

Grado en Ingeniería Informática  
Seguridad en Tecnologías de la Información  
Curso 2017/18

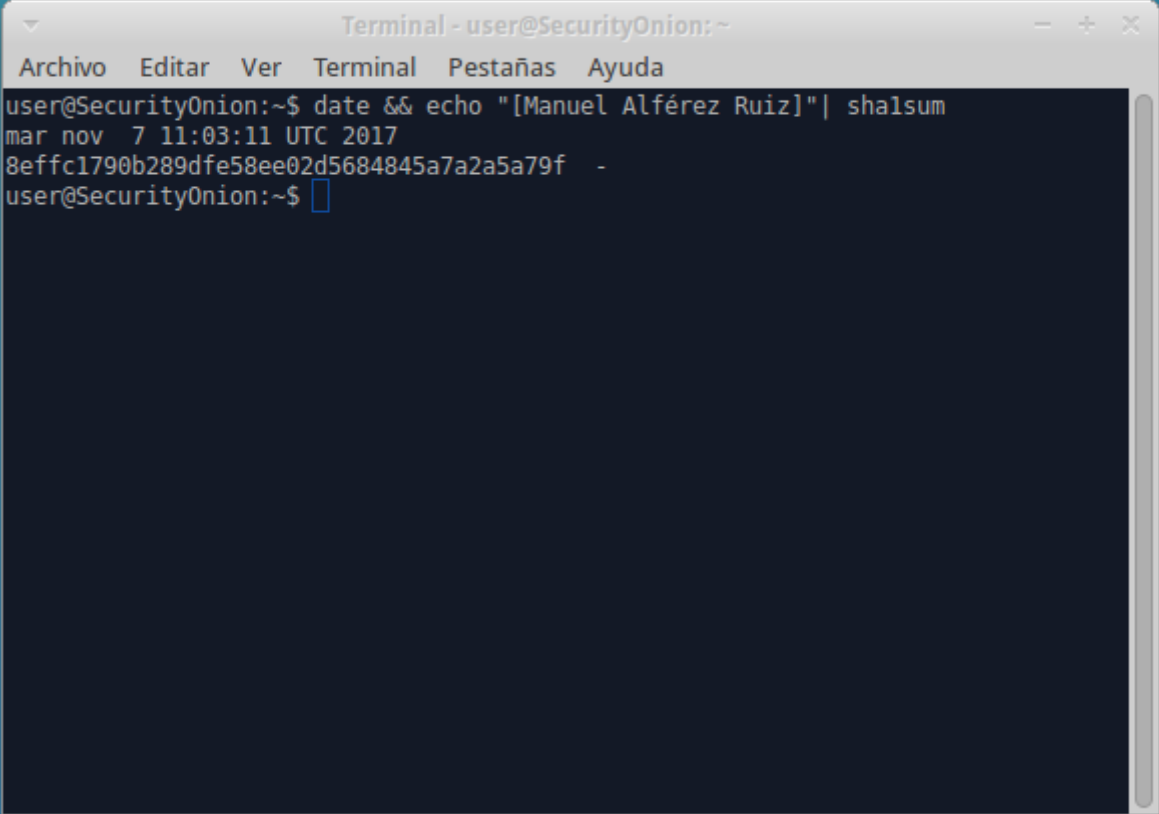
Práctica Número 7



**UNIVERSIDAD DE JAÉN**

Autor: Manuel Alférez Ruiz

**date && echo "[Manuel Alf3rez Ruiz]"| sha1sum**



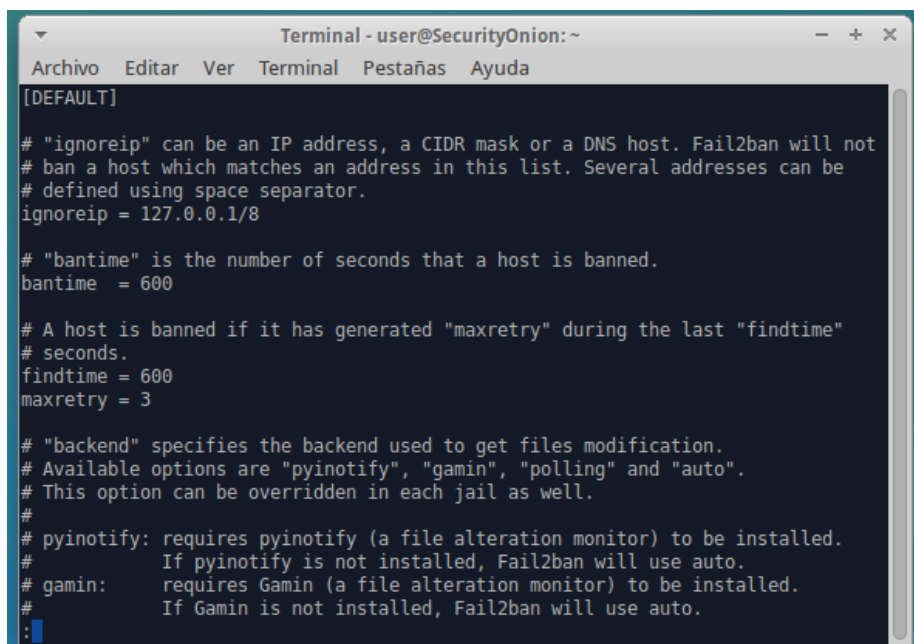
```
Terminal - user@SecurityOnion: ~
Archivo  Editar  Ver  Terminal  Pestañas  Ayuda
user@SecurityOnion:~$ date && echo "[Manuel Alf3rez Ruiz]"| sha1sum
mar nov  7 11:03:11 UTC 2017
8effc1790b289dfe58ee02d5684845a7a2a5a79f  -
user@SecurityOnion:~$
```

## Revisando el fichero de configuración de Fail2ban jail.conf

**bantime:** Es el tiempo que se mantiene una IP baneada. Por defecto viene 600 segundos, que son 10 minutos.

**maxretry:** Se refiere al número de intentos (está por defecto puesto a 3) que podemos ingresar usuario y contraseña.

**findtime:** Fija el tiempo durante el cual una IP tiene prohibida la entrada, después de haber sido baneada al haber superado el *maxretry*.



```
