Capítulo V
Pruebas

5.1 Introducción

Este capítulo tiene como objetivo mostrar el correcto funcionamiento del software "Listry-AIGC" implementado en la institución en sus dos principales actividades:

- Enfocado hacia el monitoreo de la red interna de la institución.
- Enfocado hacia la detección de malware mediante el plugin "escaneo".

Por cuestiones de integridad y confidencialidad de la información presente en la institución se decidió realizar pruebas con ayuda de un software que genera paquetes en formato Netflow llamado "Paessler Netflow Generator".

5.2 Pruebas

Para la demostración del correcto funcionamiento del software "Listry-AIGC" se simularon dos edificios: En cada edificio trabajan aproximadamente 250 personas. La tabla 5.1 muestra algunas subredes creadas y asignadas a cada edificio para cuestiones de pruebas.

Tabla 5.1 Subredes creadas en el proceso de simulación

Edificio	A		B	
Red	Usuarios	Servidores	Usuarios	Servidores
Subred	172.16.5.0/24	172.16.10.0/28	172.16.6.0/24	172.16.11.0/28

La empresa requiere monitorear la actividad realizada en la red central de los trabajadores debido a que se ha detectado un consumo excesivo en las subredes presentes, sospechando de la presencia de un malware que ha infectado a la red central.

La Figura 5.1 muestra el esquema creado para la realización de las pruebas.

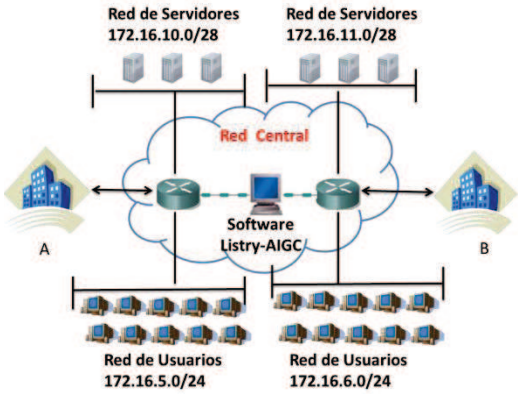


Figura 5.1 Esquema creado para ejemplos

5.2.1 Pruebas enfocadas a monitoreo.

En el capítulo III se mostraron algunas pruebas realizadas en el software Nfsen enfocadas en el monitoreo de red. Por este motivo en esta sección se crearon solamente profiles que observan conexiones realizadas hacia servidores de la siguiente forma:

- Monitorear todo el tráfico que llega de redes de usuarios al servidor de correos del edificio A con IP 172.16.10.3 y del edificio B con IP 172.16.11.6
- Monitorear todo el tráfico que llega al servidor web del edificio A con IP 172.16.10.4 y del edificio B con IP 172.16.11.7

- Monitorear todo el tráfico que llega al servidor de base de datos del edificio A con IP 172.16.10.5 y del edificio B con IP 172.16.11.8

La figura 5.2 muestra la simulación de flujos mediante el software "Paessler Netflow Generetor"

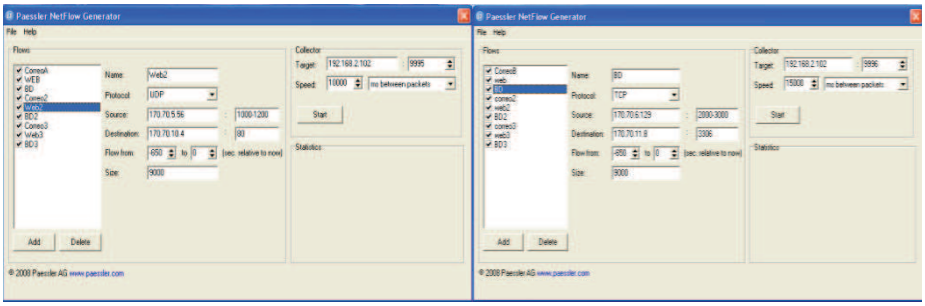


Figura 5.2 Simulación de flujos.

Mediante los flujos creados se está simulando la actividad presente en dos edificios. En la ventana izquierda de la figura se emula el tráfico generado en el edificio A y en la parte derecha el tráfico generado en el edificio B. En ambos edificios se crearon inicialmente nueve flujos; cada uno de ellos emula una conexión realizada hacia el servidor de correo, web o de bases de datos *(B.D.)* respectivamente. En la simulación se varia el puerto origen, el tamaño de los flujos y el tiempo que llevan activos, para tratar de hacer la simulación lo más real posible. En el edificio A inicialmente se enviaban flujos cada 10000 ms (10 S), mientras que en el edificio B se enviaban flujos cada 15000ms (15 S).

La figura 5.3 muestra el comportamiento de los edificios en el profile 'live' correspondiente al periodo 02-Octubre-2010 21:40 al 03 Octubre-2010 00:40.

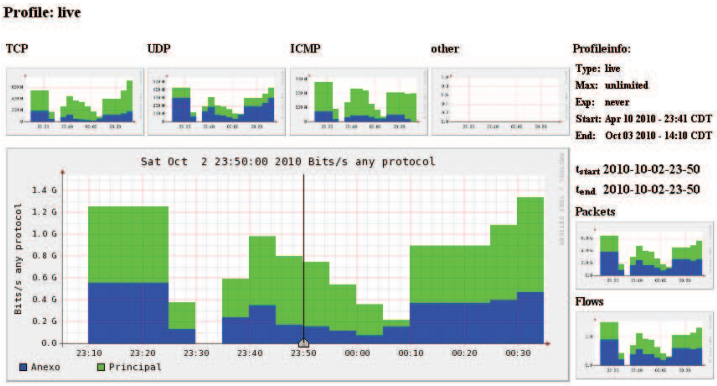


Figura 5.3 Grafica obtenida del profile "live"

Al realizar un análisis sobre esta grafica obtenida no se encuentran grandes variaciones con respecto al tráfico generado en cada edificio. Se observa que el edificio A tiene una mayor actividad que el edificio B. Por este motivo se decidió observar detalladamente un archivo estadísticas *TOPN* en este archivo, se obtuvo la siguiente información:

** nfdump -M /Listry-AIGC/nfsen-1.3.2/profiles-data/live/Principal:Anexo -T -r 2010/10/02/nfcapd.201010022350 -n 20 -s srcip/flows
nfdump filter: any
Top 20 Src IP Addr ordered by flows:

