Intrusión y respuesta

Yeray Santana Benítez

Introducción

- Las empresas manejan gran cantidad de información que guardan en sus sistemas informáticos.
- Como administradores de sistemas debemos asegurar la integridad y seguridad de nuestros equipos.
- Un sistema de detección de intrusiones (IDS) es un proceso o dispositivo que analiza al sistema y/o la actividad de la red con el objetivo de encontrar entradas no autorizadas o actividad maliciosa.

Clasificación de los IDS

- IDS basados en hosts: intentan determinar actividades maliciosas, abusivas o intrusión. Para ello comparan los logs del sistema con una base de logs interna que representan ataques conocidos.
  - Tripwire, SWATCH, RPMs (verificación de cambios en archivos: tamaño, permisos).

- IDS basados en la red: escanean los paquetes que circulan por la red creando logs asociados a paquetes sospechosos. Luego comparan dicha información con una base de datos interna. Muchos de estos sistemas de detección necesitan actuar en modo promiscuo para poder capturar todos los paquetes que circulan por la red.
  - Ifconfig eth0 promisc

1. Audición y monitorización

- Usaremos dos herramientas:
  - Saint para escuchar hosts de nuestra red y descubrir vulnerabilidades.
  - Swatch para monitorizar logs.

SAINT: Security Administrator's Integrated Network Tool

- Escanea ordenadores de una red y comprueba las vulnerabilidades mediante una base de datos dependiente del S.O.
- Reporta la información necesaria para determinar dichas vulnerabilidades.
- Necesita ciertos requisitos para ser instalado:
  - Perl 5.0 o superior.
    - http://www.cpam.org
  - Samba: en caso de tener equipos en la red con Windows.

- Nmap: comprueba puertos de la red
  - http://www.insecure.org/nmap/

```
$ tar -xzf nmap-2.53.tgz
$ cd nmap-2.53
$ ./configure
[...]
$ make
[...]
$ su
Password:
# make install
[...]
#  exit
$
```

- Descargamos Saint desde http://www.wwdsi.com/saint/downloads/

```
$ tar –xzf saint-3.1.2.tar.gz.tgz
$ cd saint-3.1.2
$ ./configure
[...]
$ make
[...]
$ su
Password:
# make install
mkdir –p /usr/local/man/man1
install –c –o root –g 0 –m 444 saint.1
   /usr/local/man/man1/saint.
#
```

- Debemos tener una versión actualizada del programa ya que los ataques y las vulnerabilidades están en continua evolución.

Usando Saint

- Se ha de tener privilegios de superusuario y ejecutarlo en un terminal X.
- Saint se ejecuta en una ventana de navegador.
  - ./Saint
- Una vez se ha abierto la ventana, debemos ir a la opción “Target Selection”, que nos llevará a otra ventana en la que declararemos los hosts que queremos escanear.
- Podemos poner el nombre del host “myhost.mynet.net”, direcciones IP o subredes enteras. Si ponemos más de un equipo deberá haber un espacio entre ellos.

- Una vez elegidos los equipos a escanear, seleccionamos la intensidad del escaneado. Ahora estamos listos para proceder con la audición pinchando sobre el botón “Start the scan”.

- NO se debe usar la ventana web que se abre para navegar fuera de la red, ya que SAINT es ejecutado con privilegios de root y guarda información usando el Netscape.

- Picamos sobre la opción de recargar la pagina del navegador y pinchamos sobre “Yes”: empezará entonces la busqueda de vulnerabilidades.

- Una vez que SAINT termine de escanear, pinchamos sobre ”Continue with report and analysis”.

- En la pantalla de “Data analysis” se nos muestra una serie de opciones cada una de las cuales muestra información sobre vulnerabilidades o posibles vulnerabilidades que SAINT encontró.

- Pinchamos sobre “By approximate danger level” y se nos mostrarán todas las vulnerabilidades del sistema.

- Cada vulnerabilidad está listada por host y titulo. Pinchando sobre el link obtenemos información detallada:
  - El nombre y links a información más detallada.
  - Información para determinar como afecta la vulnerabilidad al sistema.
  - El nivel de peligro.
  - Los tipos y versiones del software y S.O. a los que afecta.
  - Posibles soluciones para eliminar o recuperarse de un ataque.

