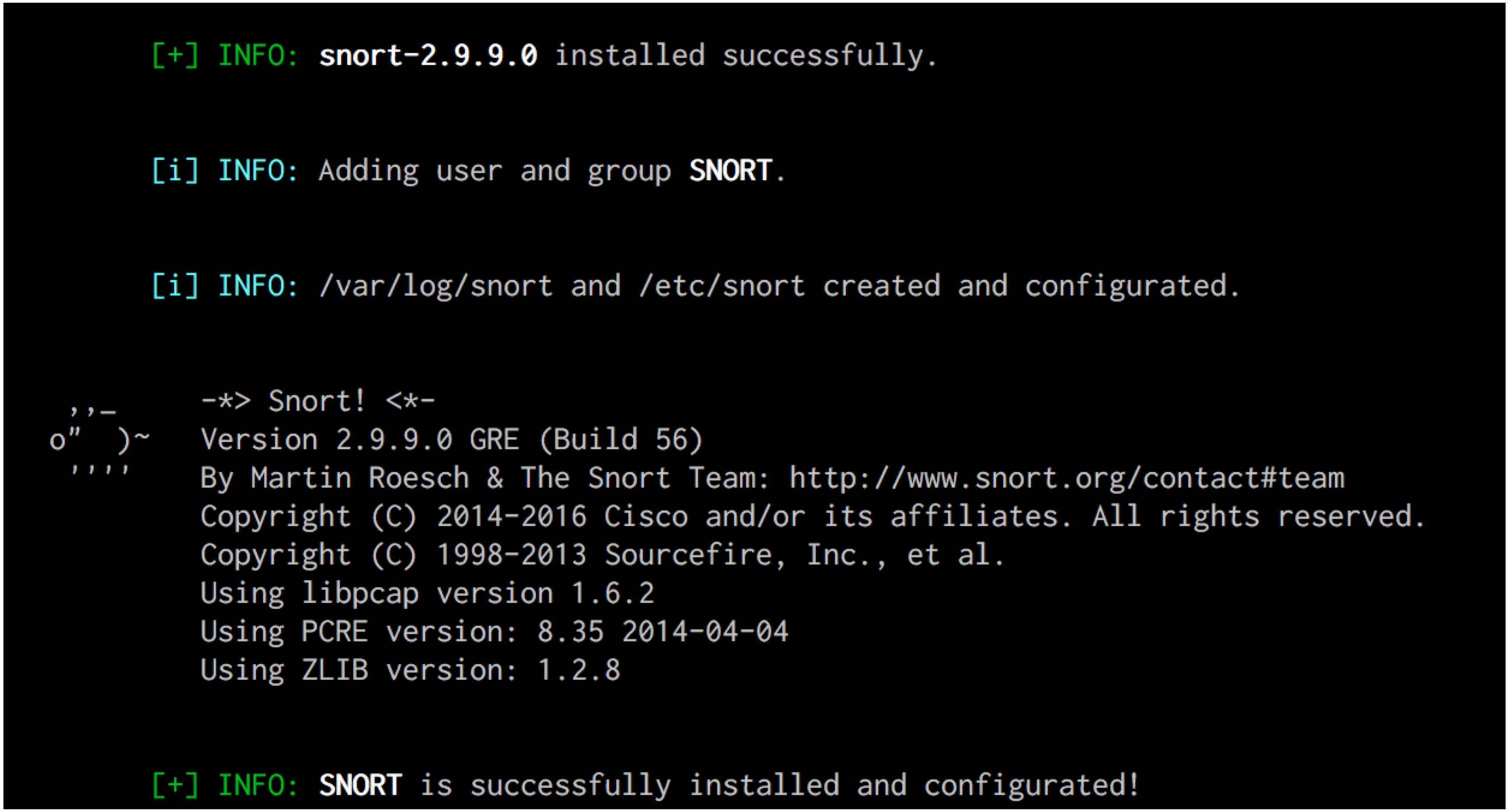
Instalación de `Snort`

- Contraseña de superusuario, y esperar...



