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.

Tak	ola 5.1 Su	Subredes creadas en el proceso de simulación							
Edificio		Α	В						
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.



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"

Paessler NetFlow Gen				2	Paessler NetFlow Generator		
Heb Flows ✓ Coneck ✓ WEB ✓ SB ✓ Coneck ✓ Urbs ✓ Coneck ✓ Vorb ✓ Coneck ✓ Vorb ✓ Coneck ✓ Vorb ✓ SB ✓	Name Piolocal Source Destination Flow from Size	[web2 [UDP [170,70,5 56 [170,70,10,4 [650 €] to [0 [9000]	▼ : [1000.1200 : [0] : [0] (loc: relative to now)	Colecter Tager 112:192.702 1995 S Speet 11000 S m benergastes • Statistics	Re Neb Fors ✓ const ✓ const	80 100 mm 100 mm 1000 mm 1000 mm 1000 mm 1000 mm 1000 mm 1000 mm 1000 mm	Column 996 Tage: 911102.1102 996 Spect 5000 1 mb three patient Spect Spect 5000 1 mb three patient
Add Delete	siler.com				Add Delete		

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.



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 <u>172.16.5.10</u> 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 <u>172.16.5.15</u> 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) 7	778.2 M(2.8)	1.4 G 1	.03.8 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	2) 135.5 M	VI 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 packet	s: 1.1 T, av	vg bps: 192.9	M, avg pps: 9	980.7 M, a	avg bpp: 0	
Time window: 2030-01-27	11:12:32 - 2030	-01-27 11:31:48						
Total flows processed: 26	5, Blocks skipped	: 0, Bytes read: 1	3836					

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.

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

 Tabla 5.2
 Filtros aplicados para el profile "Monitoreo_redes"

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 <u>172.16.6.129:2890</u> -><u>172.16.11.8:3306</u> 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 <u>172.16.6.129:2841</u> -><u>172.16.11.8:3306</u> 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 <u>172.16.6.129:2900</u> -><u>172.16.11.8:3306</u> 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 <u>172.16.6.129</u> 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.

la	bla 5.3 Filtros aplicados para el profile "puer	rtos_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.



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-Al0	GC/nfsen-1.3.2/p	rofiles-data/Pu	ertos_Con	ocidos/otro:ne	etflow:SNMP:	HTTP:SM	TP:Telnet:	SSH:FTP -T -r
2010/10/03/nfcapd.2010)10030035 -n 10	-s srcip/flows						
nfdump filter: any								
Top 10 Src IP Addr order	ed 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: 18	9, total bytes: 26	.0 G, total pacl	kets: 808.6	G, avg bps: 30).6 M, avg pps	: 119.0 N	I, avg bpp:	0
Time window: 2030-01-2	7 11:16:42 - 203	0-01-27 13:09:	56					
Total flows processed: 18	39, Blocks skippe	d: 0, Bytes read	d: 10052					
Svs: 0.005s flows/second	: 31505.3 Wall:	0.000s flows/	second: 35	3932.6				

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.



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:
                                   Src IP Addr Flows(%) Packets(%)
Date first seen
                  Duration Proto
                                                                       Bytes(%)
                                                                                           bps bpp
                                                                                    pps
2030-01-27 11:21:48.634 600.000 any
                                                      90(9.6) 385.0 G(9.6) 1.6 G(1.7) 641.7 M 21.2 M
                                                                                                       0
                                      172.16.5.156
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
                                                     60(6.4) 256.7 G(6.4) 2.9 G(3.1) 855.6 M 78.6 M
2030-01-27 11:26:48.634 300.000 any
                                      172.16.5.12
                                                                                                       0
                                      <u>172.16.5.157</u> 60( 6.4) 256.7 G( 6.4) 9.6 G(10.1) 401.1 M 120.4 M 0
2030-01-27 11:21:08.634 640.000 any
2030-01-27 11:29:18.634 150.000 anv
                                                    60( 6.4) 256.7 G( 6.4) 10.3 G(10.8) 1.7 G 550.5 M 0
                                      172.16.5.78
2030-01-27 11:21:48.634 600.000 any
                                                     60(6.4) 256.7 G(6.4) 983.0 M(1.0) 427.8 M 13.1 M 0
                                      172.16.5.15
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
                                                      52(5.6) 222.5 G(5.6) 8.5 G(8.9) 1.9 G 567.9 M 0
                                      172.16.6.141
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.

