

7. TESTEO DE PRELUDE.

7.1. Testeo del conexiones.

De manera opcional, se puede testear prelude-lml con el siguiente comando mientras se produce una alerta en otra ventana.

```
# tail -f /var/log/prelude.log
```

los logs recibidos se almacenarán en /var/log/prelude.log y tendrán el siguiente formato en el caso de error de autenticación.

/var/log/prelude.log

```
*** Additional data within the alert *****
* Log received from: /var/log/auth.log
* Original Log:
Jan 1 19:03:56 <hostname> sshd(pam_unix) [23693]: authentication
failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=localhost
user=<your username>
*
*****
```

Veamos que con el comando *netstat* se muestra como hay una conexión establecida (rojo) y se sigue escuchando por el puerto especificado (azul).

```
Linux# netstat --inet --apn
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State                   PID/Program name
tcp        0      0 127.0.0.1:4960          0.0.0.0:*                 LISTEN                  9039/prelude-manage
tcp        0      0 127.0.0.1:5432          0.0.0.0:*                 LISTEN                  8987/postmaster
tcp        0      0 127.0.0.1:445          0.0.0.0:*                 LISTEN                  9042/smbd
tcp        0      0 127.0.0.1:40362        127.0.0.1:5432          ESTABLISHED             9039/prelude-manage
tcp        0      0 127.0.0.1:5432        127.0.0.1:40362        ESTABLISHED             9050/postgres: prel
udp        0      0 127.0.0.1:32768        127.0.0.1:32768        ESTABLISHED             8987/postmaster
tcp        0      0 0.0.0.0:111            0.0.0.0:*                 LISTEN                  8664/portmap
tcp        0      0 127.0.0.1:5335         0.0.0.0:*                 LISTEN                  8936/mDNSResponder
tcp        0      0 127.0.0.1:797          0.0.0.0:*                 LISTEN                  8677/famd
udp        0      0 192.168.100.72:137     0.0.0.0:*                 9045/nmbd
udp        0      0 0.0.0.0:137            0.0.0.0:*                 9045/nmbd
udp        0      0 192.168.100.72:138     0.0.0.0:*                 9045/nmbd
udp        0      0 0.0.0.0:138            0.0.0.0:*                 9045/nmbd
udp        0      0 0.0.0.0:5353           0.0.0.0:*                 8936/mDNSResponder
udp        0      0 0.0.0.0:111            0.0.0.0:*                 8664/portmap
```

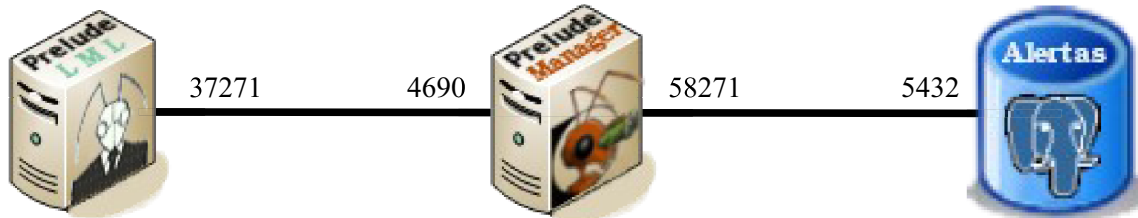


Figura 32.- Esquema mínimo de conexión y puertos.

Cuando usemos PGAdmin 3, para uso de la base de datos, aparecen dos líneas más de conexión TCP establecida.

tcp	0	0	127.0.0.1:40361	127.0.0.1:5432	ESTABLISHED	9039/pgadmin3
tcp	0	0	127.0.0.1:5432	127.0.0.1:40361	ESTABLISHED	9050/postgres: prel

7.2. Testeo del envío de mensajes del cortafuegos Shorewall al Prelude-Manager.

Para testear los logs generados con el cortafuegos, configuramos el cortafuegos Shorewall. Para su correcto uso será necesario tener cargado el módulo *ip_tables*, entre otros, de modo que nos deberemos asegurar en primer lugar que en el menuconfig están habilitados:

7.2.1. Carga de módulos para configuración de Shorewall.

```
localhost ~ # cd /usr/src/linux/
localhost linux ~ # make menuconfig
```

Networking → Networking support → Networking options → [*] Network packet filtering (replaces ipchains) → IP: Netfilter Configuration

