PANDORAFMS
ENTERPRISE

Pandora FMS

Manual Administrador

Monitorización con IPTraf

Manual Administrador Monitorización con IPTraf

Índice de contenido

1 Histórico de cambios

Fecha	Autor	Cambio	Versión
10/07/12	Dario	Primera Versión	v1r1

2 Introducción

Con Pandora FMS es posible realizar una monitorización del tráfico de red que resulta del procesamiento realizado por la aplicación **IPTraf**.

A traves de la utilidad de estadísticas de red IPTraf se recogera la actividad de la red en una interfaz determinada (IPTraf tambien nos da la posibilidad de escoger todas las interfaces). Toda la activdad de la red es almacenada en un log.

Un **recolector pasivo** filtra la información basándose en unas reglas establecidas y crea un árbol con la información. Con este árbol, que contiene toda la información de la actividad de red, se generán un archivo XML por cada dirección IP detectada con toda la información de su tráfico de red.

Una vez los archivos XML son procesados por Pandora FMS verá un agente por cada IP detectada y como módulos la información de su tráfico de red asociado.

3 Matriz de compatibilidad

Sistemas donde se ha probado	• IPTraf 1.1.1

Sistemas donde debería funcionar	• IPTraf 1.1.1 y superiores

4 Documentación que debe entregar el Área que requiere la monitorización

Los parámetros necesarios para la monitorización que tiene que proporcionar el área que requiere los servicios de monitorización son:

- Ruta del archivo de log de IPTraf
- Reglas de filtrado para el log (se describen más abajo)

4.1. Reglas de filtrado

Para entender las reglas debemos entender primero la estructura del log que nos generara el IPTraf.

4.1.1. Estructura del log de IPTraf

Un ejemplo de registro del log:

```
Mon Nov 22 15:41:59 2010; TCP; eth0; 52 bytes; from 192.168.50.2:54879 to
91.121.0.208:80; first packet
```

Tras el registro de la fecha y hora de registro, aparece el protocolo, el nombre de la interfaz, el numero de bytes transferidos, la ip y puerto de origen y la ip y puerto de destino de la comunicacion. Después aparecera algo mas de informacion que en este caso es un indicardor de que la comunicacion se trata del primer paquete.

Los datos importantes de este registro de cara al script sera el nombre de la interfaz, el numero de bytes transferidos y las IPs y Puertos de origen y destino.

4.1.2. Reglas de filtrado del recolector

Las reglas tienen la siguiente estructura:

```
[process/discard] [!][ip_src/ip_dst] ip/mask [!][port_src/port_dst] port [!]
[protocol] protocol
```

El **primer parametro** puede ser process si queremos que los registros que coincidan con la regla se introduzcan en el arbol o discard si por el contrario queremos descartar las coincidencias.

El **segundo parametro** indica si la coincidencia debe ser con la ip de origen (ip_src) o de destino (ip_dst). Este parametro puede ir negado con el caracter de exclamacion (!) delante, indicando que queremos los registros que NO coincidan con esa IP.

El **tercer parametro** es una IP seguida de una mascara de red. Si se desea solamente una IP en la regla se podra especificar o bien sin mascara o bien con la mascara 32. Si se especifica otra mascara se consideraran las IPs que esten dentro de dicho rango.

Por ejemplo, 192.168.50.0/24 seran las IPs del rango 192.168.50.1-192.168.50.254. En cambio 192.168.50.23 y 192.168.50.23/32 corresponden de igual manera a la IP 192.168.50.23.

El **cuarto parametro** es parecido al segundo, solamente que en vez de con la IP se especifica si vamos a procesar o descartar (dependiendo de que aparezca o no el simbolo de exclamacion delante) un puerto de origen (port_src) o de destino (port_dst).

El **quinto parametro** es el puerto o conjunto de puertos que la regla hara coincidir.

Se pueden especificar en los siguientes formatos:

- Un solo puerto con tan solo poner dicho numero. Por ejemplo 8080.
- Un intervalo de puertos con un guion como separador. Por ejemplo 21-34 para que evalue los puertos del 21 al 34 ambos incluidos.
- Una enumeracion de modulos separados por comas. Por ejemplo 21,23,80,8080.
- Una combinacion de intervalos y enumeraciones. Por ejemplo 21-34,80,8080,43234-43244.

El **sexto parametro** es el protocolo por el que se realiza la comunicacion. Este parametro puede ir negado con el caracter de exclamacion (!) delante, indicando que queremos los registros que NO coincidan con ese protocolo.

Se pueden especificar en los siguientes formatos:

- Un solo protocolo. Por ejemplo TCP.
- Una enumeración de protocolos. Por ejemolo TCP,UDP,FTP
- Una palabra especial para indicar que se escuchen las transferencias de todos los protocolos. En lugar de los puertos se pone la palabra "all"

4.1.2.1. Ejemplos

Algunos ejemplos validos de reglas serian:

```
discard src_ip 192.168.70.222/32 !port_dst 21-23,80,8080 protocol all
process src_ip 192.168.70.0/24 !port_src 0 !protocol TCP
process src_ip 192.168.80.0/24 !port_dst 80,8080 protocol UDP,TCP
```

La combinacion de estas reglas nos hara que se procesen:

- Todos los registros que tengan como IP origen IPs de la red 192.168.80.X siempre que no tengan como puerto destino ni el 80 ni el 8080 y sean de protocolo TCP o UDP.
- Todos los registros que tengan como IP origen IPs de la red 192.168.70.X independientemente del puerto de origen y que no sean de protocolo TCP excepto los descartados por la primera regla, que seran aquellos registros con la IP 192.168.70.222 de origen cuyo puerto destino sea diferente a los puertos 21,22,23,80 y 8080 independientemente del protocolo.