Home Graphs Details	Alerts Stats Plu	gins live <u>Bookmark URL</u>	Profile:	live v				
escaneo								
No se encontraron and	omalias en el anali	sis realizado						
Se analizo el archivo:								
/usr/local/bin/nfdump -	-H /Listry-AIGC/nfs	en-1.3.2/profiles-dat	/live/	Anexo:Principal -r n	fcapd.201	010030005		
Datos guardados.								
Date flow start	Duration Proto	Src IP Addr:Port		Dst IP Addr:Port	Packets	Bytes	Flows	
2030-01-27 11:30:48.634	60.000 TCP	170.70.5.10:1976	->	170.70.10.3:25	4.3 G	16.4 M	1	
2030-01-27 11:21:48.634	600.000 TCP	170.70.5.15:1149	->	170.70.10.4:80	4.3 G	16.4 H	1	
2030-01-27 11:30:48.63	60.000 TCP	170.70.5.45:1084	->	170.70.10.5:3306	4.3 G	41.0 M	1	
2030-01-27 11:20:58.634	650.000 UDP	170.70.5.56:1133	->	170.70.10.4:80	4.3 G	147.4 H	1	
2030-01-27 11:28:48.634	180.000 ICMP	170.70.5.123:0	->	170.70.10.3:232.3	4.3 G	72.1 H	1	
2030-01-27 11:21:48.634	600.000 ICMP	170.70.5.156:0	->	170.70.10.4:232.3	4.3 G	17.7 H	1	
2030-01-27 20:45:28.634	60.000 TCP	170.70.5.10:1811	->	170.70.10.3:25	4.3 G	16.4 H	1	
2030-01-27 20:36:28.634	600.000 TCP	170.70.5.15:1784	->	170.70.10.4:80	4.3 G	16.4 M	1	
2030-01-27 20:45:28.634	60.000 TCP	170.70.5.45:1446	->	170.70.10.5:3306	4.3 G	41.0 H	1	
2030-01-27 20:41:28.634	300.000 UDP	170.70.5.12:10017	->	170.70.10.3:25	4.3 G	49.1 M	1	
2030-01-27 20:35:38.634	1 650.000 UDP	170.70.5.56:1164	->	170.70.10.4:80	4.3 G	147.4 H	1	
Figura 5.7	Сог	nportamient	o de	el plugin esc	aneo	con t	ráfico	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:

demoplugin Objetivo malizar	escaneo del plugin: el ultimo archivo	nfcand obtenido en	besou	eda de anomal	ias tinicas de aleun n	alware.	
e encont	raron las siguien	ntes anomalias: 2011-01-11 22-30-10	601				
herrisse] e	10 neigen	Parata artists	2	10 Destine	Parto Sestino	Preparine	Transferre
TCP	172.16.6.25	10785	->	172.16.6.30	20000	o	16.4 M
TCP	172.16.6.25	10575	->	172.16.6.30	20001	0	26.4 10
TCP	172.16.6.25	10716	->	172.16.6.30	20602	0	16.4 10
TCP	172.16.6.25	10882	->	172.16.6.30	20003	o	16.4 M
TCP	172.16.6.25	10572	->	172.16.6.30	20004	0	26.4.11
TCP	172.16.6.25	10648	->	172 . 16 . 6 . 30	20085	0	16.4 M
TCP	172.16.4.26	10826	->	172.16.6.30	20004	0	16.4 18
TCP	172 .16 .6 .25	10742	->	172.16.6.30	20007	0	16.4 12
TCP	172.16.6.25	10800	->	172.16.6.30	20008	0	16.4 H
ICP	172.16.6.25	10732	->	172.16.6.30	20089	0	26.4 11
TCP	172.16.6.25	10805	->	172.16.6.30	20010	0	16.4 M

01 172.16.6.30 sta realizando de forma ' con ID= 779195177 L localdomato' con

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.