Date first seen	Duration	Proto	Src IP Addr	Flows(%)	Packets(%)	Bytes(%)	pps	bps	bpp
2030-01-27 11:30:48.634	60.000	any	172.16.5.10	19(7.2)	81.3 G(7.2)	311.3 M(1.1)	1.4 G	41.5 M	0
2030-01-27 11:21:48.634	600.000	any	172.16.5.15	19(7.2)	81.3 G(7.2)	311.3 M(1.1)	135.5 M	4.2 M	0

```
2030-01-27 11:20:58.634   650.000 any    172.16.5.56     19( 7.2)  81.3 G( 7.2)   2.8 G(10.1)  125.1 M   34.5 M    0
2030-01-27 11:28:48.634   180.000 any    172.16.5.123    19( 7.2)  81.3 G( 7.2)   1.4 G( 4.9)  451.6 M   60.9 M    0
2030-01-27 11:30:48.634    60.000 any    172.16.5.45     19( 7.2)  81.3 G( 7.2)  778.2 M( 2.8)   1.4 G  103.8 M    0
2030-01-27 11:21:48.634   600.000 any    172.16.5.156    19( 7.2)  81.3 G( 7.2)  336.2 M( 1.2)  135.5 M    4.5 M    0
2030-01-27 11:20:02.634   450.000 any    172.16.6.222    17( 6.4)  72.7 G( 6.4)   2.4 G( 8.7)  161.6 M   43.1 M    0
2030-01-27 11:12:32.634   900.000 any    172.16.6.127    17( 6.4)  72.7 G( 6.4)   1.4 G( 5.1)   80.8 M   12.5 M    0
2030-01-27 11:22:32.634   300.000 any    172.16.6.241    17( 6.4)  72.7 G( 6.4)   4.2 G(15.2)  242.4 M  112.9 M    0
2030-01-27 11:19:12.634   500.000 any    172.16.6.10     17( 6.4)  72.7 G( 6.4)   2.8 G( 9.9)  145.5 M   44.1 M    0
2030-01-27 11:16:42.634   650.000 any    172.16.6.14     17( 6.4)  72.7 G( 6.4)   3.1 G(11.1)  111.9 M   38.2 M    0
2030-01-27 11:16:42.634   650.000 any    172.16.6.129    17( 6.4)  72.7 G( 6.4)   2.5 G( 9.0)  111.9 M   30.9 M    0
2030-01-27 11:22:32.634   300.000 any    172.16.6.159    17( 6.4)  72.7 G( 6.4)   1.4 G( 5.2)  242.4 M   38.6 M    0
2030-01-27 11:20:02.634   450.000 any    172.16.6.234    16( 6.0)  68.5 G( 6.0)   1.5 G( 5.2)  152.1 M   25.9 M    0
2030-01-27 11:25:32.634   120.000 any    172.16.6.141    16( 6.0)  68.5 G( 6.0)   2.6 G( 9.4)  570.4 M  174.8 M    0
Summary: total flows: 265, total bytes: 27.9 G, total packets: 1.1 T, avg bps: 192.9 M, avg pps: 980.7 M, avg bpp: 0
Time window: 2030-01-27 11:12:32 - 2030-01-27 11:31:48
Total flows processed: 265, Blocks skipped: 0, Bytes read: 13836
Sys: 0.012s flows/second: 20389.3   Wall: 0.000s flows/second: 293466.2
```

Analizando estas estadísticas obtenidas no se observa algún valor que consuma el ancho de banda drásticamente, todos los flujos observados contienen valores aceptables (Consumen un tráfico no mayor al 20% del total de BW consumido). Sin embargo, se someterá este mismo lapso de tiempo establecido a un análisis más detallado mediante la creación deprofiles.

El primer profile creado, Monitoreo_redes, pretende observar la cantidad de tráfico que llega a cada servidor en el edificio A o B. La tabla 5.2 muestra los canales creados para este profile y los filtros aplicados a cada uno estos canales. El profile creado es de tipo continuo.

Tabla 5.2 Filtros aplicados para el profile "Monitoreo_redes"

Edificio	Canal	Acción Realizada	Filtro aplicado
A	1	Ver las conexiones que llegan al servidor de correos	src net 172.16.5/24 && dst ip 172.16.10.3 && dst port 25
	3	Ver las conexiones que llegan al servidor web	src net 172.16.5/24 && dst ip 172.16.10.4 && dst port 80
	5	Ver las conexiones que llegan al servidor de BD	src net 172.16.5/24 && dst ip 172.16.10.5 && dst port 3306
B	2	Ver las conexiones que llegan al servidor de correos	src net 172.16.6/24 && dst ip 172.16.11.6 && dst port 25
	4	Ver las conexiones que llegan al servidor web	src net 172.16.6/24 && dst ip 172.16.11.7 && dst port 80
	6	Ver las conexiones que llegan al servidor BD	src net 172.16.6/24 && dst ip 172.16.11.8 && dst port 3306

La figura 5.4 muestra la gráfica obtenida correspondiente al mismo periodo de tiempo indicado en el profile live. Esta gráfica muestra la actividad presente en los dos edificios, la información se ha clasificado mediante los filtros creados en el profile "Monitoreo_redes"

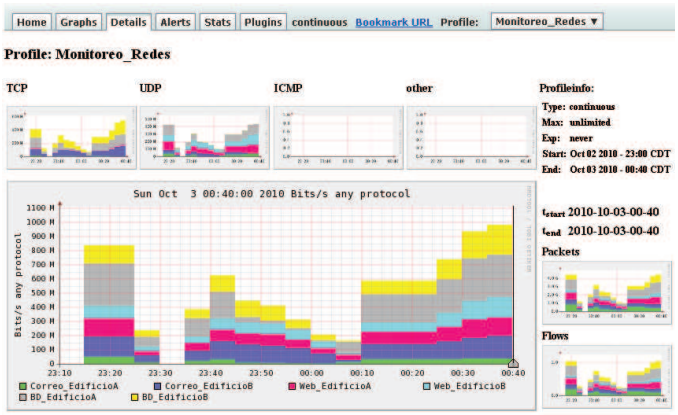


Figura 5.4 Grafica obtenida del profile “Monitoreo_redes”

