6.SENSORES.

6.1.Instalación de los Sensores.

Los sensores son los dispositivos hardware o software que se encargarán de transmitir específicamente un tipo de mensaje log. Los sensores que dispondremos serán:

- Sensor del sistema de detección de intrusiones: Snort IDS.
- Sensor de flujo de red: Netflow.
- Sensor de consistencia del sistema de ficheros: Samhain
- Sensor de cortafuegos: Firewall.
- Sensor de detección de dispositivos: Pads, Arpwatch.

6.1.1.Registro de Prelude-LML.

Una vez que tenemos instalado el marco formado por prelude manager, su configuración y los paquetes de bases de datos, el paso siguiente es instalar los sensores. Para ello, bastará con registrarlos con el marco Prelude-Manager. Antes de introducir el password, deberemos abrir otra ventana como root (Ctrl+T) para ejecutar el servidor de registro.

```
 # prelude-adduser register prelude-lml "idmef:w admin:r" 192.168.100.72 --uid 0 --
gid 0

 - Using default TLS settings from /etc/prelude/default/tls.conf:
   - Generated key size: 1024 bits.
   - Authority certificate lifetime: unlimited.
   - Generated certificate lifetime: unlimited.

 - Adding analyzer prelude-lml.
   - Creating /etc/prelude/profile/prelude-lml...
   - Using already allocated ident for prelude-lml: 3023198534532421.
   - Creating /var/lib/spool/prelude/prelude-lml...

 - Registering analyzer idmef:w admin:r to localhost:5553.

   You now need to start "prelude-adduser" on the server host where
   you need to register to:

   use: "prelude-adduser registration-server <analyzer profile>"
   example: "prelude-adduser registration-server prelude-manager"

   This is used in order to register the 'sending' analyzer to the
   'receiving' analyzer. <analyzer profile> should be set to the
   profile name of the 'receiving' analyzer, the one where 'sending'
   analyzer will register to.
```

```
  Please remember that "prelude-adduser" should be used to register
  every server used by this analyzer.
  Enter the one-shot password provided by the "prelude-adduser"
  program:

  - Enter registration one shot password:
```

Este password será requerido cada vez que se ejecute el *prelude-adduser* de aquí en adelante. No lo podemos introducir a nuestra elección, dado que será generado por el servidor de registro.

En otra ventana, ejecutamos lo siguiente: el servidor de registro del gestor de prelude (Prelude-Manager registration server)

Consola del Servidor de Registro con Prelude-Manager.

```
# prelude-adduser registration-server prelude-manager

- Using default TLS settings from /etc/prelude/default/tls.conf:
  - Generated key size: 1024 bits.
  - Authority certificate lifetime: unlimited.
  - Generated certificate lifetime: unlimited.

- Adding analyzer prelude-manager.
  - Creating /etc/prelude/profile/prelude-manager...
  - Using already allocated ident for prelude-manager:
    3023198534532421.
  - Creating /var/lib/spool/prelude/prelude-manager...

- Starting registration server.
  - generated one-shot password is "demm73gx".

    This password will be requested by "prelude-adduser" in order to
    connect. Please remove the first and last quote from this
    password before using it.

  - Waiting for peers install request on 0.0.0.0:5553...
```

En este momento se queda a la espera de que en la otra ventana, el servidor de registro del Prelude-Manager asienta la operación. Cambiamos de ventana de nuevo y pulsamos **y** (yes) con lo que obtenemos el siguiente mensaje:

Consola del Sensor Prelude-LML.

```
  - connecting to registration server (localhost:5553)...
  - Sending certificate request.
  - Receiving signed certificate.
  - Receiving CA certificate.
- prelude-lml registration to localhost successful.
```

Al mismo tiempo, el servidor del registro genera los siguietes mensajes por pantalla:

Consola del Servidor de Registro.

```
- Connection from 192.168.100.72:5553.
  - Waiting for client certificate request.
```

```
- Analyzer with ID="1537698187535812" ask for registration with
  permission="idmef:w admin:r".
  Approve registration [y/n]: y

  Registering analyzer "1537698187535812" with permission "idmef:w
  admin:r".
- Generating signed certificate for client.
- Sending server certificate to client.
- 192.168.100.72:30098 successfully registered.
```

6.1.2.Configuración, ejecución y testeo de Prelude-LML.

En primer lugar editamos el archivo /etc/prelude-lml/prelude-lml.conf para configurar los archivos logs para el monitor. Para asignar una dirección y un puerto concreto, se puede dejar deshabilitado en dicho fichero ya que busca por defecto en client.conf ([25])

Podemos añadir líneas como las siguientes al archivo de configuración de Prelude-LML. Si poseemos una versión anterior a la 0.9.1 será necesario éstas de los syslogs y las de los metalogs

/etc/prelude-lml/prelude-lml.conf

```
[format=syslog]
time-format = "%b %d %H:%M:%S"
prefix-regex = "^(?P<timestamp>.{15}) (?P<hostname>\S+)
                    (?:(?P<process>\S+?)(?:\[(?P<pid>[0-9]+)\])?: )?"
file = /var/log/messages
# udp-server = 0.0.0.0

#[format=metalog]
#prefix-regex = "^(?P<timestamp>.{15}) \[(?P<program>\S+)\] "
#time-format = "%b %d %H:%M:%S"
#file = /var/log/everything/current
# udp-server = 0.0.0.0
```

De manera opcional, podemos añadir tantos ficheros de log como sensores poseamos. Se puede añadir auth.log para autenticación al hacer login ssh, shorewall.log para mensajes del cortafuegos, y como ejemplo se ilustra a continuación las líneas del registro de logs del servidor apache.