Back N	lew Reply ReplyA	Fo	Ward FwdAsAtt	FundAsOr	rig Print AddrBool	k Cale	andar WebDisl	Pref	Logout	ToTrash
Feebar	Tuo 11 lan 20	11 1	22-20-19 060							Todas los ancabazados
Pecha:	rue, 11 Jan 20	11.2	2.30.10-000	10 2						Todos los encadezados
Remite	tosiou oldo@lou	enno	m_nisen@io	camost.	localdomain Ny	XXX				
Acuntor	Acusto del mo	-ain	is > Alastall		alian datactadan					
Asunto.	Asunto del me	1130	ije-> Alenaini	Allotta	allas uelectadas					
Escane	2011.01.1	1.21	2:30:18							
Protoco	la la origen	1.2.	Pto origen		In destino		Pto desti	00	Partietes Trafico	
TCP	172 16 6 25		10785		172 16 6 30		20000	0	16 d M	
TCP	172 16 6 25		10575	>	172 16 6 30		20001	Ő	16.4 M	
TCP	172.16.6.25		10716	>	172.16.6.30		20002	ō	16.4 M	
TCP	172.16.6.25		10882	->	172.16.6.30		20003	0	16.4 M	
TCP	172.16.6.25		10572	->	172.16.6.30		20004	0	16.4 M	
TCP	172.16.6.25		10648	->	172.16.6.30		20005	0	16.4 M	
TCP	172.16.6.25		10828	>	172.16.6.30		20006	0	16.4 M	
TCP	172.16.6.25		10742	>	172.16.6.30		20007	0	16.4 M	
TCP	172.16.6.25		10800	>	172.16.6.30		20008	0	16.4 M	
TCP	172.16.6.25		10732	>	172.16.6.30		20009	0	16.4 M	
TCP	172.16.6.25		10805	>	172.16.6.30		20010	0	16.4 M	
Se obse El escar Se ha in	rva que la ip or neo de puertos sertado la anor	igen se e nali	esta realizan a en tabla 'ej	5 esta b do de fo puertos'	ouscando algun p orma secuencial con ID= 779195	iuerto 177	disponible	e den	ro de la ip destino: 172.16.6.30 que pueda infectar.	
4 1/6 .									A	
Mapa de	caracteres is	0-8	859-1 > utf-8	•					Membrete 💌 🕤	GUARDADOS + Mover Copiar

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'.

<u>.</u>		Untitled @	anomalia	ıs (mysql)		
File Edit Format View Window Help						
🕨 Run 📕 Stop 🔚 Explain 📑 Expe	ort Wizard	New 📄 Loan	d 🖬 Save	Save As	🔍 Find 📑 Word Wrap	Grid View 💽 Form View
Query Builder Query Editor						
1 select * from epuertos where	ID like '77919	5177;				
Message Result1 Profile Status	1					
ID fecha	Protocolo	ip_origen	ip_destino	pto_destino		
779195177 2011-01-11 22:30:18	TCP	172.16.6.25	172.16.6.30	20000, 20001	1, 20002, 20003, 20004, 20005	5, 20006, 20007, 20008, 20009, 20010
M - F H + - F - K - K -	° 0					
select * from epuertos where ID like '779'	95177';				Query time: 0.001s	Record 1 of 1

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:

escaneo					
Objetivo del plugin:		5.8.5		S	
Analizar et ultimo archivo n	tcapd obtenido en bi	esqueda de anoma	has tipicas de aigui	i marware.	
Se encontraron las siguiente	s anomalias:				
Escaneo	1P'S encontrado: 2011-01-11 22:50:17				
				14	