Terminal - user@SecurityOnion: ~
Archivo  Editar  Ver  Terminal  Pestañas  Ayuda

[DEFAULT]

# "ignoreip" can be an IP address, a CIDR mask or a DNS host. Fail2ban will not
# ban a host which matches an address in this list. Several addresses can be
# defined using space separator.
ignoreip = 127.0.0.1/8

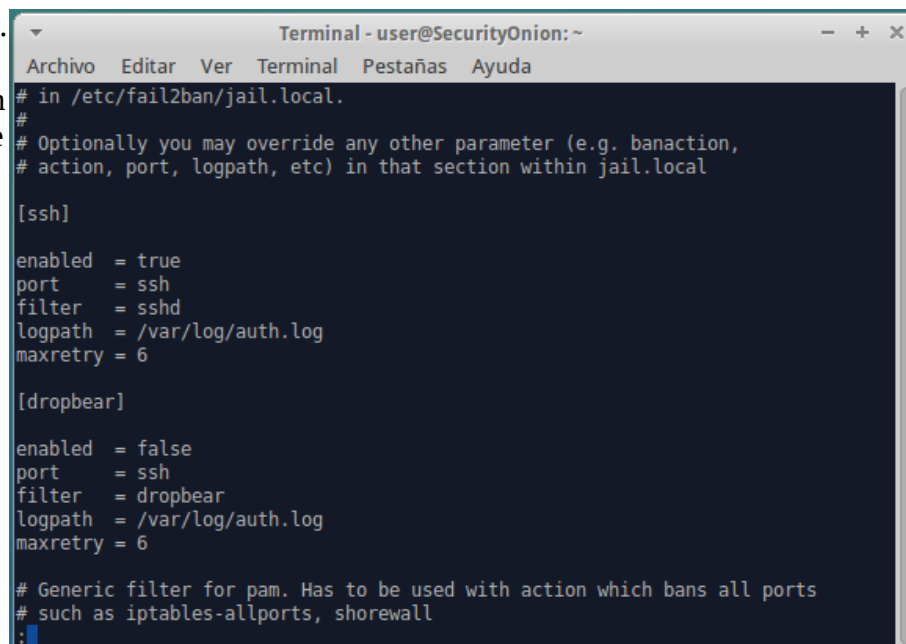
# "bantime" is the number of seconds that a host is banned.
bantime = 600

# A host is banned if it has generated "maxretry" during the last "findtime"
# seconds.
findtime = 600
maxretry = 3

# "backend" specifies the backend used to get files modification.
# Available options are "pyinotify", "gamin", "polling" and "auto".
# This option can be overridden in each jail as well.
#
# pyinotify: requires pyinotify (a file alteration monitor) to be installed.
#           If pyinotify is not installed, Fail2ban will use auto.
# gamin:    requires Gamin (a file alteration monitor) to be installed.
#           If Gamin is not installed, Fail2ban will use auto.
:
```