/etc/prelude-lml/prelude-lml.conf (continuación)

```
[format=apache]
time-format = "%d/%b/%Y:%H:%M:%S"
prefix-regex = "^(?P<hostname>\S+) - - \[(?P<timestamp>.{20})
                                                          \+.{4}\] "
file = /var/log/apache2/access_log
```

Necesitamos especificarle como puerto de escucha el que está usando prelude-manager, es decir, el 4960. Eso se lo haremos editando el client.conf. La dirección especificada como server_addr es la de escucha del prelude-manager. El puerto de escucha de los sensores lo escogerá el sistema para terminar el establecimiento de la conexión TCP/IP.

[25] Este fichero se encuentra en /etc/prelude/default/ y en /usr/local/etc/prelude/default/

/etc/prelude/default/client.conf

```
server_addr = 192.168.100.72:4960
```

Para la ejecución del monitor de logs de prelude (prelude-lml) podemos hacer dos cosas: ejecutar prelude en background o iniciar el servicio desde una consola del root.

```
# prelude-lml &
[1] 18460
# - Subscribing plugin pcre[default]
- Monitoring /var/log/messages through pcre[default]
- Checking for FAM writev() bug: FAM working nicely, enabling.
- pcre plugin added 307 rules.
- Connecting to 192.168.100.72:4690 prelude Manager server.
- TLS certificate: server certificate is trusted.
- TLS authentication succeed with Prelude Manager.
- /var/log/messages: Metadata available, starting log analyzis at
                                                    offset 6067311.
```

O bien se arranca el servicio:

```
# /etc/init.d/prelude-lml start
```

Por último, lo actualizamos el registro de arranque default para que se cargue la próxima vez al iniciar Gentoo.

```
# rc-update add prelude-lml default
```

6.1.3. Errores comunes al arrancar Prelude-LML:

6.1.3.1. Conexión no establecida con Prelude-Manager.

```
- Subscribing plugin pcre[default]
- Monitoring /var/log/messages through pcre[default]
     ...
- pcre plugin added 304 rules.
- Connecting to 127.0.0.1:4690 prelude Manager server.
prelude-connection: connection error with 127.0.0.1:4690:Connection refused.Failover enabled
```

Se debe a que el puerto especificado para escuchar en el prelude-manager no coincide con el del cliente por defecto. Hay que asegurarse que el puerto en la dirección de escucha en el archivo /etc/prelude-manager/prelude-manager.conf sea el mismo que en la del /etc/prelude/default/client.conf.

6.1.3.2. No se puede abrir fichero del perfil para escritura.

```
- Connecting to 127.0.0.1:4960 prelude Manager server.
couldn't open /usr/local/var/spool/prelude/prelude-lml/global/141 for writing: File exists.
```

No hay que preocuparse por estas advertencias de mensajes previos a la conexión entre prelude-lml y prelude-manager. Al finalizar las advertencias se establece la conexión TCP/IP, con la notificación del número de mensajes que no se pudo recuperar por el failover.

6.1.3.3. Opciones inválidas en las secciones de prelude-lml.conf.

```
/etc/prelude-lml/prelude-lml.conf:56: invalid option "time-format" in "global" section at depth 0.
/etc/prelude-lml/prelude-lml.conf:57: invalid option "prefix-regex" in "global" section at depth 0.
```

```
/etc/prelude-lml/prelude-lml.conf:58: invalid option "file" in "global" section at depth 0.
```

Se produce cuando en la edición del fichero /etc/prelude-lml/prelude-lml.conf, se han definido "time-format", "prefix-regex" y "file" para la sección global. Este error no lo dan versiones anteriores a la 0.9.1, y se soluciona escribiendo en el fichero indicado prelude-lml.conf, justo antes de las líneas que han dado el error, una sección entre corchetes. Por ejemplo: [format=syslog]

6.1.3.4. No se encuentra la plantilla de configuración del fichero.

```
- Using analyzer prelude-lml.
  - Using /etc/prelude/profile/prelude-lml...
could not open template configuration file: No such file or directory.
Usage prelude-adduser <subcommand> [options] [args]
Type "prelude-adduser <subcommand>" for help on a specific subcommand.
```

Se produce cuando se ha ejecutado *prelude-adduser add* y no están actualizados los ficheros de configuración de /etc/prelude/default. Actualizando a la última versión dichos ficheros y eliminando los anteriores se soluciona el problema y ya se permite la creación de perfiles.