Protocolo	IP origen	Puerto origen	->	IP Destino	Puerto Destino	Paquetes	Trafico
TCP	172.16.6.81	2031	-9.	172.16.6.141	8060	o	163 0 H
TCP	172.16.6.61	1408	->	172.16.6.142	8060	0	171 2 M
TCP	172.16.6.41	1324	->	172.16.6.143	8060	0	247.4.11
тср	172.16.6.41	1175	->	172.16.6.144	8060	e	163.7 B
TCP	172.16.6.41	1684	->	172.16.6.145	8060	0	16.4 N
TCP	172 16 6 41	1768	->	172.16.5.146	8060	0	16.4 N
TCP	172.16.6.41	2513	->.	172.16.6.147	8060	0	16.4 M
TCP	172.16.6.81	2724	->	172.16.6.140	8040	0	165.4 H
TCP	172.16.6.41	2033	->	172.16.6.149	8060	o	16.4 M
TCP	172.16.6.41	2017	->	172.16.6.150	6060	0	16.4 10

Se observa que la 1p 172.16.6.41 esta buscando alguna otra 1p dentro de la red que pueda infectar!

El escaneo de Ip's realizado es de forma secuencial con una variación en el tercer o cuar del caso encontrado

insertado la anomalia en tabla 'eips' con ID- 97452838 ha notificado via email a: 'aldo§localhost.localdomain' sobre la anomalia de dectectada.

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.

Back	New Reply ReplyA	For	C OQ ward FuedAsAt	E) FundAs	orig Print AddrBoo	k Cale	d ndar Web() Disk Pr	a Logout		ToTrash
4 5/16 Fecha: Remite Destine Asunto	Tue, 11 Jan 20 mte: aldeano_d atario: aldo@lo : Asunto del me	11 2 emo calh ensa	2:50:17 -06 n_nfsen@k ost.localdor je-> Alerta!!	00 🔬 nain III Ano	st.localdomain 🕱, malias detectadas	. Q.				Todos los	encabezados
Escane	o de Ip'S encon 2011-01-1	trad	0:								
Protoco	lo Iporigen		Pto origen	-	> Ip destino		Pto de	stino	Paquetes Trafico		
TCP	172.16.6.41		1031	->	172.16.6.141		8060	0	163.8 M		
TCP	172.16.6.41		1408	->	172.16.6.142		8060	0	171.2 M		
TCP	172.16.6.41		1324	->	172.16.6.143		8060	0	147.4 M		
TCP	172.16.6.41		1175	>	172.16.6.144		8060	0	163.7 M		
TCP	172.16.6.41		1684	->	172.16.6.145		8060	0	16.4 M		
TCP	172.16.6.41		1768	->	172.16.6.146		8060	0	16.4 M		
TCP	172.16.6.41		2513	>	172.16.6.147		8060	0	16.4 M		
TCP	172.16.6.41		2724	->	172.16.6.148		8060	0	165.4 M		
TCP	172.16.6.41		2033	>	172.16.6.149		8060	0	16.4 M		
TCP	172.16.6.41		2017	->	172 16.6.150		8060	0	16.4 M		
Se obs El esca del cas Se ha i	erva que la ip 17 ineo de lp's reali o encontrado nsertado la anoi	2.10 izad	5.6.41 esta o es de forn a en tabla 'e	buscan na sec lips' co	ndo alguna otra ip uencial con una va in ID= 97452838.	dentr	o de la re on en el t	ed que	pueda infectar! o cuarto octeto dependiendo		
4 5/16									A		
Mapa d	e caracteres is	0-88	359-1 > utf-8						Membrete · •	GUARDADOS - Move	r Copiar
									OpenWebMail version 2.53 ¿Ayuda?		

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'

52			Untitled @an	omalias (mysql)	*	>
File Edit Form	at <u>Y</u> iew <u>W</u> indow <u>H</u> elp					
🕨 Run 📕 Ste	op 😸 Explain 🎇 Expon	Wizard	🖥 New 💼 Load	Save 🔚 Save As	🔍 Find 📑 Word Wrap	🕜 Grid View 🔄 Form View 🚆
Query Builder	Query Editor					
1 select *	* from eips where ID like	97452838	13			
Message Res	sult1 Profile Status					
ID	fecha	Protocolo	ip_origen	ip_destino		pto_destino
974528	38 2011-01-11 22:50:17	TCP	172.16.6.41	172.16.6.141, 172.16	.6.142, 172.16.6.143, 172.16.6.	144, 172.16.6.145 8060
	• + - • ~ × e	0				
select * from eig	os where ID like '97452838':				Query time: 0.000s	Record 1 of 1