En esta gráfica se observa que el máximo valor obtenido fue el 3 de octubre del 2010 a las 00:40 correspondiente a conexiones realizadas hacia el servidor de BD del edificio B. Seleccionando el máximo valor obtenido y sometiéndolo a un análisis, se observa que los siguientes flujos han generado este comportamiento:

** nfdump -M /Listry-AIGC/nfsen-1.3.2/profiles-data/Monitoreo_Redes/BD_EdificioB -T -r 2010/10/03/nfcapd.201010030040 -o long -c 20
nfdump filter: -c 6

Date flow start	Duration	Proto	Src IP Addr:Port	Dst IP Addr:Port	Flags	Tos	Packets	Bytes	Flows
2030-01-27 12:59:06.634	650.000	TCP	172.16.6.129:2890	->172.16.11.8:3306	0xff	255	4.3 G	147.4 M	1
2030-01-27 13:02:26.634	450.000	TCP	172.16.6.234:695	->172.16.11.8:3306	0xff	255	4.3 G	91.0 M	1
2030-01-27 12:59:06.634	650.000	TCP	172.16.6.129:2841	->172.16.11.8:3306	0xff	255	4.3 G	147.4 M	1
2030-01-27 13:02:26.634	450.000	TCP	172.16.6.234:630	->172.16.11.8:3306	0xff	255	4.3 G	91.0 M	1
2030-01-27 12:59:06.634	650.000	TCP	172.16.6.129:2900	->172.16.11.8:3306	0xff	255	4.3 G	147.4 M	1
2030-01-27 13:02:26.634	450.000	TCP	172.16.6.234:962	->172.16.11.8:3306	0xff	255	4.3 G	91.0 M	1

Summary: total flows: 6, total bytes: 715.4 M, total packets: 25.7 G, avg bps: 8.8 M, avg pps: 39.5 M, avg bpp: 0
Time window: 2030-01-27 12:59:06 - 2030-01-27 13:09:56
Total flows processed: 68, Blocks skipped: 0, Bytes read: 3564
Sys: 0.020s flows/second: 3238.7 Wall: 0.002s flows/second: 27903.2

Mediante un análisis realizado a esta estadística obtenida, se observa que la dirección IP 172.16.6.129 esta generado una conexión con un tráfico mayor a 100Mb. Analizando esta dirección IP mediante estadísticas top N se observa lo siguiente:

** nfdump -M /Listry-AIGC/nfsen-1.3.2/profiles-data/Monitoreo_Redes/BD_EdificioB -T -r 2010/10/03/nfcapd.201010030040 -n 10 -s srcip/flows
nfdump filter: src ip 172.16.6.129 Top 10 Src IP Addr ordered by flows:

Date first seen	Duration	Proto	Src IP Addr	Flows(%)	Packets(%)	Bytes(%)	pps	bps	bpp
2030-01-27 12:59:06.634	**650.000**	**any**	**172.16.6.129**	**34(100.0)**	**145.5 G(100.0)**	**5.0 G(100.0)**	**223.8 M**	**61.7 M**	**0**

Summary: total flows: 34, total bytes: 5.0 G, total packets: 145.5 G, avg bps: 61.7 M, avg pps: 223.8 M, avg bpp: 0
Time window: 2030-01-27 12:59:06 - 2030-01-27 13:09:56
Total flows processed: 68, Blocks skipped: 0, Bytes read: 3564
Sys: 0.006s flows/second: 9717.1 Wall: 0.000s flows/second: 184782.6

Por medio de las estadisticas Top N se observa que la dirección IP 172.16.6.129 esta generando un mayor tráfico que las demas direcciones pertenecientes al edificio B, sin embargo se observa un comportamiento normal: El plugin escaneo no arrojo algun comportamiento anormal generado en este lapso de tiempo, ademas el valor del tráfico no subió drásticamente.

El profile “puertos_conocidos” tiene el objetivo de clasificar la información de los dos edificios en base al puerto utilizado para su conexión, sin importar si es un puerto origen o puerto destino. La tabla 5.3 muestra la creación de los canales y los filtros aplicados para este profile.

Tabla 5.3 Filtros aplicados para el profile “puertos_conocidos”

Canal	Acción Realizada	Filtro aplicado
1	Ver las conexiones realizadas hacia FTP	port 20 || port 21
2	Ver las conexiones realizadas hacia SSH	port 22
3	Ver las conexiones realizadas hacia TELNET	port 23
4	Ver las conexiones realizadas hacia SMTP	port 25
5	Ver las conexiones realizadas hacia HTTP	port 80
6	Ver las conexiones realizadas hacia SNMP	port 161
7	Ver las conexiones realizadas hacia Netflow	port 9900

La figura 5.5 muestra la aplicación del profile “puertos_conocidos” en el mismo periodo de tiempo indicado en el profile live.

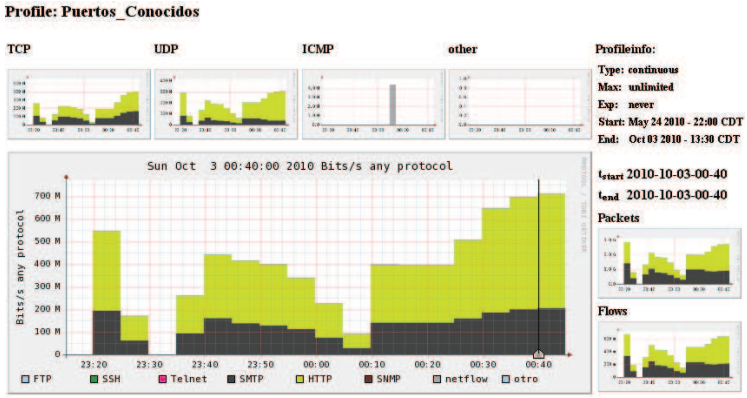


Figura 5.5 Grafica obtenida del profile “puertos_conocidos”