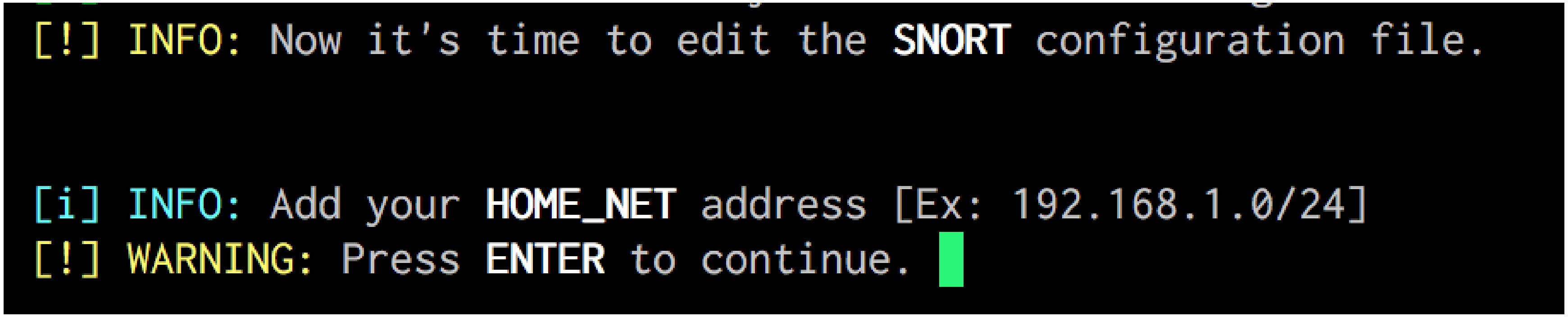
```
debian@debian:~/Snorter/src$ bash Snorter.sh -o [redacted] -i eth0

                        ,-,------,
                        \(\(_,--
                 <\--/\>/(/(__
                 /. .           \
                ('')  ,         @
                 \_._,         /
                    )-)_/--( >
                   ''''  ''''


                [+] OINKCODE: [redacted]
                [+] INTERFACE: eth0
                [+] DAQ: daq-2.0.6
                [+] SNORT: snort-2.9.9.0
                [+] ARCH: x86_64


        [i] INFO: Updating and Upgrading repositories...

[sudo] password for debian: 
```

- `Snort` y `daq` se han instalado.



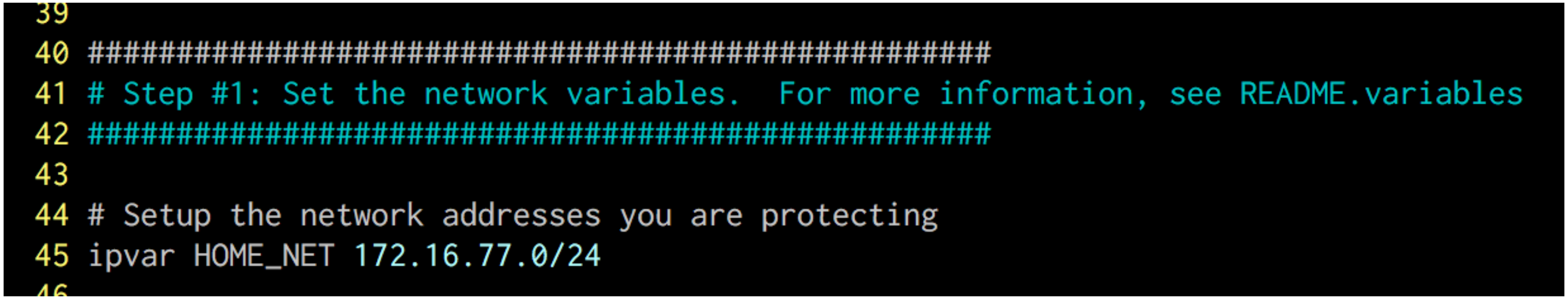
```
      [+] INFO: snort-2.9.9.0 installed successfully.


      [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!
```

- Ahora toca añadir la `HOME_NET` y la `EXTERNAL_NET`.



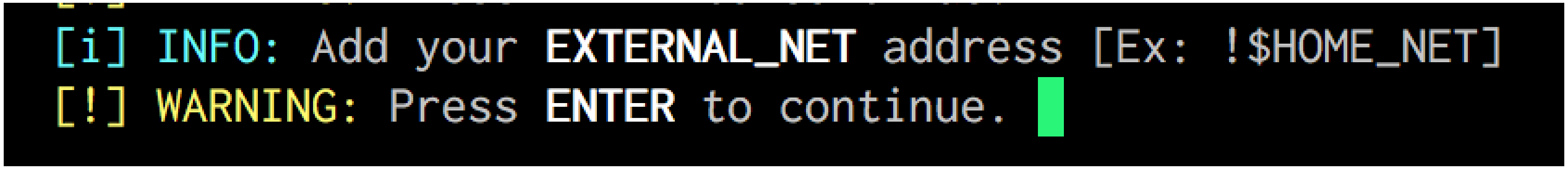
```
[!] INFO: Now it's time to edit the SNORT configuration file.


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

- Pulsa `Intro` para continuar. Abrirá `vim`:
  - Pulsa `A` para ir al final de la línea.
  - Añade la dirección y la máscara de la red a proteger.
  - Pulsa `Esc` y después `:wq!` para guardar cambios.



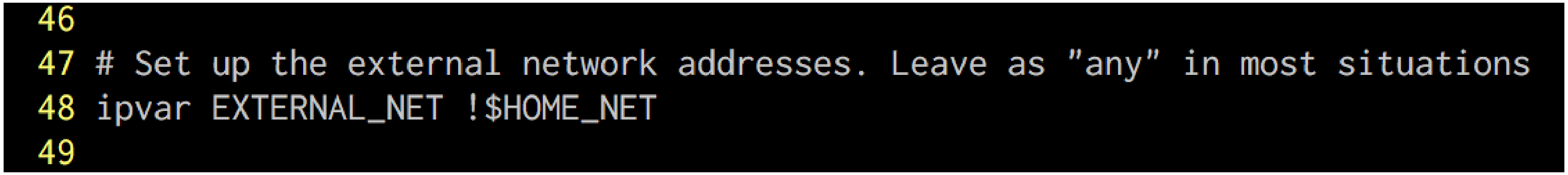
```