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:

Objetivo de Analizar el Se encontra	l plogin: ultimo archivo ron las siguien Envio	nfcapd obtenido en tes anomalias: de informacion hacia e 2011-01-11 23:25:18	busqu 1 exteri	rda de anomal or encontrado:	ias tipicas de algun u	ialware,	
Protocolo	1P origon	Puerto origen	->	IP Destino	Puerto Destino	Paguntes	Trafico
10P	172.16.10.4	10500	-5	80,204.54.65	20082	0	235.1 8
400	172.16.10.4	10501	->	80.204.54.65	20067	0	233.1 H
40F	172.16.10.4	10502	->	80.204.54.65	20089	0	239.1 H
TOP	172.16.10.4	10503	->	80.204.54.65	20058	0	233.1 M
JDP	172.16.10.4	10504	->	80.204.54.65	20112	0	233.1 8
1DP	172.16.10.4	10505	->	80.204.54.65	20012	0	239 1 M
902	172.16.10.4	10506	->	80.204.54.65	20062	0	233.1 M
IDP	172.16.10.4	10507	->	80.204.54.65	20027	o	239 1 N
TOP	172.16.10.4	10508	->	80.204.54.65	20181	0	233.1 H
TDP	172.16.10.4	10509	->	80.204.54.65	20041	0	230.1 8
CDP	172.16.10.4	10510	->	80.204.54.65	20017	0	233.1 N

Se observa que la 1p origen: 172.16.10.4 perteneciente a una red de usuarios esta enviando

información con un tratico mayor a sub nacia pos fuera del rango permitido. Tambien se detecta que la fio rigen 172.16.10, stillas puertos origen de forma secuencial en el envio de la información Se ha insertado la anomalia en tabla "axterior" con De 149754654 Y se ha notificade via emanía a: "iddollcalhest.icondimanio" abbre la anomalia de dectectada.

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.

Fecha:	Fue, 11 Jan 20	112	3:25:18 -060	0 0								To	dos los en	cabezado
Remiter	te: aldeano_d	emo	n_nfsen@loo	calhost.	localdomain 🕵	Q.								
Destinat	ario: aldo@lo	calho	ost localdom	ain										
Asunto:	Asunto del me	nsaj	e-> Alerta!!!!	Anom	alias detectadas									
Envio de	información ha	1.02	el exterior el	ncontra	00:									
Drotocol	2011-01-1	1 23	.20.10 Dto origon	2	In dection		Dta dastina	Deeu	inter	antina.				
LIDP	172 16 10 A		10500		80 204 54 65		20082	n aqu	233 1	M				
UDP	172 16 10 4		10501		80 204 54 65		20067	0	233 1	M				
UDP	172 16 10 4		10502	->	80 204 54 65		20089	0	233 1	M				
UDP	172 16 10 4		10503	->	80 204 54 65		20058	õ	233 1	M				
UDP	172.16.10.4		10504	->	80,204,54,65		20112	0	233.1	M				
UDP	172.16.10.4		10505	->	80.204.54.65		20012	0	233.1	M				
UDP	172.16.10.4		10506	->	80.204.54.65		20062	0	233.1	M				
UDP	172.16.10.4		10507	->	80.204.54.65		20027	0	233.1	M				
UDP	172.16.10.4		10508	->	80.204.54.65		20181	0	233.1	M				
UDP	172.16.10.4		10509	->	80.204.54.65		20041	0	233.1	M				
UDP	172.16.10.4		10510	->	80.204.54.65		20017	0	233.1	M				
Se obse	va que la ip or	gen	172.16.10.4	4 perten	eciente a una red	de u	suarios esta	enviand	lo inform	cion con un trafico mayor a 5 MB hacia lp's fuera de	el rango permitido	6		
ambien	se detecta qu	e la	p origen 1/2	2.16.10.	4 utiliza puertos d	e tori	ma secuenci	al en el	envio de	a información				
Se ha in	sertado la anoi	nalia	a en tabla 'ex	cterior o	con ID= 149/5465	4.								
₫ 3/25 ₽										A			_	
Mapa de	caracteres is	0-88	59-1 > utf-8						N	ambrete		GUARDADOS -	Mover	Copiar
Contraction of the local distance of the loc	CONTRACTOR OF STREET	-	and the second second							NAMES AND A DESCRIPTION OF A DESCRIPTION				