**port:** hace referencia al puerto.

**banaction:** Establece la acción que se usará cuando se alcance el umbral.



```
Terminal - user@SecurityOnion: ~
Archivo  Editar  Ver  Terminal  Pestañas  Ayuda

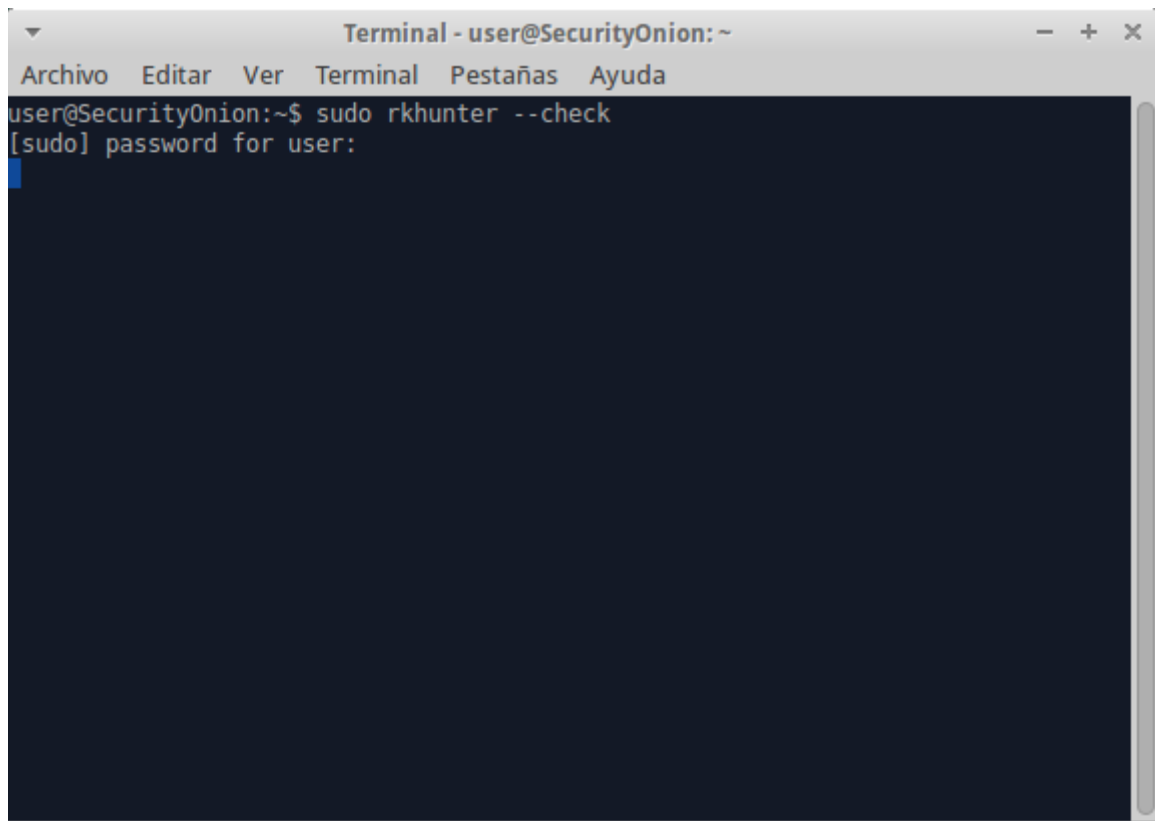
# in /etc/fail2ban/jail.local.
#
# Optionally you may override any other parameter (e.g. banaction,
# action, port, logpath, etc) in that section within jail.local

[ssh]
enabled = true
port    = ssh
filter  = sshd
logpath = /var/log/auth.log
maxretry = 6

[dropbear]
enabled = false
port    = ssh
filter  = dropbear
logpath = /var/log/auth.log
maxretry = 6

# Generic filter for pam. Has to be used with action which bans all ports
# such as iptables-allports, shorewall
:
```