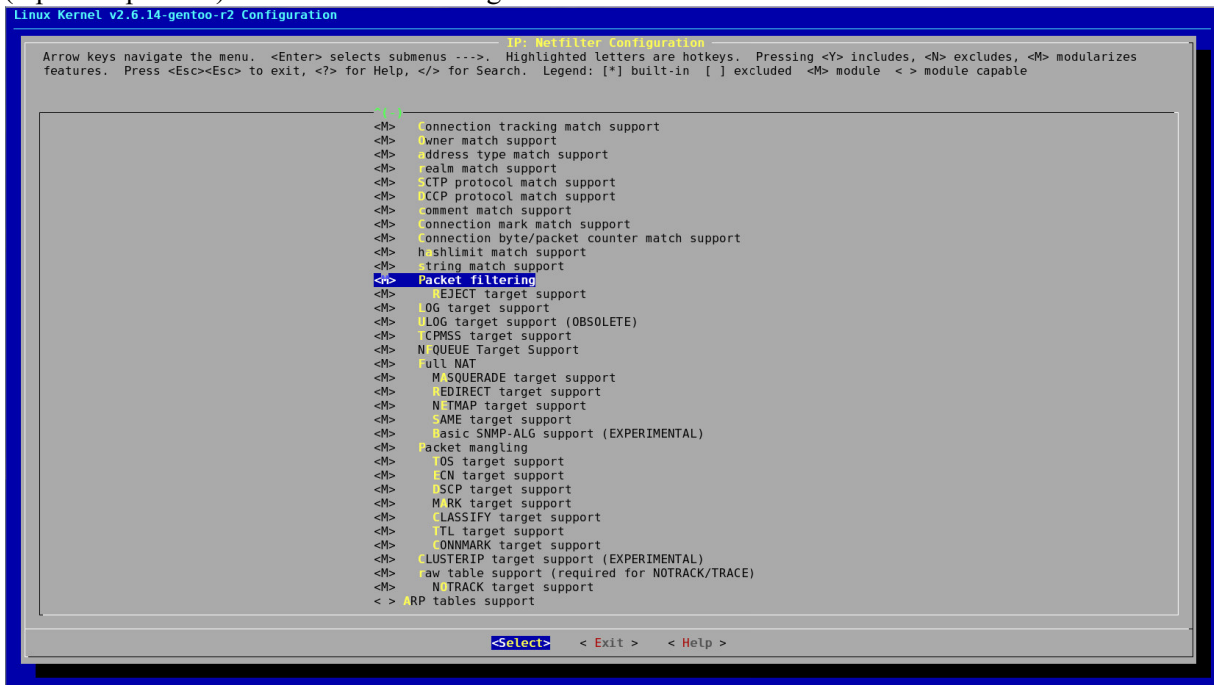


Figura 33.- Activación de módulos en el panel de configuración del núcleo de Linux.

Activamos todos los módulos a excepción del soporte para tablas ARP, que no será necesario y creamos la imagen.

```
localhost linux ~ # make bzImage modules_install
localhost linux ~ # mount /boot
localhost linux ~ # cp arch/i386/boot/bzImage /boot/bzImage-2.6.14-r2
localhost linux ~ # cp System.map /boot/System.map
localhost linux ~ # cp .config /boot/config
```

7.2.2. Configuración de ficheros de Shorewall.

/etc/shorewall/shorewall.conf

```
STARTUP_ENABLED=Yes
```

/etc/shorewall/interfaces

```
net      eth0          detect
```

/etc/shorewall/rules

```
#ACTION      SOURCE DEST   PROTO  DEST   SOURCE  ORIGINAL RATE USER
ACCEPT:info  fw     all    icmp
ACCEPT:info  fw     all    tcp    22
```

Hemos configurado a modo de ejemplo que se generen logs de firewall al hacer ping (icmp) o al conectar por ssh (puerto 22). Se pueden añadir tantas reglas como sea necesario.