- El grado en que la vulnerabilidad afecta al sistema se declara con un semáforo:
  - Si el indicador es amarillo, se ha de estudiar la vulnerabilidad para ver si realmente afecta al sistema.
  - Si el indicador es rojo, la vulnerabilidad afecta al sistema.

SWATCH

- Herramienta escrita en PERL cuya función es la de monitorizar logs y actuar en consecuencia:
  - Mandar un fax, lanzar un beeper,...
- Se puede descargar de: ftp://ftp.stanford.edu/general/security-tools/swatch/

Instalando SWATCH

- Instalación:

```
$ tar -xf swatch.tar
$ cd swatch-3.0.1
$ perl Makefile.PL
[...]
$ make
[...]
$ su
Password:
# make install
[...]
#
```

Usando SWATCH

- Interfaz: Línea de comandos al que se la pasan parametros:
  - Swatch –c matchfile - -tail logfile
    - Logfile es el path a cualquiera de los logs del sistema.
    - Matchfile es el path a un fichero de texto que contendrá la configuración.
- Una vez configurado, se puede considerar la posibilidad de ejecutar el programa en segundo plano, o dedicar un equipo en exclusiva para monitorizar todas las acciones de las subredes en cuestión.

El fichero matchfile

- Se empieza el fichero indicando cadenas que contendrán el log especificado para las que queremos una alerta:
  - Watchfor /ROOT LOGIN|UID=0/
    - Indica si hay actividad del root en el log especificado.
- Después especificamos las acciones a realizar.

Acciones soportadas

- echo [mode]: muestra el log vigilado, por la terminal. Mode indica el formato del texto: bold, undescore, blink, inverse, black, red, , green, yellow, cyan, blue, white, black_h, red_h, etc.
- bell [count]: emite una señal. Count indica el numero de tonos.
- exec command [args]: ejecuta el comando especificado.
- mail [addr], [subj]: envía un mensaje de correo electrónico a las direcciones especificadas en addr con el título especificado en subj.

- Pipe command: envía la entrada que se busca en el log como parámetro al comando.
- write [user]: escribe la entrada del log en el terminal definido por user. Podemos poner más usuarios separándolos con “:”.
- Throttle h:m:s: si se repite la entrada en el log más de una vez en el periodo de tiempo descrito, la acción a realizar sólo se ejecutará una vez.
- Continue: encadena comandos watchfor.

Ejemplo

- El siguiente fichero busca las cadenas root, login o UID=0 (actividad del root), muestra por la terminal el log en rojo, envía un correo a admin@mynet.net y emite dos pitidos:

```
Watchfor /root LOGIN|UID=0/
Echo red
Mail addresses=admin@mynet.net,
        subject=".SW. Actividad del root"
Bell 2
```

2. Detección de ataques en progreso

- Snort: programa que nos permite monitorizar el tráfico de nuestra red en tiempo real y descubrir paquetes maliciosos y tomar decisiones basadas en reglas con respecto a dichos paquetes.

- Consume muchos recursos por lo que no es aconsejable para redes pequeñas (uno o dos equipos).

Consideraciones previas

- Es aconsejable dedicar una maquina en exclusiva para ejecutar el programa.
- También el disponer de un firewall, ya que el tráfico que se tendrá que controlar se reduce considerablemente.

Descarga e instalación

- Antes de instalar el programa debemos instalar las librerias libcap (ftp://ftp.ee.lbl.gov) y libnet (http://www.packetfactory.net/projects/libnet/dist/).

- Snort se puede descargar de:
  - http://www.snort.org/snort-files.html/

- Instalación:

```
$ tar -xzf snort-1.7.tar.gz
$ cd snort-1.7
$ ./configure - - prefix=/usr/local \
>- - with – lipcab-includes=/usr/include/pcap \
>- - with lipcab-libraries=/usr/lib \
>- - enable – smbalerts \
>- - enable - flexresp
[...]
$ make
[...]
$ su
Password:
# make install
[...]
#  exit
$
```

Reglas

- Snort hace uso de un sniffer para buscar patrones en el trafico de la red.