## sudo rkhunter --check



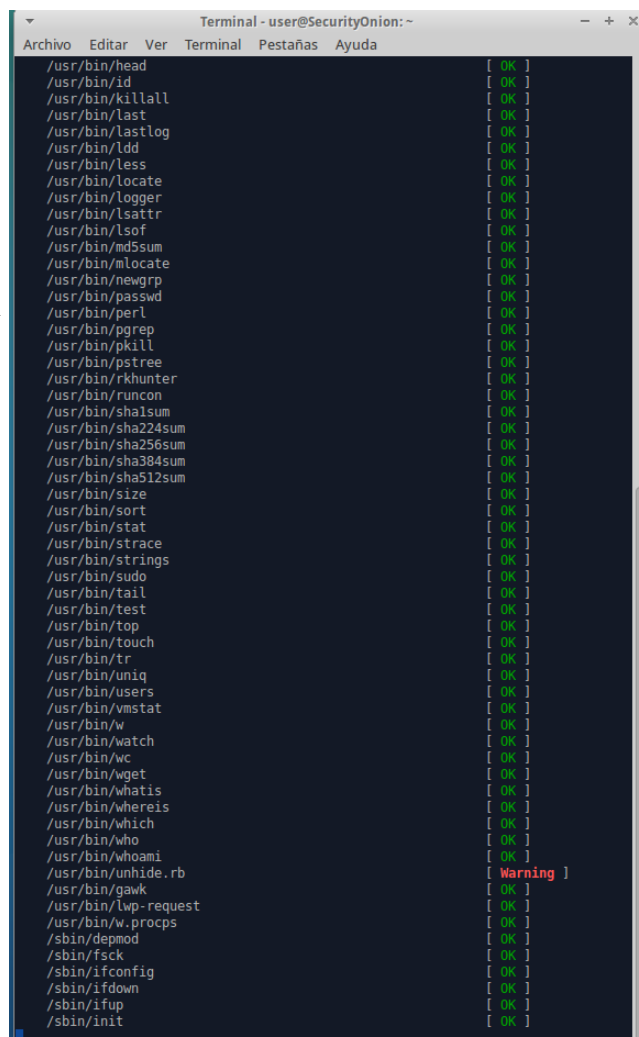
```
Terminal - user@SecurityOnion: ~
Archivo  Editar  Ver  Terminal  Pestañas  Ayuda
user@SecurityOnion:~$ sudo rkhunter --check
[sudo] password for user:
```

El *Warning* que aparece simplemente editando `/etc/rkhunter.conf` y agregando la siguiente línea en el lugar apropiado:

```
SCRIPTWHITELIST = / usr / bin /
unhide.rb
```

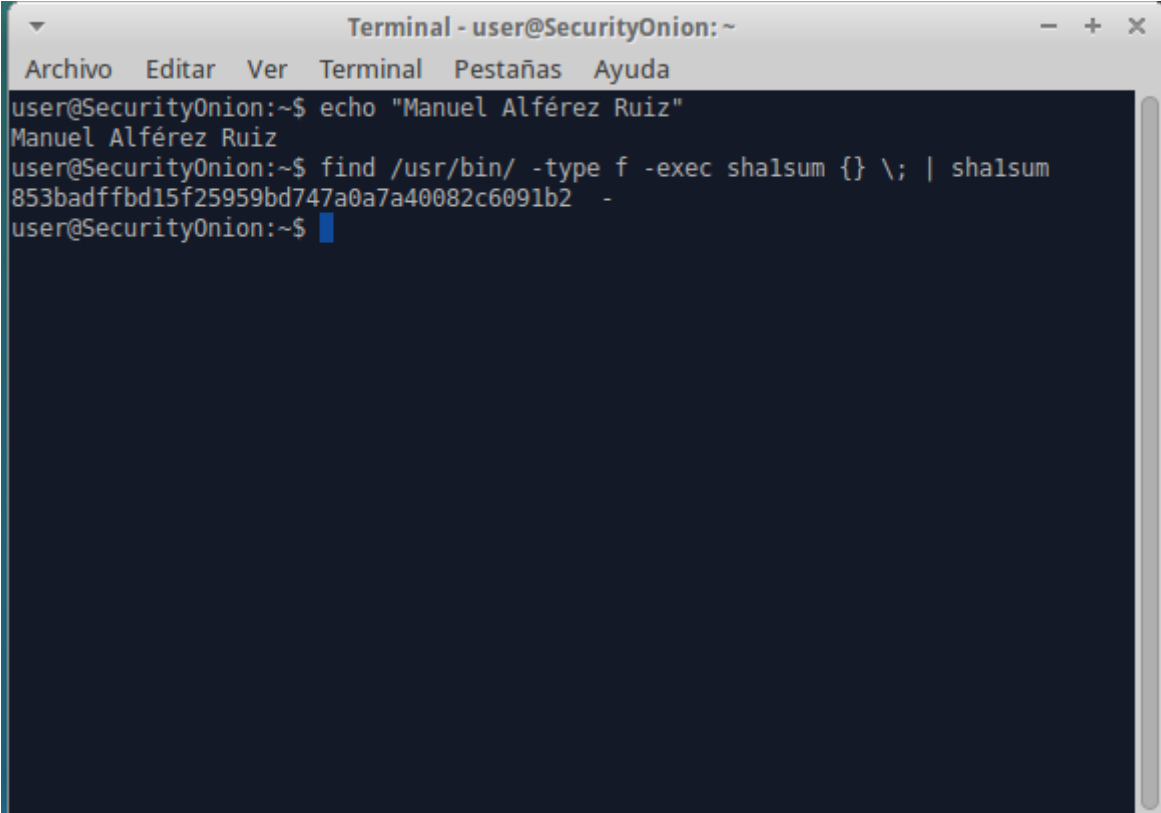
Se solucionaría. Y el problema es debido que está comparando la base de Linux en su estado original (como si la instalación estuviera recién hecha), pero al haber instalado ya varias aplicaciones desde la instalación de Linux aparece ese error.