/etc/shorewall/policy

```
#SOURCE      DEST      POLICY  LOG      LIMIT:BURST
all          all       ACCEPT
```

/etc/shorewall/zones

```
#ZONE          DISPLAY  COMMENTS
net            Net
```

7.2.3. Comprobación de los mensajes en la base de datos.

Hecho lo anterior hemos habilitado la regla de ssh. Supongamos que Prelude-Manager está instalado en la máquina *linux1* Hacemos desde una máquina:

```
linux2# ssh root@linux1
```

Accedemos a la consola de Postgre desde la máquina *linux1* y ejecutamos el comando SQL para obtener las últimas alertas ordenadas por fecha. El campo *_parent_type = 'A'* indica que no se muestren los *heartbeats*. Se comprueba cómo se detecta un registro como administrador como última alerta recibida por el Prelude-Manager y almacenada en la base de datos de eventos.

```
linux1# psql -U usuario eventdb
Bienvenido a psql 8.1.3, el terminal interactivo de PostgreSQL.
Digite: \copyright para ver los términos de distribución
         \h para obtener ayuda sobre comandos SQL
         \? para obtener ayuda sobre comandos internos
         \g o punto y coma (;) para ejecutar consulta
         \q para salir
eventdb=> SELECT t1.text, t0.time, t0.gmtoff FROM prelude_classification AS t1,
prelude_createtime AS t0 WHERE t0._message_ident = t1._message_ident AND
t0._parent_type = 'A' ORDER BY t0.time DESC;
      text                |      time                | gmtoff
-----+-----
Admin login successful    | 2006-05-17 06:55:35      | 7200
User authentication successful | 2006-05-17 06:55:35      | 7200
User authentication successful | 2006-05-17 06:55:14      | 7200
Admin login successful    | 2006-05-17 06:54:55      | 7200
User authentication successful | 2006-05-17 06:54:43      | 7200
(6 filas)
```

7.3. Testeo del sistema Prelude con Prewikka.

Prewikka es una herramienta de monitorización por medio de una interfaz web de los logs recibidos a los archivos especificados en `/etc/prelude-lml/prelude-lml.conf`, por lo que será de gran ayuda para monitorizar pruebas y ajustes en la definición de las clases para el manejo de `libpreludedb`.

Tras haber instalado con `emerge` la versión 0.9.2 (7-dic-2005), procedemos a la creación de la base de datos *prewikka*.

```
# su - postgres
postgres# createdb -W prewikka
  Contraseña: prewikka

postgres# createuser -W prewikka
  Contraseña: prewikka

postgres# psql -U prewikka -d prewikka
Bienvenido a psql 8.1.3, el terminal interactivo de PostgreSQL.

Digite: \copyright para ver los términos de distribución
        \h para obtener ayuda sobre comandos SQL
        \? para obtener ayuda sobre comandos internos
        \g o punto y coma (;) para ejecutar consulta
        \q para salir
```

Ya tenemos creada la base de datos y el usuario *prewikka*. A continuación se añaden las tablas de Prewikka a la base de datos. Y editamos el fichero de configuración.

```
prewikka=# \i /usr/share/prewikka/database/pgsql.sql
prewikka=# \i /usr/share/prewikka/database/pgsql-update-0.9.1.sql
```

`/etc/prewikka/prewikka.conf`

```
[interface]
software: Prewikka
place: Empresa de Seguridad S.L.
title: Prelude Management

[command]
whois: /usr/bin/whois
traceroute: /usr/sbin/traceroute

[idmef_database]
type: postgresql
host: localhost
user: eventdb
pass: prelude
name: eventdb

[database]
type: postgresql
host: localhost
user: prewikka
pass: prewikka
name: prewikka
```

```
[log stderr]

[auth loginpassword]
expiration: 60
```

Hay dos opciones para usar prewikka: crear un host virtual o un alias.

7.4. Creación de un host virtual para Apache.

Creamos un host virtual en Apache 2 para testear Prewikka-0.9.2, editando el fichero vhost.conf:

/etc/apache/conf/vhosts/vhosts.conf

```
<VirtualHost 127.0.0.1:80>
    ServerName prewikka.domain.tld
    ErrorLog /var/log/apache2/error_log
    CustomLog /var/log/apache2/access_log combined
    <Location "/">
        AllowOverride None
        Options ExecCGI
        <IfModule mod_mime.c>
            AddHandler cgi-script .cgi
        </IfModule>
    Order allow,deny
    Allow from all
    </Location>
Alias /prewikka/ /usr/share/prewikka/htdocs/
ScriptAlias / /usr/share/prewikka/cgi-bin/prewikka.cgi
</VirtualHost>
```

Bastará con acceder por el navegador a la dirección <http://mihostname> especificada en el fichero anterior. Para el caso especificado, sería <http://127.0.0.1>. Tanto el login como el password por defecto serán “admin”.