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'

8		Untitled @a	inomalias	(mysql) *					
File Edit Format View Window Help									
🕨 Run 📕 Stop 🎦 Explain 🎇 Export	Wizard	a New 📄 Load	Save 4	Save As	🔍 Find 📑 Wor	d Wrap	Grid View	S Form View	
Query Builder Query Editor									
1 select * from exterior where ID	like '149754	4654';							_
Message Result1 Profile Status									
ID fecha	Protocolo	ip_origen	pto_origen					ip_dest	ino
149754654 2011-01-11 23:25:18	UDP	172.16.10.4	10500, 10501,	10502, 10503,	10504, 10505, 105	606, 10507,	10508, 10509, 1	0510 80.204	54.65
N ~	ø								

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 máguinas "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
тср	172.16.6.12	2011	->	172.16.10.5	3306	0	947.6 10
CP	172.16.5.14	2640	->	172.16.10.5	3306	0	947.6 10
CP	172 16 5 16	2329	->	172.16.10.5	3306	0	947.6 M
CP	172.16.5.18	2836	->	172.16.10.5	3306	0	947.6 10
CP	172.16.6.12	2640	->	172.16.10.5	3306	C	947.6.2
CP	172.16.5.14	2838	->	172.16.10.5	3306	o	947.6 11
CP	172.16.5.16	2608	->	172.16.10.5	3306	0	947.6 12
CP	172.16.5.18	2567	->	172.16.10.6	8306	0	947.6 11
CP	172.16.5.12	2927	->	172.16.10.5	3306	0	947.6 18
CP	172 16 5 14	2619	->	172.16.10.5	3306	0	947.6 18
CP	172.16.5.16	2052	->	172.16.10.5	3306	0	947 6 1
CP	172.16.5.10	2030	->	172.16.10.5	3306	0	947.6 11

Se observa que la Ip destino 172.16.10.5 Esta recibiendo multiples conexiones sobre le puerto 3306 de una o varias Ip origem. Con un trafico mayor a 50 MB. Con el objetivo de saturar la conexion Se ha insertado la ancmalia en tabla "DoS" con ID» 65951185 Y se ha notificado via email a: 'aldoblocalhost.localdomain' sobre la anomalia de dectectada.

Ataque de negación de servicios encontrado Figura 5.18

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	Reply Reply All	Forward: Fundaz.A	a Fund	Rooma Print Address	Cale	vdar Wet	China Pr	t Logod		To Tresh
4 6/311										March 1997
Fecha:	Tue, 11 Jan 201	1 23 40 24 -06	000	8						Todos los encabezados
Remite	nte: aldeano_de	mon_ntsen@h	ocalho	ost localdomain 🕵	n _x					
Destina	tario: aldo@loc	alhost localdor	main							
ASUMO	Asonto del mer	isaje-> Menar		onnanas derectadas						
Andre	2011-01-11	23:40:24	trado							
Protoco	lo lo origen	Pto origen	10	-> Ip destino		Pto de	stino	Paquetes	Trafico	
TCP	172 16 5 12	2011	->	172.16.10.5		3306	0	947.6 M		
TCP	172.16.5.14	2640	-3	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 obse Con el o Se ha in	erva que la lp dei objetivo de saturi isertado la anom	stino 172 16 10 ar la conexion talia en tabla 1	DoS' o	ta recibiendo multip	les ci	onexior	ies sol	bre le puerto 33	95 de una o varias Ip origen. Con un trafico mayo	a 50 MB.
4 6/31			-							
Mapa de	e caracteres iso	-8859-1 > uff-8						M	mbrete - • 1	GUARDADOS - Mover Copiar
								OpenWebMa	version 2.53 (Ayuda?	
	I	-igura 5	5.19	9				Notifica	ción de la fuga de inforn	ación 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.