Ese es el único *Warning* que me apareció.



```
Terminal - user@SecurityOnion: ~
Archivo  Editar  Ver  Terminal  Pestañas  Ayuda
/usr/bin/head [ OK ]
/usr/bin/id [ OK ]
/usr/bin/killall [ OK ]
/usr/bin/last [ OK ]
/usr/bin/lastlog [ OK ]
/usr/bin/ldd [ OK ]
/usr/bin/less [ OK ]
/usr/bin/locate [ OK ]
/usr/bin/logger [ OK ]
/usr/bin/lsattr [ OK ]
/usr/bin/lsof [ OK ]
/usr/bin/md5sum [ OK ]
/usr/bin/mlocate [ OK ]
/usr/bin/newgrp [ OK ]
/usr/bin/passwd [ OK ]
/usr/bin/perl [ OK ]
/usr/bin/pgrep [ OK ]
/usr/bin/pkill [ OK ]
/usr/bin/pstree [ OK ]
/usr/bin/rkhunter [ OK ]
/usr/bin/runcon [ OK ]
/usr/bin/sha1sum [ OK ]
/usr/bin/sha224sum [ OK ]
/usr/bin/sha256sum [ OK ]
/usr/bin/sha384sum [ OK ]
/usr/bin/sha512sum [ OK ]
/usr/bin/size [ OK ]
/usr/bin/sort [ OK ]
/usr/bin/stat [ OK ]
/usr/bin/strace [ OK ]
/usr/bin/strings [ OK ]
/usr/bin/sudo [ OK ]
/usr/bin/tail [ OK ]
/usr/bin/test [ OK ]
/usr/bin/top [ OK ]
/usr/bin/touch [ OK ]
/usr/bin/tr [ OK ]
/usr/bin/uniq [ OK ]
/usr/bin/users [ OK ]
/usr/bin/vmstat [ OK ]
/usr/bin/w [ OK ]
/usr/bin/watch [ OK ]
/usr/bin/wc [ OK ]
/usr/bin/wget [ OK ]
/usr/bin/whatis [ OK ]
/usr/bin/whereis [ OK ]
/usr/bin/which [ OK ]
/usr/bin/who [ OK ]
/usr/bin/whoami [ OK ]
/usr/bin/unhide.rb [ Warning ]
/usr/bin/gawk [ OK ]
/usr/bin/lwp-request [ OK ]
/usr/bin/w.procps [ OK ]
/sbin/depmod [ OK ]
/sbin/fsck [ OK ]
/sbin/ifconfig [ OK ]
/sbin/ifdown [ OK ]
/sbin/ifup [ OK ]
/sbin/init [ OK ]
```

**find /usr/bin/ -type f -exec sha1sum {} \; | sha1sum**

A terminal window titled "Terminal - user@SecurityOnion: ~" with a menu bar containing "Archivo", "Editar", "Ver", "Terminal", "Pestañas", and "Ayuda". The terminal shows the following commands and output:

```
user@SecurityOnion:~$ echo "Manuel Alf  rez Ruiz"
Manuel Alf  rez Ruiz
user@SecurityOnion:~$ find /usr/bin/ -type f -exec sha1sum {} \; | sha1sum
853badffbd15f25959bd747a0a7a40082c6091b2 -
user@SecurityOnion:~$
```