###################################################
# Step #1: Set the network variables.  For more information, see README.variables
###################################################

# Setup the network addresses you are protecting
ipvar HOME_NET 172.16.77.0/24
```

- Haz lo mismo para la `EXTERNAL_NET`:



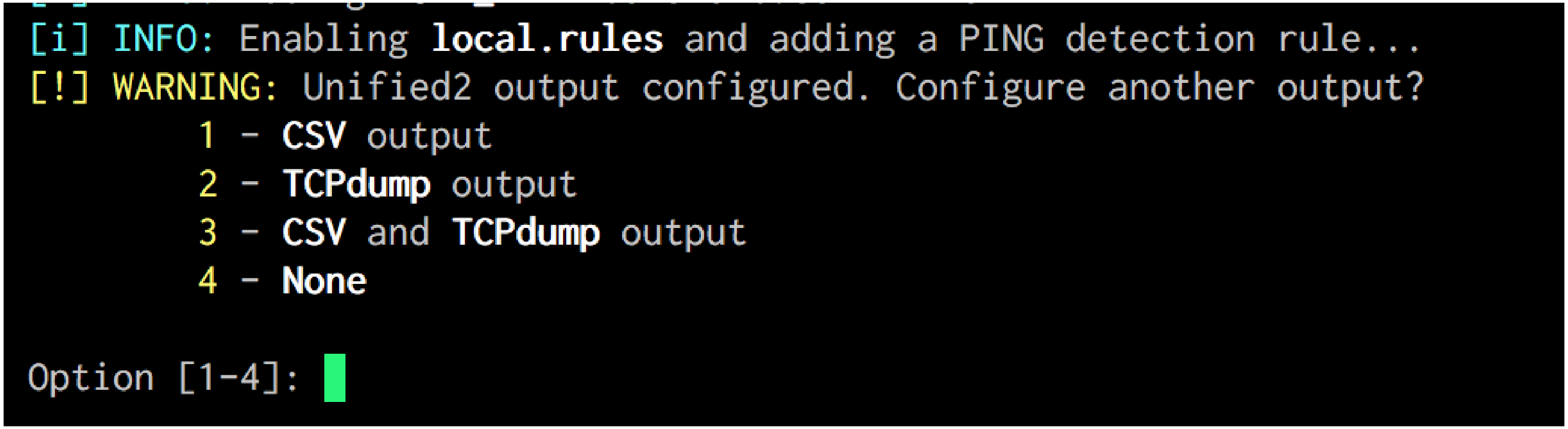
```
[i] INFO: Add your EXTERNAL_NET address [Ex: !$HOME_NET]
[!] WARNING: Press ENTER to continue.
```

- Pulsa `Intro` para continuar. Abrirá `vim`:
    - Pulsa `A` para ir al final de la línea.
    - Añade la dirección *atacante*. Recomendado: `!$HOME_NET`.
    - Pulsa `Esc` y después `:wq!` para guardar cambios.



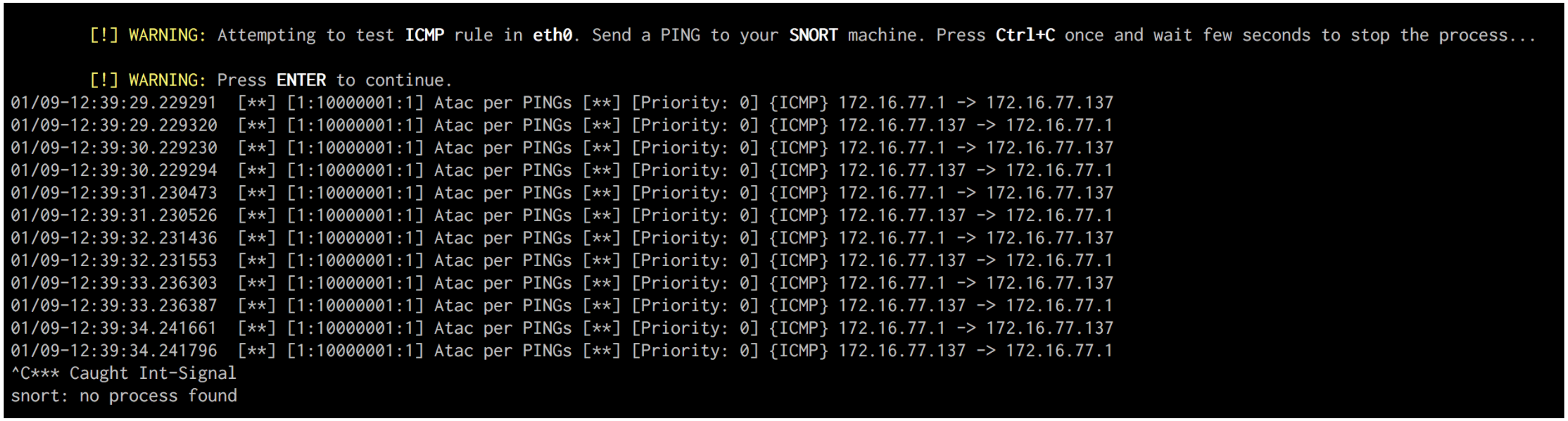
```

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

```

- Ahora la salida. Por defecto, se habilita el formato de salida `unified2`, pero puedes habilitar más de una salida. Voy a habilitar la salida en CSV y formato TCPdump.