- Estos patrones se definen por medio de reglas:
  - Acción a llevar a cabo (alerta, log, pasar).
  - El protocolo.
  - La dirección y el puerto fuente y la dirección y puerto destino.
  - Opciones adicionales.
    - Ejemplo Alert tcp any any -> 192.168.1.0/24 142 (msg “Desbordamiento buffer Imap”} ; content: “90E8 C0FF FFFF /bin/sh;”)
    - Snort genera una alerta si detecta un ataque en el puerto 143. La etiqueta content especifica una firma.

- Existen numerosas reglas ya creadas que podemos incorporar en la sección rules de la pagina oficial:
  - http://www.snort.org/

Reglas más usuales

- Backdoor activity: Más apropiado para equipos con Windows; genera múltiples falsas alarmas. No recomendada.
- Backdoor attempts: Más apropiado para equipos con Windows; genera múltiples falsas alarmas. No recomendada.
- Backdoor (Sig.): Más apropiado para equipos con Windows. Recomendado para entornos con Linux y Windows.
- DDos: Recomendado para todas las instalaciones.
- Exploits: Esencial para todas las instalaciones.

- Finger: Recomendado para todas las instalaciones.
- FTP: esencial si disponemos de servidores FTP.
- ICMP: Recomendado para todas las instalaciones.
- MISC: Recomendado para todas las instalaciones.
- NetBIOS: Esencial si ejecutamos Samba en equipos Linux o disponemos de clientes windows.
- RPC: Recomendado para todas las instalaciones.
- RServices: Recomendado para todas las instalaciones.
- Scans: Recomendado para todas las instalaciones.
- SMTP: Esencial si ofrecemos servicios de SMTP.
- Telnet: Esencial si ofrecemos servicios de Telnet.

- Virus: Más apropiado para hosts Windows; Recomendado si equipos Windows acceden a correo.
- Web-cgi: Esencial si esta disponible el acceso a web.
- Web-ColdFusion: Esencial si esta disponible el acceso a web basadas en ColdFusion.
- Web-FrontPage:Más apropiado para hosts Windows; Esencial si equipos Windows disponen de este recurso.
- Web-IIS:Más apropiado para hosts Windows; Esencial si equipos Windows disponen de este recurso.
- Hig False Alert: Conjunto de reglas que generan falsas alarmas. No recomendado

- Una vez hayamos seleccionado las reglas, las descargamos y las pasamos al fichero /etc/snort.rules.

- Debemos ir actualizando dicho fichero con las reglas que vayan saliendo y que se acomoden a nuestros intereses.

- Una buena opción es ejecutar Snort en segundo plano y luego con un herramienta como SWATCH estar atento a los logs del sistema.

- Para ejecutar Snort:
  - Snort –D –A alert –c /etc/snort.rules

Salida

- La salida del programa es de difícil comprensión, por lo que se ha creado un programa para facilitar la lectura de dicha salida, convirtiéndola en documentos html con alertas tabuladas y links: SnortSnarf.
  - http://www.snort.org/dl/contrib/data_analysis/snortsnarf/

3. Preservando información

- La información es un elemento esencial en las empresas.
- Debemos asegurarnos de que si dicha información se pierde a o se deteriora, podemos recuperarla.
- No sólo los datos corren peligro, también los binarios y los ficheros de configuración son susceptibles a ataques de intrusos.
  - Puertas traseras.

Root kit

- Un Root kit es un grupo de binarios modificados que ejecutan las funciones de login, ls, syslog, etc.

- Diseñados para que su descubrimiento sea difícil.
  - Un login modificado puede enviar guardar la información del usuario y el password.
  - Un ls modificado no nos mostrará los ficheros extras que han sido modificados por el atacante.

- Si el tenemos indicios de que el sistema está comprometido:
  - Reinstalar Linux por completo
  - Restaurar el sistema por medio de copias de seguridad.

Backups: Tar y afio

- Herramientas para la creación y restauración de copias de seguridad.
- No requieren programas adicionales para su funcionamiento y caben en un disco.