Analizando esta figura se observa que solo se tienen conexiones en el puerto 25 y 80 (en este profile no se creó un canal que este monitoreando la actividad generada por el servidor de B.D.); se observa que el servidor web está generando un mayor tráfico que el servidor de correos. Por medio de un análisis mediante estadísticas topN se observa lo siguiente:

```
** nfdump -M /Listry-AIGC/nfsen-1.3.2/profiles-data/Puertos_Conocidos/otro:netflow:SNMP:HTTP:SMTP:Telnet:SSH:FTP  -T  -r
2010/10/03/nfcapd.201010030035 -n 10 -s srcip/flows
nfdump filter: any
Top 10 Src IP Addr ordered by flows:
Date first seen             Duration Proto    Src IP Addr   Flows(%)     Packets(%)     Bytes(%)       pps    bps  bpp
2030-01-27 13:01:36.634   500.000 any      172.16.6.10    33(17.5)  141.2 G(17.5)   5.4 G(20.6)  282.4 M  85.6 M    0
2030-01-27 12:59:06.634   650.000 any      172.16.6.14    33(17.5)  141.2 G(17.5)   6.0 G(23.2)  217.2 M  74.2 M    0
2030-01-27 13:04:56.634   300.000 any      172.16.6.241   33(17.5)  141.2 G(17.5)   8.2 G(31.6)  470.6 M  219.1 M   0
2030-01-27 11:17:32.634   600.000 any      172.16.5.15    30(15.9)  128.3 G(15.9)  491.5 M( 1.9)  213.9 M   6.6 M    0
2030-01-27 11:22:32.634   300.000 any      172.16.5.12    30(15.9)  128.3 G(15.9)   1.5 G( 5.7)  427.8 M   39.3 M   0
2030-01-27 11:16:42.634   650.000 any      172.16.5.56    30(15.9)  128.3 G(15.9)   4.4 G(17.0)  197.5 M   54.4 M   0
Summary: total flows: 189, total bytes: 26.0 G, total packets: 808.6 G, avg bps: 30.6 M, avg pps: 119.0 M, avg bpp: 0
Time window: 2030-01-27 11:16:42 - 2030-01-27 13:09:56
Total flows processed: 189, Blocks skipped: 0, Bytes read: 10052
Sys: 0.005s flows/second: 31505.3   Wall: 0.000s flows/second: 353932.6
```

Analizando las estadísticas generadas se observa un tráfico normal en los servidores web y de correo, no se detecta un comportamiento anormal presente en estos servidores.

El ultimo profile creado, puertos, tiene el objetivo de monitorear las conexiones realizadas hacia puertos bien conocidos, registrados/dinámicos o privados sin importar si esta conexión fue realizada en un puerto origen o un puerto destino. La tabla 5.4 muestra los filtros creados en este profile.

Tabla 5.4 Filtros aplicados para el profile “puertos”

Canal	Acción Realizada	Filtro aplicado
1	Ver las conexiones realizadas por puertos altos (Dinámicos o privados)	port > 41151 && port < 65535
2	Ver las conexiones realizadas por puertos registrados	port > 1023 && port < 41152
3	Ver las conexiones realizadas por puertos bien conocidos	port > 0 && port < 1024

La figura 5.6 muestra la aplicación del profile “puertos” en el mismo periodo de tiempo indicado en el profile live.

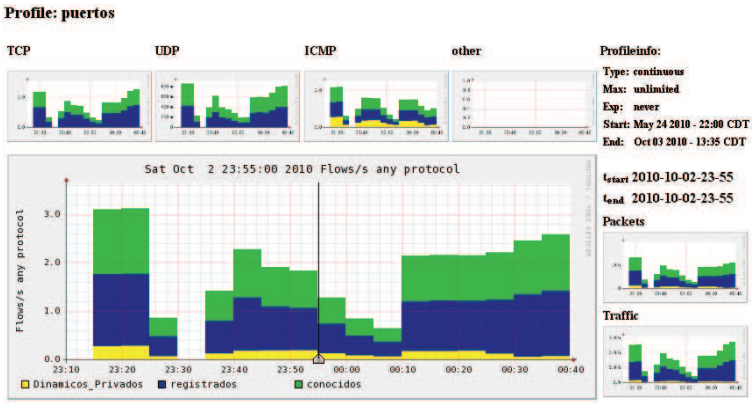


Figura 5.6 Grafica obtenida del profile “puertos_conocidos”

Analizando esta gráfica, se observa que se tienen mayores conexiones realizadas en puertos bien conocidos (en estos puertos opera el servidor de correos y el servidor web). Además se observan conexiones realizadas en puertos altos porque en el software “Paessler Netflow Generator” se simularon algunos puertos orígenes altos. Analizando un archivo nfcapd aleatorio por medio de estadísticas TopN se observa lo siguiente.

```
** nfdump -M /Listry-AIGC/nfsen-1.3.2/profiles-data/puertos/conocidos:registrados:Dinamicos_Privados -T -r
2010/10/02/nfcapd.201010022320 -n 10 -s srcip/flows
nfdump filter: any
Top 10 Src IP Addr ordered by flows:
Date first seen        Duration Proto      Src IP Addr   Flows(%)     Packets(%)      Bytes(%)        pps     bps  bpp
2030-01-27 11:21:48.634   600.000 any     172.16.5.156     90( 9.6)  385.0 G( 9.6)   1.6 G( 1.7)  641.7 M   21.2 M    0
2030-01-27 11:28:48.634   180.000 any     172.16.5.123     90( 9.6)  385.0 G( 9.6)   6.5 G( 6.8)   2.1 G  288.3 M    0
2030-01-27 11:26:48.634   300.000 any     172.16.5.12      60( 6.4)  256.7 G( 6.4)   2.9 G( 3.1)  855.6 M   78.6 M    0
2030-01-27 11:21:08.634   640.000 any     172.16.5.157     60( 6.4)  256.7 G( 6.4)   9.6 G(10.1)  401.1 M  120.4 M    0
2030-01-27 11:29:18.634   150.000 any     172.16.5.78      60( 6.4)  256.7 G( 6.4)  10.3 G(10.8)   1.7 G  550.5 M    0
2030-01-27 11:21:48.634   600.000 any     172.16.5.15      60( 6.4)  256.7 G( 6.4)  983.0 M( 1.0)  427.8 M   13.1 M    0
2030-01-27 11:30:48.634    60.000 any     172.16.5.10      59( 6.3)  252.4 G( 6.3)  966.6 M( 1.0)   4.2 G  128.9 M    0
2030-01-27 11:20:58.634   650.000 any     172.16.5.56      58( 6.2)  248.1 G( 6.2)   8.6 G( 8.9)  381.7 M  105.3 M    0
2030-01-27 11:25:32.634   120.000 any     172.16.6.141     52( 5.6)  222.5 G( 5.6)   8.5 G( 8.9)   1.9 G  567.9 M    0
2030-01-27 11:20:02.634   450.000 any     172.16.6.222     47( 5.0)  201.1 G( 5.0)   6.7 G( 7.0)  446.8 M  119.2 M    0
Summary: total flows: 935, total bytes: 95.6 G, total packets: 4.0 T, avg bps: 661.9 M, avg pps: 3.5 G, avg bpp: 0
Time window: 2030-01-27 11:12:32 - 2030-01-27 11:31:48
Total flows processed: 935, Blocks skipped: 0, Bytes read: 48704
Sys: 0.013s flows/second: 66800.0    Wall: 0.001s flows/second: 745019.9
```

En este archivo se observa que la subred 172.16.5.0/24 genera mayores conexiones hacia puertos conocidos que las demás subredes, este dato corresponde satisfactoriamente a la información mostrada en el profile live donde se observó que el edificio A tiene una mayor actividad que el edificio B.