```
[i] INFO: Enabling local.rules and adding a PING detection rule...
[!] WARNING: Unified2 output configured. Configure another output?
        1 - CSV output
        2 - TCPdump output
        3 - CSV and TCPdump output
        4 - None

Option [1-4]: 
```

- Ahora `SNORT` arrancará en modo `consola`. Manda un `PING` desde otra máquina para comprobar el funcionamiento.

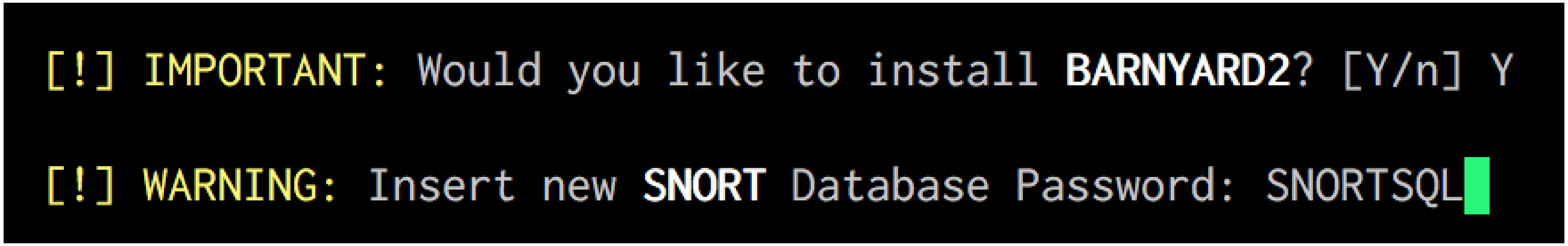


```
        [!] WARNING: Attempting to test ICMP rule in eth0. Send a PING to your SNORT machine. Press Ctrl+C once and wait few seconds to stop the process...