7.5. Creación de un Alias Apache Prewikka sin host virtual.

Esta opción es muy útil si es posible cambiar la configuración DNS. Para ello basta con crear el siguiente archivo en la dirección especificada.

/etc/apache/modules.d/98_prewikka.conf

```
Alias /prewikka/prewikka/ /usr/share/prewikka/htdocs/
ScriptAlias /prewikka/ /usr/share/prewikka/cgi-bin/prewikka.cgi
<Directory /usr/share/prewikka/htdocs/>
    Options None
    AllowOverride None
    Order allow,deny
    Allow from all
</Directory>
<Directory /usr/share/prewikka/cgi-bin/>
    AllowOverride None
    Options ExecCGI
    <IfModule mod_mime.c>
```

```
AddHandler cgi-script .cgi
</IfModule>
Order allow,deny
Allow from all
</Directory>
```

En este caso, el acceso sería con <http://mihostname/prewikka>, siempre y cuando se hayan incluido las siguientes líneas en el httpd.conf.

/etc/apache2/httpd.conf

```
# Gentoo VHosts
#
# For Gentoo we include External Virtual Hosts Files.
# See vhosts.d/00_default_vhost.conf for the default virtual host
#
Include /etc/apache/vhosts.d/*.conf
Include /etc/apache/conf/vhosts/*.conf
Include /etc/apache/modules.d/*.conf
```

Para ambos casos hay que arrancar el servicio y añadirlo al rc-conf para la próxima vez que se inicie.

```
% /etc/init.d/apache start
% rc-update add apache default
```

7.6. Capturas del testeo.

Prewikka posee tres niveles de monitorización. El primero de ellos, es el listar todas las alertas producidas en el tiempo especificado agrupadas por tres parámetros: dirección origen, dirección destino e intervalo temporal. A continuación se detallan las capturas de estos tres niveles de monitorización.

Prewikka 0.9.2 Alejandro Galera

Alerts | Heartbeats | Filters prewikka on Thursday December 29 2005 | logout

Classification	Source	Target	Sensor	Time	
2 x Admin login failed (failed)			sshd (palocortado)		
6 x Promiscuous mode detected (succeeded)		palocortado	sudo (palocortado)		
88 x User authentication successful (succeeded)	user: 0	127.0.0.1	kernel (palocortado)	2005-12-21 10:54:30 - 2005-12-14 17:25:23	
4 x User Created (succeeded)		user: postgres process: su(pam_unix) (12037)	shadow-utils (palocortado)		
2 x Group Created (succeeded)			PAM (palocortado)		
79 x SUDO Command Executed (succeeded)					
5 x User authentication failed (failed)	user: 1000	palocortado	PAM (palocortado)	2005-12-20 00:46:48 - 2005-12-14 17:23:39	
1 x User login successful (succeeded)	192.168.100.61:41595/tcp	palocortado:22/tcp	sshd (palocortado)	2005-12-16 12:58:09 - 2005-12-15 13:47:11	
1 x Admin login successful (succeeded)		127.0.0.1:22/tcp			
		user: root process: sshd (11210)			
User authentication failed (failed)	elmo	palocortado	PAM (palocortado)	2005-12-16 12:58:04	
	user: 0	127.0.0.1			
		user: root process: sshd(pam_unix) (11212)			
User login successful (succeeded)	192.168.100.60:36422/tcp	palocortado:22/tcp	sshd (palocortado)	2005-12-15 10:27:01	
		127.0.0.1:22/tcp			
		user: aledavid process: sshd (11163)			
User authentication failed (failed)	192.168.100.72	palocortado	PAM (palocortado)	2005-12-14 17:26:09	
	user: 0	127.0.0.1			
		user: root process: sshd(pam_unix) (16344)			
31 x User authentication successful (succeeded)	user: 1000	palocortado	PAM (palocortado)	2005-12-14 12:30:14 - 2005-12-12 11:19:44	
2 x Promiscuous mode detected (succeeded)		192.168.100.72	kernel (palocortado)		
		user: root process: su(pam_unix) (12072)			
Logfile inconsistency (succeeded)	n/a	/var/log/messages	prelude-lml	2005-12-12 18:56:42	Delete

Filter: [] Step: 13 | Unlimite | Tz: Frontend localt | Limit: 100 | Apply | Save | Unlimited | +01:00 | prev | current | next | 1 ... 8 (total:8) | Done

Figura 34.- Primer nivel de información agrupada de Prewikka.