6.1.3.5. No se puede compilar la expresión regular para los syslog en prelude-lml.conf

```
prelude-lml
- Subscribing plugin pcre[default]
- pcre plugin added 314 rules.
Unable to compile regex:
 ^(?P<timestamp>.{15}) (?P<hostname>\S+) (?:((?P<process>\S+)(\[(?P<pid>[0-9]+)\])?)?: )? :
 unrecognized character after (?.
failed to set log message prefix.
error while setting option 'format'.
```

Se debe a un error con la versión de *pcre* (Perl Common Regular Expressions). Se soluciona instalando la última versión y asegurándonos que no haya una versión existente anterior.

6.2.Snort IDS.

Se trata del sensor configurado como sistema de detección de intrusiones, de modo que informa de todos los intentos de ataques que se producen, incluidos falsos positivos. Cada intento de ataque entre un mismo origen y destino genera un nuevo mensaje IDS. Para *n* intentos de ataque, no generaría un mensaje con el número de intentos, sino que generaría *n* mensajes.

6.2.1.Registro y conexión de Snort a Prelude-Manager.

Una vez instalado prelude-lml y registrado con el prelude-manager, procedemos a la instalación del sensor Snort, utilizando el mismo procedimiento que en para *prelude-lml*.

Snort ha reemplazado el hasta hace poco obsoleto Prelude-NIDS como sistema de detección de intrusiones. Lo que hará será generar logs de todos los ataques o intentos de ataque que se hayan producido, hayan sido fructífieros o no. Es decir, que Snort no es capaz de identificar falsos positivos.

A continuación escribimos en el snort.conf la línea referente a la habilitación de la comunicación de Snort con Prelude.

/etc/snort/snort.conf

```
output alert_prelude: profile=snort sensor_name=snort
                              config=/path/specific-prelude-config.conf
```

Los argumentos anteriormente descritos en snort.conf son opcionales ya que por ejemplo, se toma como profile por defecto "snort".

De manera análoga a lo que se hizo para registrar prelude-lml procedemos para snort y para todos los sensores que queramos utilizar.

Consola del sensor.

```
# prelude-adduser register snort "idmef:w admin:r" 192.168.100.72 --uid 0 --gid 0
```

Obviaremos los mensajes que se muestran por pantalla ya que son muy similares a los del registro de Prelude-LML.

Consola del Servidor de Registro con Prelude-Manager.

```
# prelude-adduser registration-server prelude-manager
```

Volvemos a la consola del sensor Snort para pegar la contraseña generada por el servidor de registro y luego de nuevo a la consola de dicho servidor para asentir (“y”=yes) la operación.

Estamos en disposición de probar la instalación y ejecutar Snort.

```
# snort -c /etc/snort/snort.conf -i eth0
```

Luego añadimos snort al grupo por defecto para que arranque automáticamente la próxima vez que iniciemos:

```
# /etc/init.d/snort start
# rc-update add snort default
```

Fichero de configuración del run-script de Snort:

/etc/conf.d/snort

```
# Config file for /etc/init.d/snort
# This tell snort which interface to listen on (any for every interface)
IFACE="eth0"
```

```
# Make sure this matches your IFACE
PIDFILE="/var/run/snort_$IFACE.pid"

# You probably don't want to change this, but in case you do
LOGDIR="/var/log/snort"

# Probably not this either
CONF="/etc/snort/snort.conf"

# This pulls in the options above
#SNORT_OPTS="-D -u snort -i $IFACE -l $LOGDIR -c $CONF"
SNORT_OPTS="-c $CONF -i $IFACE -D"
```

Con -c especificamos el archivo de configuración, con -i la interfaz y con -D forzamos a que la ejecución sea en background.

6.2.2. Errores Comunes.

6.2.2.1. No se encuentran las reglas de Snort.

```
ERROR: Unable to open rules file:
           /etc/snort/rules/local.rules or /etc/snort//etc/snort/rules/local.rules
```

Se debe lógicamente a que no ha encontrado la ruta de la que leer las reglas que definen los ataques para poder informar generando logs.

Si tenemos Gentoo Linux, basta con copiarlas del portage:

```
# cp /var/tmp/portage/snort-2.3.3/work/snort-2.3.3/rules/*.rules /etc/snort/rules/
```

Si no se encuentran los archivos *.rules, búsquese desde root con el comando find:

```
# find / -name "*.rules"
```

De todos modos, es conveniente regitrarse en la web de Snort y actualizar dichas reglas.

6.2.2.2. Parámetro inválido en snort.conf

```
Log directory = /var/log/snort
ERROR: spo_alert_prelude: Invalid parameter found: 'sensor_name'.
```

Se debe a que en el archivo de configuración /etc/snort/snort.conf hemos definido parámetros que no reconoce nuestra versión de snort. Se soluciona editando dicho archivo, buscamos en él "sensor_name" o la cadena que dé el error y la sustituimos por las opciones por defecto, o mirando en el manual de Snort de nuestra versión cómo se especifica ese parámetro.