        [!] 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
```

- Mostrará una alerta de `PING`. Pulsa `Ctrl+C` una vez, y continua la instalación.

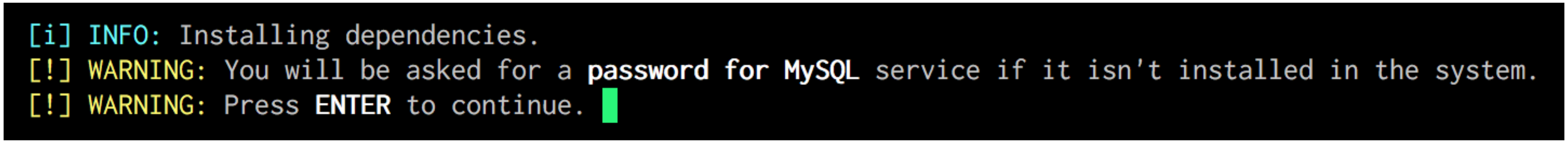
Instalación de `Barnyard2`

- Ahora toca instalar `BARNYARD2` si quieres.
- Se pide insertar una contraseña para la base de datos de `SNORT` que se va a crear. En el ejemplo uso `SNORTSQL`.



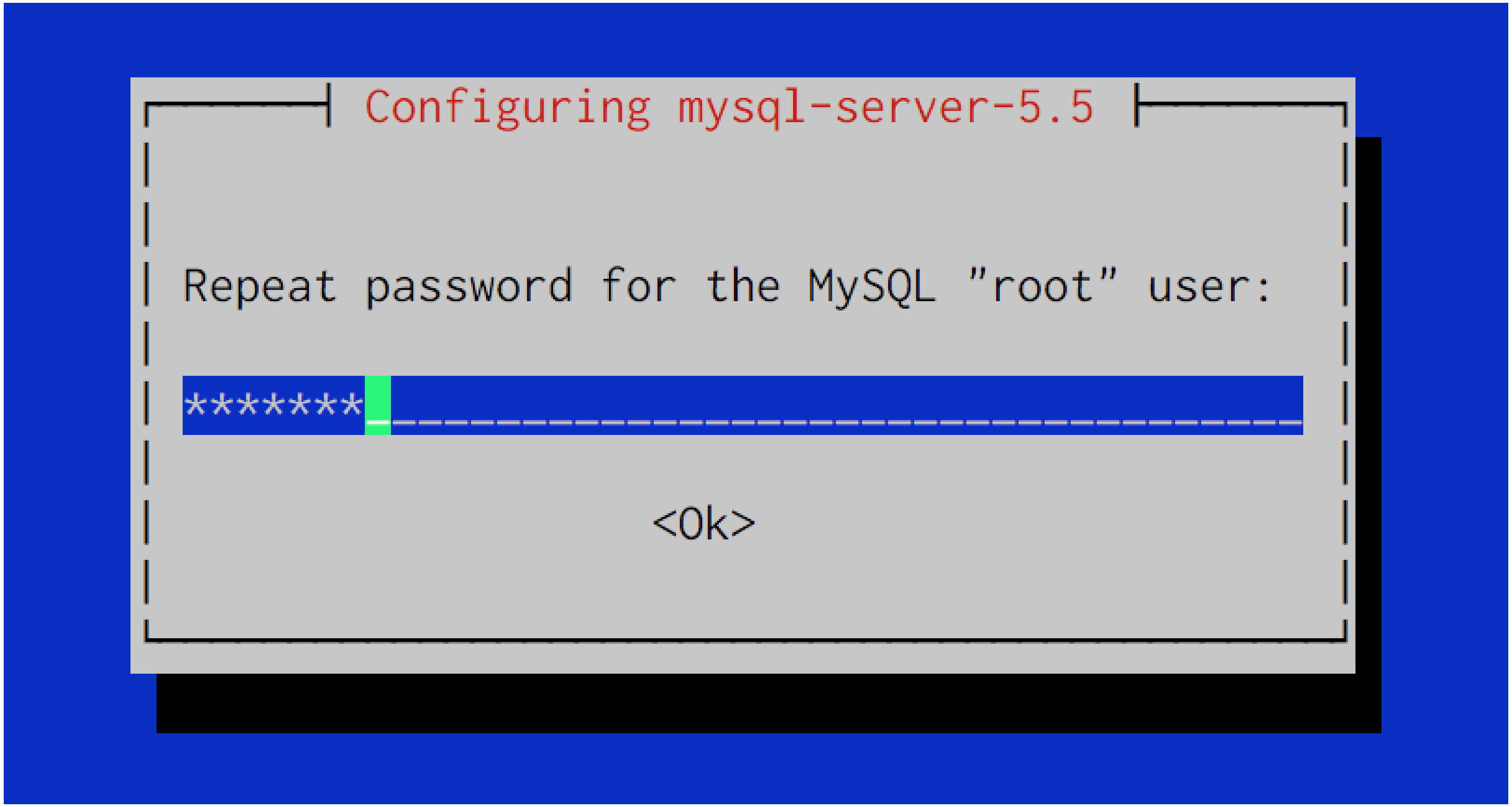
```
[!] IMPORTANT: Would you like to install BARNYARD2? [Y/n] Y

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

- Ahora el programa instalará algunas dependencias.
- Instalará `MySQL`, si no está instalado previamente, tendrás que introducir una contraseña de `root`. En el ejemplo, yo uso `ROOTSQL`.



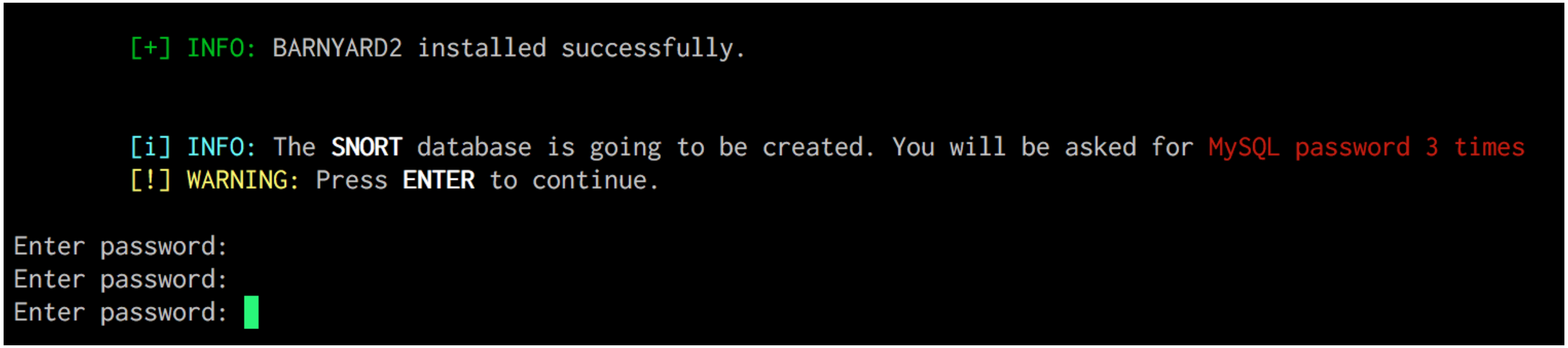
```
[i] INFO: Installing dependencies.
[!] WARNING: You will be asked for a password for MySQL service if it isn't installed in the system.
[!] WARNING: Press ENTER to continue.
```

- Y la contraseña del servicio `MySQL`.



```
Configuring mysql-server-5.5

Repeat password for the MySQL "root" user:

********

<Ok>
```