Con los profiles creados se cumple con el objetivo de mostrar el software Nfsen enfocado en el monitoreo de red. Cabe destacar que se pueden crear profiles de acuerdo a las necesidades requeridas y por medio de los filtros creados en los profiles se pueden realizar análisis muy detallados.

5.2.2 Pruebas enfocadas en la detección de malware.

El objetivo de esta sección es mostrar el funcionamiento del plugin escaneo. En las pruebas anteriores se mostró el software Nfsen enfocado hacia el monitoreo de red y se simulo tráfico normal en el lapso de tiempo 02-Octubre-2010 21:40 al 03 Octubre-2010 00:40. Observando el plugin escaneo en un lapso de tiempo 2010-10-03 00:05 perteneciente al rango establecido se observa un tráfico normal sin presencia de anomalías delectadas, tal y como se analizó en los profiles creados. El resultado de la ejecución del plugin escaneo en este lapso de tiempo se observa en la figura 5.7.

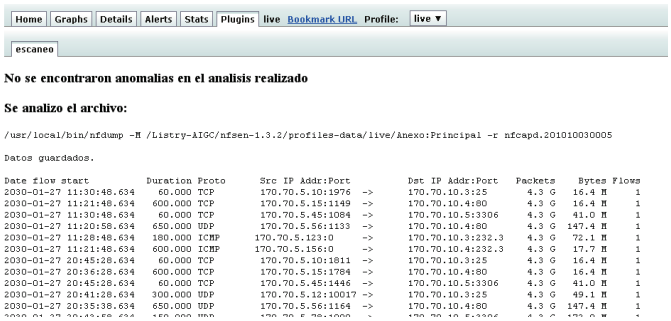


Figura 5.7 Comportamiento del plugin escaneo con tráfico normal

La figura 5.8 muestra el esquema utilizado en la realización de pruebas enfocadas en la detección de malware.

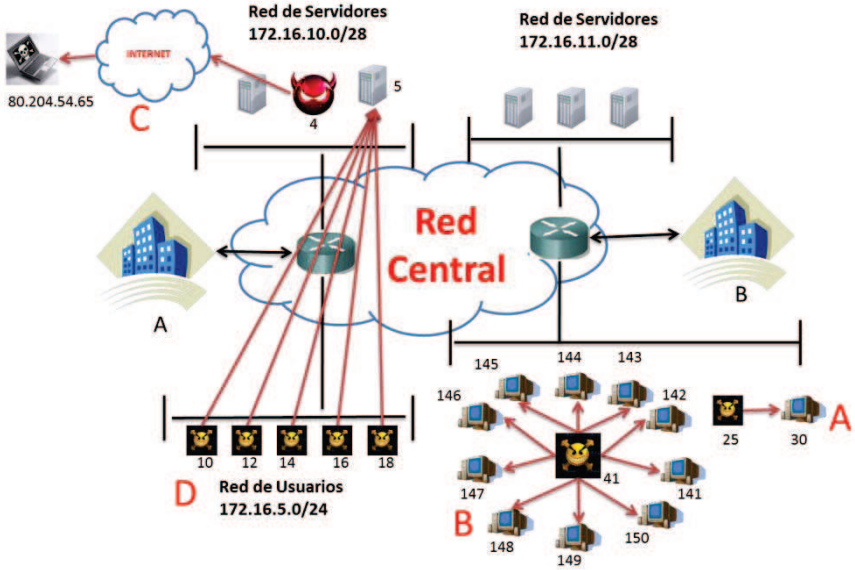


Figura 5.8 Esquema de pruebas realizadas simulando malware

En esta imagen se han simulado cuatro escenarios: cada escenario está representado por una letra y simula un comportamiento típico de algún malware. A continuación se describirá cada uno de ellos y se ejecutará el plugin 'escaneo' con el objetivo de observar los resultados que arroja el plugin.

5.2.2.1 Escenario A

En el escenario A se está simulando a una computadora infectada por el malware “blasser” con dirección IP 172.16.6.25. Este malware tratará de explotar la misma vulnerabilidad que encontró en el equipo “victima” para infectar mediante un escaneo de puertos a una computadora con dirección IP 172.16.6.30. Ambas computadoras se encuentran en la subred 172.16.6.0/24 perteneciente al edificio B. Simulado con ayuda del software “Paessles Netflow Generator” este comportamiento anormal y realizando un análisis con ayuda del plugin escaneo se detectó lo siguiente:

Figura 5.9 Escaneo de puertos encontrado

Como se observa en la figura 5.9 el plugin ‘escaneo’ ha detectado un escaneo de puertos realizado de forma secuencial en puertos altos el rango del 20000 al 20010. Además se observa que se ha notificado vía email sobre la anomalía y se ha creado un registro en la tabla ‘epuertos’ de esta anomalía detectada. La figura 5.10 muestra el uso del software OpenWebmail para visualizar los mensajes recibidos.

