Programación en SHELL

Proyecto Final

Nombre: _____ Grupo: _____

Objetivo
Desarrollar un programa para el procesamiento de biácoras de correo, que proporcione información y estadísticas sobre el correo, antivirus y antispam.

Justificación
Ante el incremento y constante evolución de las amenazas a la seguridad que llegan a través de correo electrónico (virus y spam, principalmente), es necesario contar con información precisa sobre el comportamiento de estas amenazas y de las herramientas desplegadas para su contención. Tal información está contenida, en el caso de los servidores de correo electrónico, en las bitácoras del correo y de las herramientas asociadas para su protección. Por ello es indispensable contar con herramientas que permitan analizar y sintetizar la información que se encuentra en tales bitácoras.

Desarrollo:
El desarrollo de la herramienta estará basado en el shell de Unix (preferentemente BASH o Bourne Shell) y utilerías de Unix. La herramienta operará de la siguiente manera:

1. Configuración

Deberá contar con un script de instalación que haga lo siguiente:

- Solicitar el nombre del directorio en donde se buscarán las bitácoras a procesar.
- Solicitar el nombre del directorio de salida (en el que se almacenarán los reportes)
- Solicitar el nombre del directorio de datos (Información histórica).
- Solicitar el nombre del directorio para la herramienta.
- Solicitar la frecuencia con que se ejecutará la herramienta. Para ello, deberán darse las siguiente opciones:
    - Cada hora.
    - Diario. En este caso, además, deberá solicitarse que se indique la hora del día en que deberá ejecutarse.

Elaboró: Rubén Aquino Luna

Programación en SHELL

NOTA: Ni el script ni la herramienta requieren privilegios de root en el sistema, pero sí deberán validar que tengan los permisos de lectura/escritura necesarios en los directorios configurados.

La información ingresada deberá guardarse en un archivo de configuración (de nombre arbitrario, elegido por el desarrollador), mismo que deberá almacenarse en el directorio designado para la herramienta.

2. Calendarización

Con la información sobre la frecuencia con que se ejecutará la herramienta, deberá programarse el crontab para el usuario con que se haya ejecutado el script de instalación y deberá programarse la ejecución de la herramienta según la frecuencia señalada por el usuario.

3. Operación

3.1 Entrada de datos

La herramienta deberá validar si existen archivos de bitácora que procesar en el directorio configurado. Si existe más de un archivo, deberán procesarse los archivos en orden cronológico (primero el más antiguo), basados en el primer registro de cada bitácora.

3.2 Procesamiento

Para cada bitácora procesada, deberá obtenerse la siguiente información, la cual deberá obtenerse para períodos de 1 hora.

- Número de correos recibidos en el período de tiempo.
- Número de correos analizados por el antivirus.
- Número de correos infectados con algún tipo de malware por el antivirus.
- Nombre y número de virus que se han detectado.
- Número de correos analizados por el antispam.
- Número de correos detectados como spam.
- Promedio de calificación del correo spam en el período

Elaboró: Rubén Aquino Luna

Programación en SHELL

- Promedio de calificación del correo que NO es spam en el período
- Criterios de spam y la cantidad de incidencias.

Toda esta información se deberá guardar en un archivo ubicado en el directorio de datos configurado. El formato del contenido deberá ser el siguiente:

Fecha|Hora(inicial del período)|Correos recibidos|Correos analizados por el AV|Correos Infectados|Malware1:No,Malware1:No,...|Correos analizados por Antispam | Correos detectados como spam | Prom.Cal.SPAM | Prom.Cal.NO SPAM | Criteriospam1: No,Criteriospam2:No, ...

Si la bitácora procesada inicia en un período para el que ya existe información en el archivo de datos, deberán conjuntarse la información en un sólo registro para el período.

3.4. Reportes

La herramienta podrá ser llamada en dos modos de operación:

- Procesamiento de bitácora
- Reportes

La operación por omisión será la de procesamiento de bitácora. El modo de Reportes deberá ser indicado a través de una opción en línea de comandos (-r).

En modo de reportes, la herramienta tendrá requerimientos opcionales:

- Fecha de inicio (-fi)
- Fecha final (-ff)
- Archivo de salida (-o)

Si se indica una fecha de inicio, el procesamiento se hará desde esa fecha, hasta la fecha final que se indique o el final del archivo de datos. Si se indica una fecha final, el procesamiento se realizará desde la fecha de inicio que se indique, o desde el inicio del archivo de datos. Se puede indicar un archivo de salida, en el que se escribirá el reporte.

Elaboró: Rubén Aquino Luna

Programación en SHELL

El reporte debe ser un texto que contenga una tabla con el resumen de la información del archivo de datos. Esto es, para el período que se solicite, deberá indicar:

- Número de correos recibidos en el período de tiempo.
- Número de correos analizados por el antivirus.
- Número de correos infectados con algún tipo de malware por el antivirus.
- Nombre y número de virus que se han detectado.
- Número de correos analizados por el antispam
- Número de correos detectados como spam
- Promedio de calificación del correo spam en el período
- Promedio de calificación del correo que NO es spam en el período
- Criterios de spam y la cantidad de incidencias.