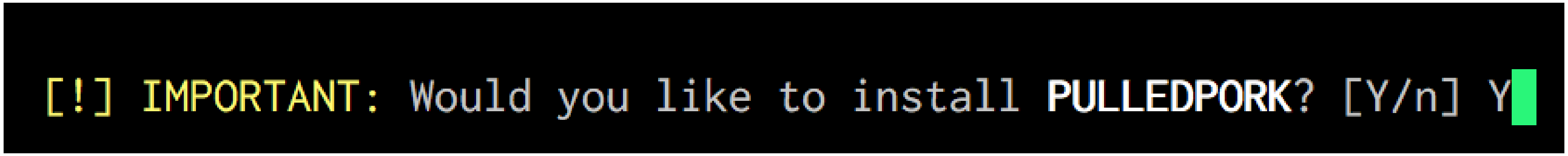
- Ahora el programa pregunta la contraseña de `MySQL` 3 veces
- Téngalo en cuenta: contraseña **`root`** de **`MySQL`** 3 veces.



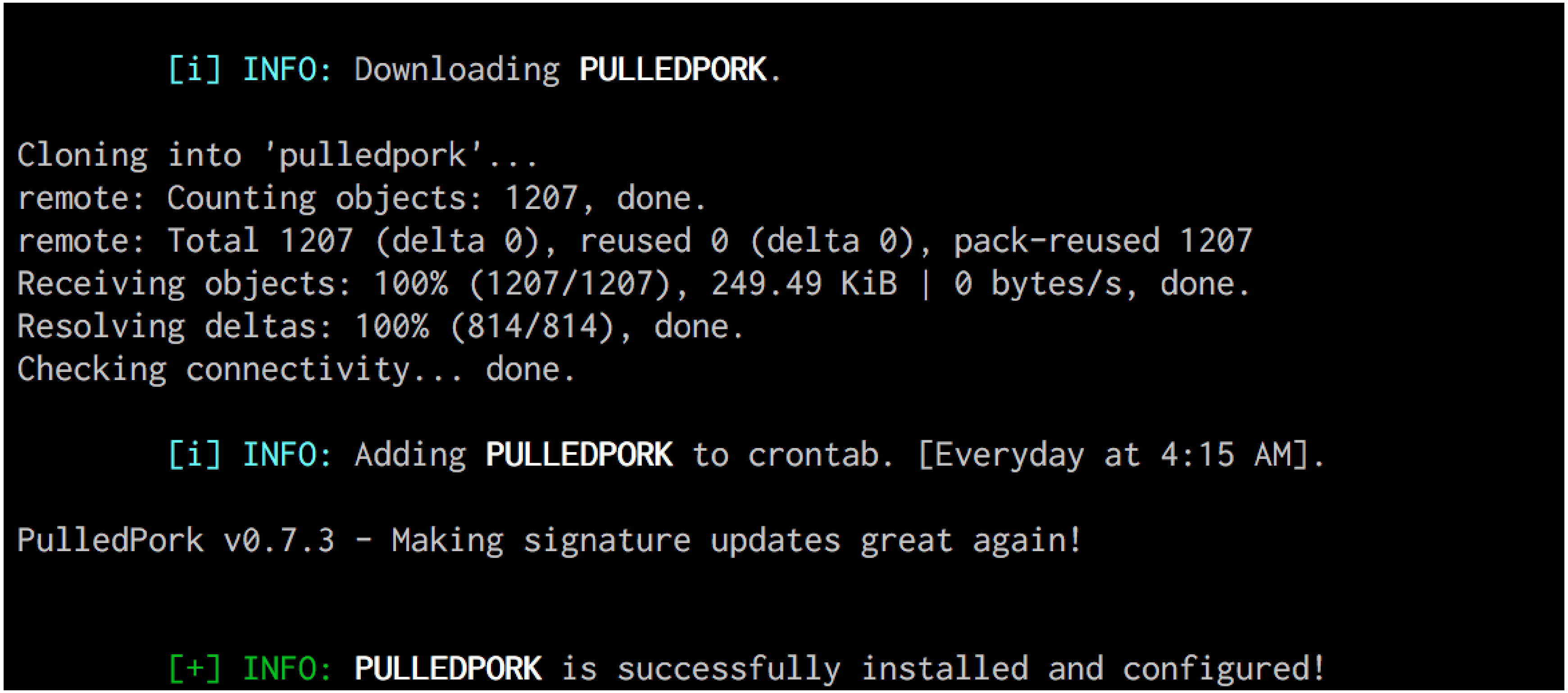
```
        [+] INFO: BARNYARD2 installed successfully.


        [i] INFO: The SNORT database is going to be created. You will be asked for MySQL password 3 times
        [!] WARNING: Press ENTER to continue.

Enter password:
Enter password:
Enter password:
```

Instalación de `PulledPork`

- Ahora toca instalar `PulledPork` si quieres.