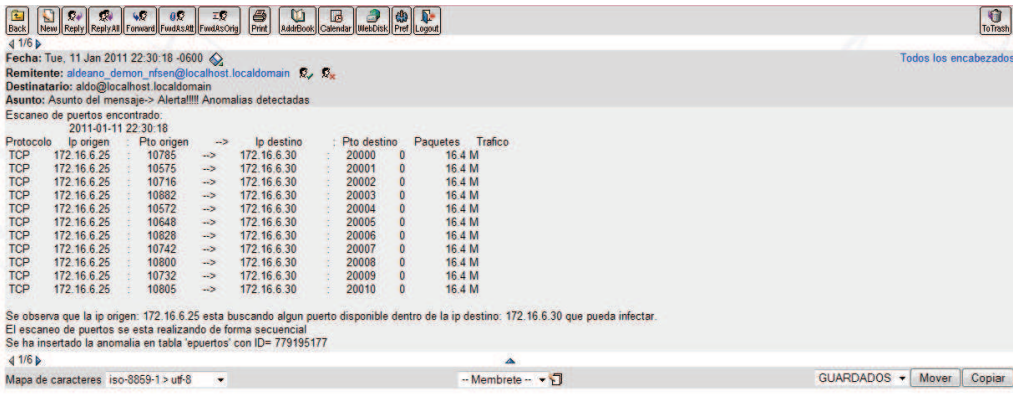


Figura 5.10 Notificación del escaneo de puertos encontrado

En la figura 5.11, mediante el uso del software Navicat, se observa que se ha creado un registro de la anomalía detectada en la tabla ‘epuertos’ con el ID ‘779195177’.

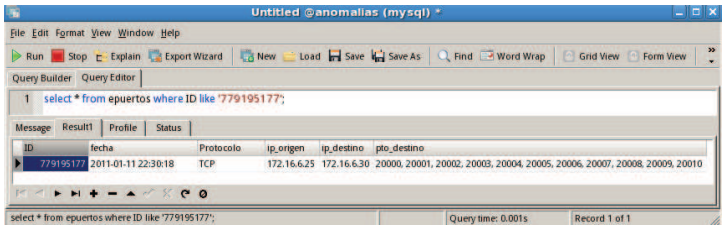


Figura 5.11 Registro de la anomalía guardado en la tabla 'epuertos'

5.2.2.2 Escenario B

En el escenario B se está simulando a una computadora infectada por el malware "conficker" con dirección IP 172.16.6.41. Este malware tratará de explotar la misma vulnerabilidad que encontró en el equipo "victima" para infectar mediante un escaneo de Ip'S a alguna computadora que se encuentre en el rango de direcciones Ip'S 172.16.6.141 al 172.16.6.150, perteneciente a la subred 172.16.6.0/24 creada en el edificio B. Simulado con ayuda del software "Paeesless Netflow Generator" este comportamiento anormal y realizando un análisis con ayuda del plugin escaneo se detectó lo siguiente:

Figura 5.12 Escaneo de IPS encontrado

Como se observa en la figura 5.12 el plugin 'escaneo' detecto un escaneo de IPS realizado de forma secuencial por la dirección IP origen 172.16.6.41 hacia un rango de direcciones IP destino 172.16.6.141 a 172.16.6.150 en el puerto destino 8060. Además se observa que se ha notificado vía email sobre la anomalía y se ha creado un registro en la tabla 'eips' de esta anomalía detectada. La figura 5.13 muestra el mensaje recibido.

Figura 5.13 Notificación del escaneo de puertos encontrado

En la figura 5.14 se observa que se ha creado un registro de la anomalía detectada en la tabla 'eips' con el ID '97452838'

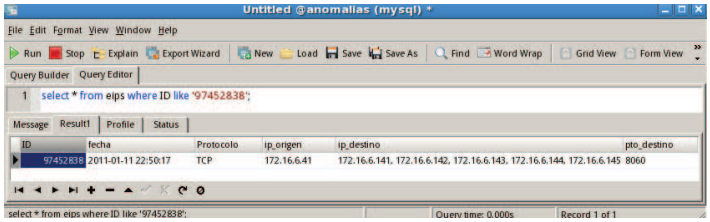


Figura 5.14 Registro de la anomalía guardado en la tabla 'epuertos'

5.2.2.3 Escenario C

En el escenario C se está simulando a un servidor web infectado por el malware "nspaint.exe". Este malware tratará de descargar a más malware y comprometer aún más al servidor web infectado con dirección IP 172.16.10.4. Adicionalmente el servidor infectado está enviando información hacia una computadora externa a la red de la institución con dirección IP 80.204.54.65 (IP asociada al creador del malware). Simulado con ayuda del software "Paessless Netflow Generator" este comportamiento anormal y realizando un análisis con ayuda del plugin escaneo se detectó lo siguiente:

Figura 5.15 Fuga de información encontrada

Como se observa en la figura 5.15 el plugin ‘escaneo’ ha detectado una fuga de información del servidor de correo del edificio A con dirección IP 172.16.10.4, utilizando puertos orígenes secuenciales para él envió de información. Hay que resaltar que el plugin 'escaneo' detecte este tipo de comportamiento, la máquina infectada tendrá que enviar información con un tráfico mayor a 5MB y utilizar puertos origen de manera secuencial. Además se observa que se ha notificado vía email sobre la anomalía y se ha creado un registro en la tabla ‘exterior’ de esta anomalía detectada. La figura 5.16 muestra el mensaje recibido.

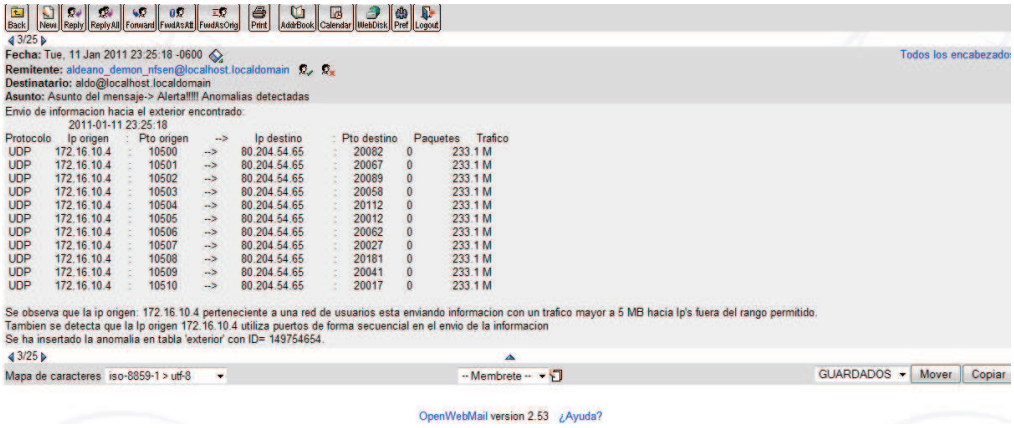


Figura 5.16 Notificación de la fuga de información encontrada

En la figura 5.17 se observa que se ha creado un registro de la anomalía detectada en la tabla ‘exterior’ con el ID ‘149754654’