4. Aspectos a considerar

Pueden encontrar ejemplos de las bitácoras que la herramienta debe procesar en:

```
http://turing.seguridad.unam.mx/progshell/mail.log.5.gz

http://turing.seguridad.unam.mx/progshell/mail.log.6.gz

http://turing.seguridad.unam.mx/progshell/mail.log.7.gz
```

4.1 Correos recibidos

Deberán contarse como correos recibidos las líneas de bitácora que contengan la cadena postfix/smtp, que indiquen que el estado es enviado (status=sent) y que la dirección de destino es un usuario de @seguridad.unam.mx o @correo.seguridad.unam.mx. A continuación se muestran ejemplos de las líneas que indican que el servidor ha recibido un correo.

```
Jun 28 06:28:21 correo postfix/smtp[30315]: C46B73A208:
to=<cguel@correo.seguridad.unam.mx>, relay=localhost[127.0.0.1],
delay=19, status=sent (250 2.6.0 Ok, id=30481-02, from MTA: 250 Ok:
queued as EAADA3A24A)
```

Elaboró: Rubén Aquino Luna

```
Jun 28 06:28:34 correo postfix/smtp[30315]: 2FF0A3A208:
to=<info@correo.seguridad.unam.mx>, relay=localhost[127.0.0.1],
delay=5, status=sent (250 2.6.0 Ok, id=30481-03, from MTA: 250 Ok:
queued as 6519D3A24C)

Jun 28 06:28:42 correo postfix/smtp[30429]: 4C9903A208:
to=<jrojas@correo.seguridad.unam.mx>, relay=localhost[127.0.0.1],
delay=5, status=sent (250 2.6.0 Ok, id=30465-04, from MTA: 250 Ok:
queued as C41963A24B)

Jun 28 06:29:11 correo postfix/smtp[30315]: 890273A208:
to=<info@correo.seguridad.unam.mx>, relay=localhost[127.0.0.1],
delay=5, status=sent (250 2.6.0 Ok, id=30481-04, from MTA: 250 Ok:
queued as BC6BA3A24A)
```

4.2 Correo SPAM

Para la información sobre correo spam, deberán considerarse las líneas de bitácora como las siguientes

```
Jun 28 06:55:29 correo amavis[31137]: (31137-06) SPAM-TAG,
<ctmtonline.com@littlesproutsdaycare.com> ->
<noticias@correo.seguridad.unam.mx>, Yes, hits=2.5 tagged_above=-10.0
required=-0.6 tests=BAYES_00, HTML_IMAGE_ONLY_12, HTML_MESSAGE,
HTML_SHORT_LINK_IMG_2


Jun 28 06:55:32 correo amavis[31114]: (31114-08) SPAM-TAG,
<institutocanzionm@institutocanzion.com> ->
<escaneos@correo.seguridad.unam.mx>, No, hits=-2.1 tagged_above=-10.0
required=-0.6 tests=BAYES_00, HTML_MESSAGE, MIME_QP_LONG_LINE
```

En estas líneas de bitácora se indica con Yes o No si el correo ha sido considerado spam. Así mismo, se muestra la calificación que se le dio al correo con hits=XX. luego del parámetro tests se muestran los criterios con los que coincidió el correo analizado, como `tests=BAYES_00, HTML_MESSAGE, MIME_QP_LONG_LINE.`

4.3. Virus/Malware

Elaboró: Rubén Aquino Luna

Programación en SHELL

La cadena run_av en la bitácora indica que el correo ha sido procesado por el antivirus. Debe tenerse cuidado de que sólo se cuente una vez la cadena run_av para un identificador único del proceso, que en los ejemplos siguientes son (03221-02)y (03216-03). Si un correo está infectado por algún tipo de malware, se podrá en contrar una línea de bitácora como la que aparece al final de los ejemplos siguientes.

```
Jun 28 10:07:21 correo amavis[3221]: (03221-02) run_av:
/usr/bin/clamscan status=0 (0 ),LibClamAV Warning:
**********************************************************\nLibClamAV
Warning: ***  This version of the ClamAV engine is outdated.
***\nLibClamA
V Warning: *** DON'T PANIC! Read http://www.clamav.net/faq.html
***\nLibClamAV Warning:
**********************************************************\nLibClamAV
Warning:**********************************************************\nLibCl
amAV Warning: ***  This version of the ClamAV engine is outdated.
***\nLibClamAV Warning: *** DON'T PANIC! Read
http://www.clamav.net/faq.html ***\nLibClamAV
Warning:**********************************************************\n/var/
lib/amavis/amavis-20070628T100658-03221/parts/part-00001:
OK\n/var/lib/amavis/amavis-20070628T100658-03221/parts/part-00002:
OK\n/var/lib/amavis/amavis-20070628T100658-03221/parts/part-00003: OK


Jun 28 10:07:55 correo amavis[3216]: (03216-03) run_av:
/usr/bin/clamscan status=1 (256 ),LibClamAV Warning:
**********************************************************\nLibClamAV
Warning: ***  This version of the ClamAV engine is outdated.
***\nLibClamAV Warning: *** DON'T PANIC! Read
http://www.clamav.net/faq.html ***\nLibClamAV
Warning:**********************************
**********************\nLibClamAV Warning:
**********************************************************\nLibClamAVWarn
ing: ***  This version of the ClamAV engine is outdated.
***\nLibClamAV Warning: *** DON'T PANIC! Read
http://www.clamav.net/faq.html *
**\nLibClamAV Warning:
**********************************************************\n/var/lib/amav
is/amavis-20070628T100652-03216/parts/part-00001:
OK\n/var/lib/amavis/amavis-20070628T100652-03216/parts/part-00003:
```

Elaboró: Rubén Aquino Luna

Programación en SHELL

```
Worm.Mydoom.M FOUND


Jun 28 10:07:55 correo amavis[3216]: (03216-03) run_av: INFECTED:
Worm.Mydoom.M
```

Elaboró: Rubén Aquino Luna