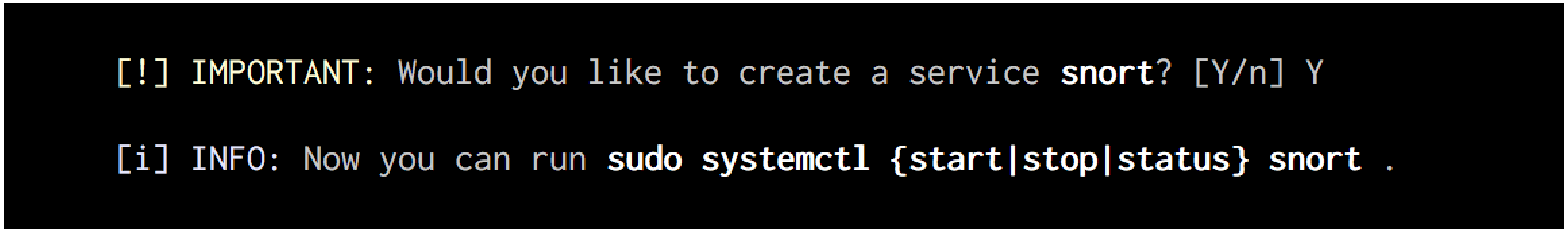
```
[!] IMPORTANT: Would you like to install PULLEDPORK? [Y/n] Y
```



```
        [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 `servicio`

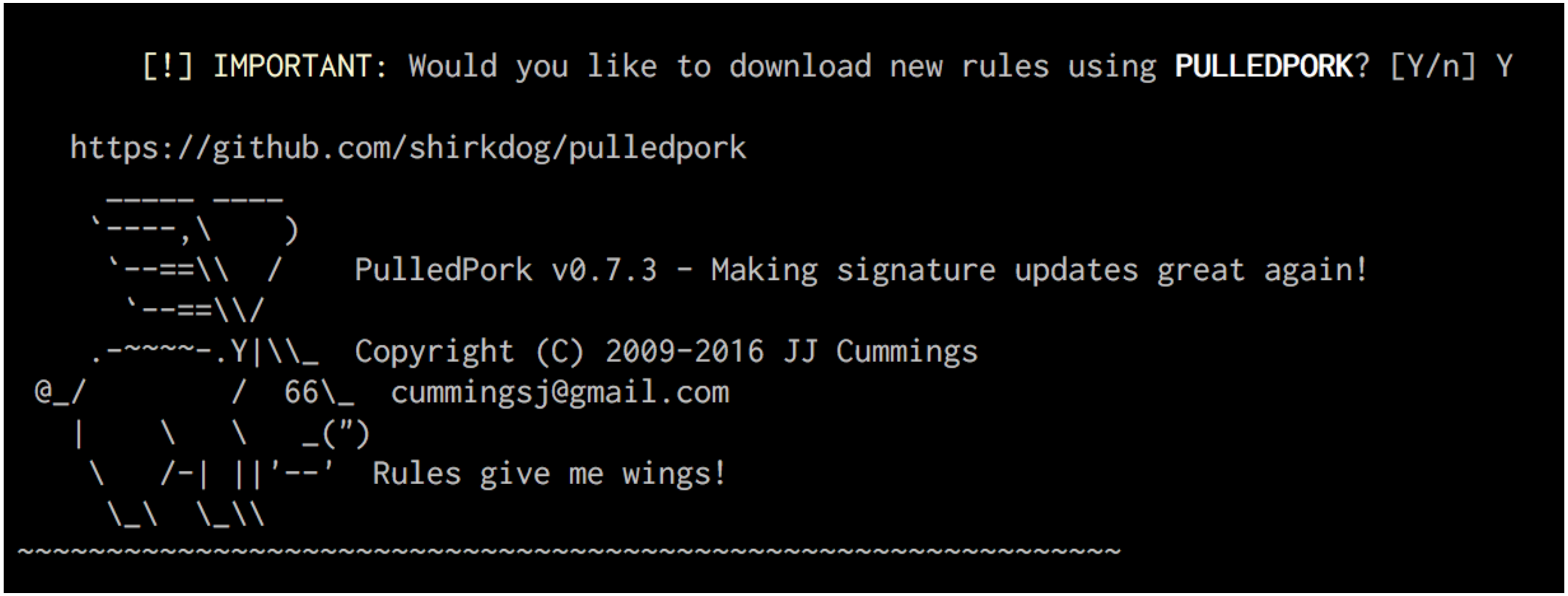
- Crear un `servicio` del sistema:



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

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

Descargar e instalar nuevas reglas

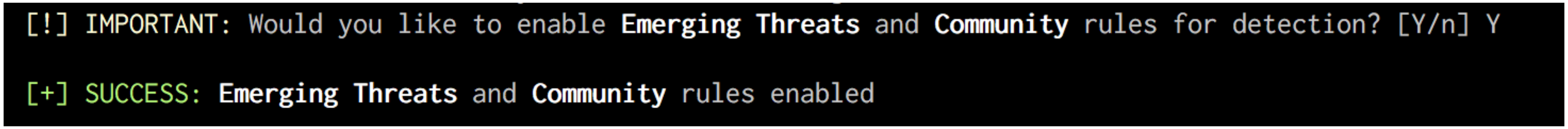
- Puedes descargar e instalar nuevas reglas cuando todo esté instalado y configurado.