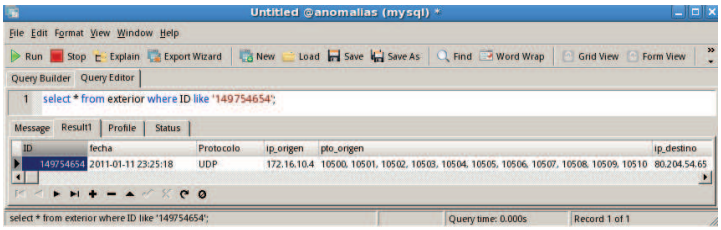
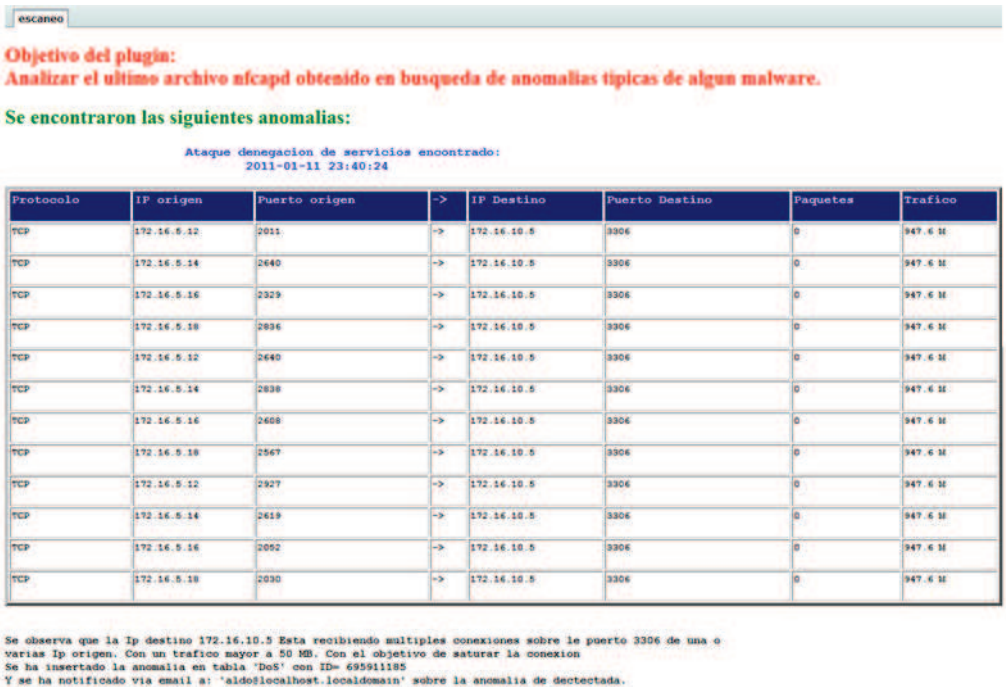


Figura 5.17 Registro de la anomalía guardado en la tabla ‘exterior’

5.2.2.4 Escenario D

En el escenario D se está simulando a un conjunto de computadoras, pertenecientes al rango de direcciones IP 172.16.5.10 al 172.16.5.18 del edificio A, que han sido infectadas por un malware “Postal.exe”. Este malware causa que las víctimas actúen como máquinas “zombies” y estén enviando múltiples peticiones hacia el servidor de bases de datos con dirección IP 172.16.10.5. El malware realiza esta acción con el objetivo de saturar o tirar al servidor. Simulado con ayuda del software “Paessless Netflow Generator” este comportamiento anormal y realizando un análisis con ayuda del plugin escaneo se detectó lo siguiente:



escaneo

Objetivo del plugin:
Analizar el ultimo archivo nfcapd obtenido en busqueda de anomalias tipicas de algun malware.

Se encontraron las siguientes anomalias:

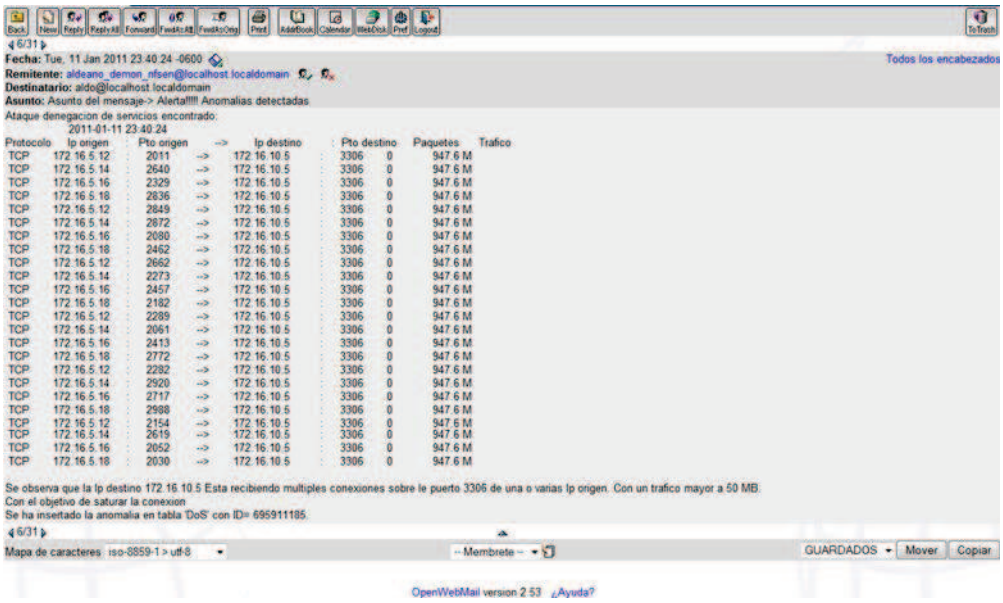
Ataque denegacion de servicios encontrado:
2011-01-11 23:40:24