Para este primero, el testeo se ha realizado teniendo en cuenta los *Syslog* únicamente. El intervalo temporal se define por el FTS y LTS. El *First Time Seen* es la marca más antigua límite del intervalo, o la primera vez que vista la alerta. Dicha marca será la especificada en la columna gris de Prewikka. El *Last Time Seen* se tomará como la hora actual del sistema, aunque el valor obtenido de la última vez vista será un poco anterior a la marca actual.

Se obtienen ocho metafilas las cuales tienen 6, 1, 2, 1, 1, 1, 2, y 1 filas respectivamente. En el campo *Classification* aparece el número de repeticiones de ese tipo de evento entre la fuente y destino especificados, en el intervalo temporal indicado.

Pinchando en una metafila cuyo mensaje se haya producido más de una vez, llegamos al segundo nivel de Prewikka, en el que se detallan tantas metafilas como veces se haya repetido.

The screenshot shows the Prewikka 0.9.2 interface. The top bar includes the version 'Prewikka 0.9.2' and the user 'Alejandro Galera'. Below the navigation tabs (Alerts, Heartbeats, Filters), there is a table of events. The table has columns for Classification, Source, Target, Sensor, and Time. The events listed are 'User authentication failed (failed)' with various sources and targets, all detected by the 'PAM (palocortado)' sensor. The interface also includes a sidebar with navigation options and a filter section.

Classification	Source	Target	Sensor	Time
User authentication failed (failed)	user: 1000	palocortado 127.0.0.1 user: root process: su(pam_unix) (19196)	PAM (palocortado)	2005-12-20 00:46:48
User authentication failed (failed)	user: 1000	palocortado 127.0.0.1 user: root process: su(pam_unix) (9725)	PAM (palocortado)	2005-12-15 09:18:14
User authentication failed (failed)	user: 0	palocortado 127.0.0.1 user: aledavid process: sudo(pam_unix) (26032)	PAM (palocortado)	2005-12-15 02:40:17
User authentication failed (failed)	user: 0	palocortado 127.0.0.1 user: aledavid process: sudo(pam_unix) (26031)	PAM (palocortado)	2005-12-15 02:40:06
User authentication failed (failed)	user: 1000	palocortado 127.0.0.1 user: root process: su(pam_unix) (16271)	PAM (palocortado)	2005-12-14 17:23:39

Figura 35.- Segundo nivel de detalle de eventos en Prewikka.

Para llegar al tercer nivel de información de Prewikka hay que pinchar en cualquier mensaje de los que se detallan en la captura anterior.

Si en el primer nivel de información agrupada por pares de direcciones origen y destino y número de repeticiones, se pincha en un evento que sólo se ha producido una vez, se pasa directamente al tercer nivel de información, mostrándose el siguiente informe detallado:

El informe consta de tantos campos más tipo Analyzer como sensores se hayan registrado en la instalación de Prelude. Por último, el campo Additional Data tendrá un número de filas dependiente del tipo de mensaje, al igual que la aparición o no de algunas filas o grupos completos.

Prewikka 0.9.2 Eneo Tecnologia SL Alejandro Galera

Alerts Heartbeats Filters prewikka on Friday December 30 2005 [logout](#)

Events

Agents

Users

About

Dates

Create time	2005-12-20T00:46:48.199468+01:00
Detect time	2005-12-20T00:46:48.00+01:00
Analyzer time	2005-12-20T00:46:48.199710+01:00

Classification

Text	User authentication failed
------	----------------------------

Impact

Description	User tried to authenticate as root and failed
Severity	high
Type	user
Completion	failed

Source

Address	
User category	os-device
current-user	1000 on tty pts/0

Target

Address	127.0.0.1
User category	os-device
target-user	root
Process	su(pam_unix)
Process Pid	19196

Analyzer

Analyzerid	1180318276865163
Name	prelude-manager
Model	Prelude Manager
Version	0.9.1
Class	Concentrator
Manufacturer	http://www.prelude-ids.com
Operating System	Linux 2.6.14-gentoo-r2

Figura 36.- Informe detallado de Prewikka (fragmento).