```
       [!] IMPORTANT: Would you like to download new rules using PULLEDPORK? [Y/n] Y

   https://github.com/shirkdog/pulledpork
     _____ ____
    `----,\    )
     `--==\\  /    PulledPork v0.7.3 - Making signature updates great again!
      `--==\\/
    .-~~~~-.Y|\\_  Copyright (C) 2009-2016 JJ Cummings
 @_/        /  66\_  cummingsj@gmail.com
   |    \   \   _(")
    \   /-| ||'--'  Rules give me wings!
     \_\  \_\\
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

Habilitar reglas `Emerging Threats` y `Community`

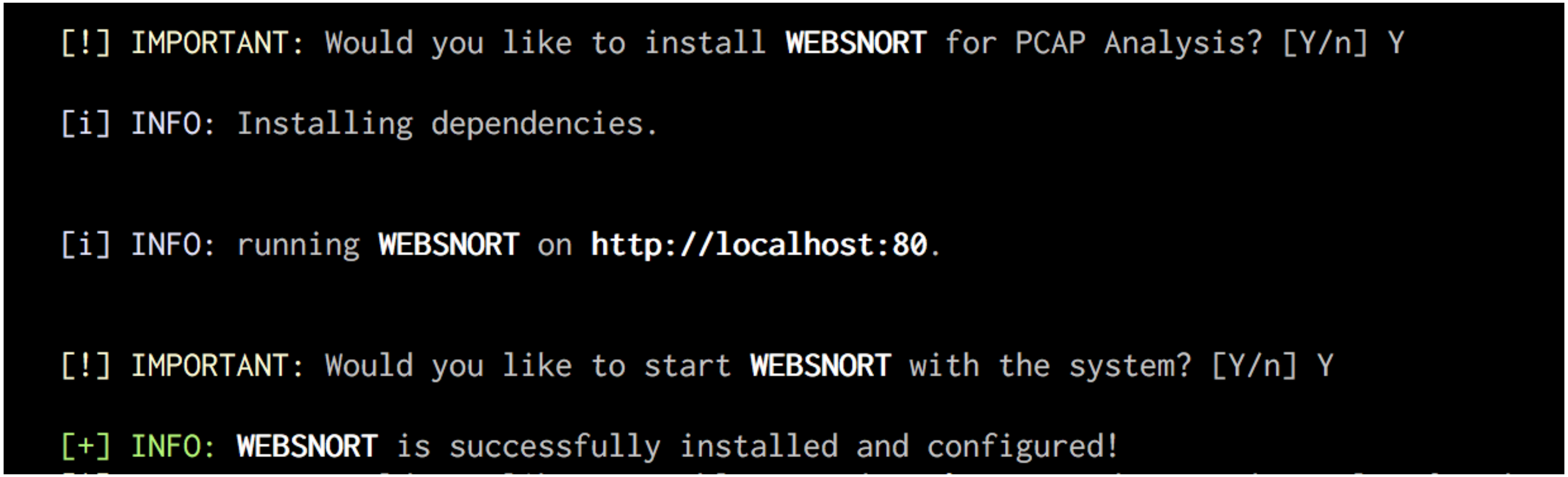
- Habilitar automáticamente en `snort.conf` las reglas de `Emerging Threats` y `Community`



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

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

WebSnort

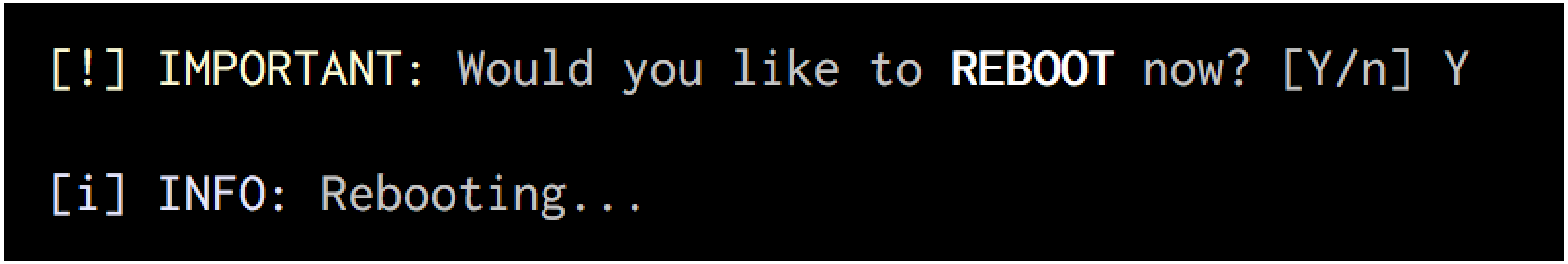
- Instalar WebSnort para análisis de `PCAPs`



```
[!] 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...
```