Protocolo	IP origen	Puerto origen	->	IP Destino	Puerto Destino	Paquetes	Trafico
TCP	172.16.5.12	2011	->	172.16.10.5	3306	0	947.6 M
TCP	172.16.5.14	2640	->	172.16.10.5	3306	0	947.6 M
TCP	172.16.5.16	2329	->	172.16.10.5	3306	0	947.6 M
TCP	172.16.5.18	2836	->	172.16.10.5	3306	0	947.6 M
TCP	172.16.5.12	2640	->	172.16.10.5	3306	0	947.6 M
TCP	172.16.5.14	2838	->	172.16.10.5	3306	0	947.6 M
TCP	172.16.5.16	2688	->	172.16.10.5	3306	0	947.6 M
TCP	172.16.5.18	2567	->	172.16.10.5	3306	0	947.6 M
TCP	172.16.5.12	2927	->	172.16.10.5	3306	0	947.6 M
TCP	172.16.5.14	2619	->	172.16.10.5	3306	0	947.6 M
TCP	172.16.5.16	2052	->	172.16.10.5	3306	0	947.6 M
TCP	172.16.5.18	2030	->	172.16.10.5	3306	0	947.6 M

Se observa que la Ip destino 172.16.10.5 Esta recibiendo multiples conexiones sobre le puerto 3306 de una o varias Ip origen. Con un trafico mayor a 50 MB. Con el objetivo de saturar la conexion
Se ha insertado la anomalia en tabla 'DoS' con ID= 695911185
Y se ha notificado via email a: 'aldo@localhost.localdomain' sobre la anomalia de dectectada.

Figura 5.18 Ataque de negación de servicios encontrado

Como se observa en la figura 5.18 el plugin 'escaneo' ha detectado a múltiples maquinas zombies que están realizando conexiones hacia el servidor de base de datos con dirección IP 172.16.10.5. Además todas las conexiones realizadas generan un tráfico anormal al que se tiene habitualmente en la institución. La figura 5.19 muestra la notificación recibida de esta anomalía que se detectó.



Back New Reply ReplyAll Forward FwdAsAtt FwdAsOrig Print AddrBook Calendar WebDisk Pref Logout ToTrash

6/31

Fecha: Tue, 11 Jan 2011 23:40:24 -0600 Todos los encabezados
Remitente: aldeano_demon_nfsen@localhost.localdomain
Destinatario: aldo@localhost.localdomain
Asunto: Asunto del mensaje-> Alerta!!!!! Anomalias detectadas

Ataque denegacion de servicios encontrado:
2011-01-11 23:40:24

Protocolo	Ip origen	Pto origen	-->	Ip destino	Pto destino	Paquetes	Trafico
TCP	172.16.5.12	2011	-->	172.16.10.5	3306	0	947.6 M
TCP	172.16.5.14	2640	-->	172.16.10.5	3306	0	947.6 M
TCP	172.16.5.16	2329	-->	172.16.10.5	3306	0	947.6 M
TCP	172.16.5.18	2836	-->	172.16.10.5	3306	0	947.6 M
TCP	172.16.5.12	2849	-->	172.16.10.5	3306	0	947.6 M
TCP	172.16.5.14	2872	-->	172.16.10.5	3306	0	947.6 M
TCP	172.16.5.16	2080	-->	172.16.10.5	3306	0	947.6 M
TCP	172.16.5.18	2462	-->	172.16.10.5	3306	0	947.6 M
TCP	172.16.5.12	2662	-->	172.16.10.5	3306	0	947.6 M
TCP	172.16.5.14	2273	-->	172.16.10.5	3306	0	947.6 M
TCP	172.16.5.16	2457	-->	172.16.10.5	3306	0	947.6 M
TCP	172.16.5.18	2182	-->	172.16.10.5	3306	0	947.6 M
TCP	172.16.5.12	2289	-->	172.16.10.5	3306	0	947.6 M
TCP	172.16.5.14	2061	-->	172.16.10.5	3306	0	947.6 M
TCP	172.16.5.16	2413	-->	172.16.10.5	3306	0	947.6 M
TCP	172.16.5.18	2772	-->	172.16.10.5	3306	0	947.6 M
TCP	172.16.5.12	2282	-->	172.16.10.5	3306	0	947.6 M
TCP	172.16.5.14	2920	-->	172.16.10.5	3306	0	947.6 M
TCP	172.16.5.16	2717	-->	172.16.10.5	3306	0	947.6 M
TCP	172.16.5.18	2988	-->	172.16.10.5	3306	0	947.6 M
TCP	172.16.5.12	2154	-->	172.16.10.5	3306	0	947.6 M
TCP	172.16.5.14	2619	-->	172.16.10.5	3306	0	947.6 M
TCP	172.16.5.16	2052	-->	172.16.10.5	3306	0	947.6 M
TCP	172.16.5.18	2030	-->	172.16.10.5	3306	0	947.6 M

Se observa que la Ip destino 172.16.10.5 Esta recibiendo multiples conexiones sobre le puerto 3306 de una o varias Ip origen. Con un trafico mayor a 50 MB.
Con el objetivo de saturar la conexion
Se ha insertado la anomalia en tabla 'DoS' con ID= 695911185.

6/31

Mapa de caracteres: iso-8859-1 > utf-8 -- Membrete -- GUARDADOS Mover Copiar

OpenWebMail version 2.53 ¿Ayuda?

Figura 5.19 Notificación de la fuga de información encontrada

En la figura 5.20 se observa que se ha creado un registro de la anomalía detectada en la tabla 'exterior' con el ID '695911185'

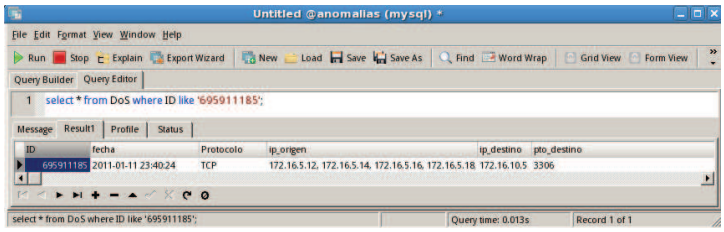


Figura 5.20 Registro de la anomalía guardado en la tabla 'DoS'

En estos ejemplos creados se decidió mostrar al plugin escaneo enfocado en la detección, de forma individual, de cada técnica implementada para detectar malware presente en la red central de la institución, Esto se realizó con el objetivo de poder hacer un análisis detallado en cada ejemplo creado y mostrar los resultados de la ejecución del plugin escaneo. Hay que señalar que este plugin es capaz de detectar las 4 técnicas implementadas de detección de malware de forma simultánea.

Con estos ejemplos creados se cumple con el objetivo de mostrar al software "Listry-AIGC" enfocado, mediante el plugin escaneo, en la detección de malware basado en patrones típicos de comportamiento.