5 Modulos del plugin

El plugin crea los módulos de forma dinámica en base a las reglas definidas y al tráfico de red analizado por la herramienta IPTraf.

En Pandora FMS aparecerán tantos agentes como IP sean detectatas y los módulos de estos agentes contendran las estadísticas de red para dichas IP.

6 FUNCIONAMIENTO

El *recolector pasivo* es un script llamado **passive.pl**. Este script realiza todo el procesamiento y la creación de los ficheros XML de forma asíncrona por lo que es necesario ejecutarlo cada vez que se requiera introducir o actualizar la información de la monitorización de tráfico en Panodra FMS.

El script debe ejecutarse con permisos de adminsitrador

Antes de ejecutar el proceso es necesario parar el proceso IPTraf. Después de la ejecución del recolector pasivo será necesario borrar el archivo de log consultado y arrancar de nuevo el proceso IPTraf

En la ejecucion se le pasara como parametro la ruta del fichero de configuracion de la siguiente manera:

```
# ./passive.pl /home/usuario/iptraf/passive.collector.conf
```

Los pasos para ejecutar el script serían los siguientes:

1. Parar IPTraf
2. Ejecutar el recolector pasivo
3. Borrar el archivo de log
4. Arrancar IPTraf

Las acciones que ejecuta el script son las siguiente:

1. Se lee el log
2. Se aplican las reglas de descarte
3. Se aplican las reglas de procesado
4. Se construye el arbol
5. Se generan y almacenan los XML en el director data_in de PandoraFMS
6. Termina la ejecución

7 Configuración

Para utilizar el script primero deberemos editar el fichero de configuracion llamado passive.collector.conf y ajustar los parametros deseados. Este fichero dispone de los siguientes ajustes:

- **incomingdir**: Ruta absoluta del directorio data_in de Pandora.
- **interval**: Intervalo en segundos en el que se ejecutara el script. Este parametro no hara que se ejecute cada ese tiempo, sino que servira para que pandora sepa cada cuando se ejecuta y de este modo sepa cuando los modulos creados estan en estado desconocido. El que el script se ejecute cada cierto tiempo se controlara externamente.
- **iface**: Nombre del interfaz donde se escuchara el trafico.
- **min_size**: Se podran filtrar los registros por un tamaño minimo, estando este desactivado por defecto con un valor 0.
- **log_path**: Se establecera la ruta absoluta del fichero de log donde IPTraf ira almacenando los registros del trafico detectado.
- **rules**: Las reglas pueden ser de dos tipos:

1. *discard* : Las reglas de descarte serán ejecutadas en primer lugar y descartarán del filtrado todos aquellos registros que coincidan con ellas.
2. *process* : Las reglas de procesado serán ejecutadas en segundo lugar y decidiran, de los registros restantes tras el descarte, cuales seran incluidos en el arbol y cuales no.

8 Datos generados

Los datos generados por el **recolector pasivo** son archivos XML. Se generan un archivo XML por cada IP detectada y que cumplen las reglas definidas en el archivo de configuración. Estos archivos se copian en la ruta definida en la variable *incomingdir* del archivo de configuración que debe coincidir con el directorio data_in de Pandora FMS.

El contenido de los archivos XML son módulos de Pandora FMS que contienen las estadísticas de red para esa IP. Un ejemplo de archivo puede ser el siguiente:

```
<agent_data interval='300' os_name='Network' os_vesion='4.0.2' version='N/A'
timestamp='AUTO'
address='192.168.70.1' agent_name='IP_192.168.70.1'>
 <module>
  <name>Port_67</name>
  <type>async_data</type>
  <description>Total bytes of port 67</description>
  <interval>300</interval>
  <data>1312</data>
 </module>
 <module>
  <name>Port_67_Protocol_UDP</name>
  <type>async_data</type>
  <description>Total bytes of port 67 for protocol UDP</description>
  <interval>300</interval>
  <data>1312</data>
 </module>
 <module>
  <name>IP_192.168.70.141</name>
  <type>async_data</type>
  <description>Total bytes of IP 192.168.70.141</description>
  <interval>300</interval>
  <data>1312</data>
 </module>
 <module>
  <name>IP_192.168.70.141_Port_67</name>
  <type>async_data</type>
  <description>Total bytes of IP 192.168.70.141 for port 67</description>
  <interval>300</interval>
  <data>1312</data>
 </module>
 <module>
  <name>Protocol_UDP</name>
  <type>async_data</type>
  <description>Total bytes of Protocol UDP</description>
  <interval>300</interval>
  <data>1312</data>
 </module>
</agent_data>
```