Copias de seguridad: Tar

- La línea de comando es la siguiente:
  - Tar –[c|x|t] [-pv] –f device path1 path2
    - C: crear.
    - X: extraer.
    - T: testear.
    - P: preservar los permisos originales.
    - V: mostrar información.
    - F: escribir en los dispositivos especificados en path1, path2, ...
  - Ejemplo de copia el directorio /usr en el dispositivo especificado por st0.
    - Tar –cf /dev/st0 /usr

Caso concreto: Copiado del sistema entero

- Si ejecutamos la siguiente sentencia: “tar –cf /dev/st0 /” para hacer una copia del sistema, estaremos copiando el directorio /proc, dicho directorio contiene un volumen elevado (cientos de megas) de datos del kernel que son innecesarios y pueden hacer que el comando se bloquee.

- También estaremos copiando el directorio /mnt que contiene todos los archivos montados en nuestra instalación de Linux.

- El comando correcto sería:
  - Tar –cf /dev/st0 $(ls -1 / |grep –v –e proc –e mnt)

Algunos casos útiles

- Para restaurar archivos al directorio original ejecutamos el siguiente comando:
  - Cd / ; tar –xpf /dev/st0
- Podemos especificar paths en los que queremos restaurar los archivos:
  - Cd /; tar –xpf /dev/st0 ‘usr/x11r6/*’ ’usr/local/*’
- Para restaurar archivos desde un disco SCSI preservando los permisos:
  - Cd /usr/local; tar –xpvf /dev/sdc
- Usando el comando tee escribimos en un fichero la lista de archivos que se han restaurado:
  - Cd /; tar –xpvf /dev/sdc | tee /var/log/restodred.files

Copias de seguridad: Afio

- Similar al comando tar pero:
  - Pueden interactuar con sistemas que soporten el comando cpio (comando de compresión).
  - Soporta compresión por archivo, lo que lo hace útil para hacer copias de seguridad sobre cintas magnéticas que no soportan compresión por hardware.
- Se puede descargar de:
  - ftp://metalab.unc.edu/pub/linux/system/backup/

- La sintaxis del comando es la siguiente:
  - Find path1 path2 ... [-opts] | afio –[i|o|t] [-vZ] device
    - i: restaura una cinta o archivo.
    - o: escribe una cinta o archivo.
    - t: testea una cinta o archivo.
    - v: lista los archivos mientras son procesados.
    - Z: comprime los archivos usando gzip antes de realizar la copia.
    - find path1 path ... : archivos a comprimir.
    - device: dispositivo al que realizar la copia.

Algunos casos útiles

- Realizar una copia del directorio /usr a la cinta insertada en /dev/st0:
  - Find /usr |afio –o /dev/st0
- Copiar y comprimir:
  - Find /usr | afio –o –Z /dev/st0
- Restaurar un archivo al directorio root:
  - Cd /; afio –i /dev/st0
- Restaurar un archivo que ha sido comprimido:
  - Cd /; afio –i –Z /dev/st0

Operando con cintas magnéticas

- Tar y afio operan con dispositivos de almacenamiento de datos, como lo pueden ser las cintas magnéticas, por lo que debemos conocer métodos para manejarlas: el comando mt.

- La sintaxis básica:
  - Mt –f device operation_command [arguments]

Comandos

- Rewind: rebobina la cinta.
- Offline: rebobina y saca la cinta.
- Status: muestra el estado del dispositivo como si existe una cinta dentro o la densidad usada para escribir sobre la cinta.
- Retension:
- Erase: borra la cinta.
- Datcompression n: si n es 0 no realiza compresión, si es 1, comprime.,
- Fsf n, bsf n: busca n archivos hacia delante o hacia atrás.
- Fsr n, bsr n: busca n grabaciones hacia delante o atrás.
- End: posiciona la cabeza de lectura/escritura justo después del final de la cinta, para añadir nuevos archivos.

Realizando copias de seguridad periódicas

- Los datos guardados están en continuo cambio por lo que debemos definir una rutina para realizar copias periódicas.

- Debemos tener cuidado:
  - Las cintas se deterioran.
  - No guardar las copias en el mismo lugar que los datos originales: robos, fuego, etc.

- Podemos programar la realización de copias de seguridad periódicas con ayuda del demonio cron (demonio que sirve para ejecutar tareas programadas según una combinación de la hora, día del mes, mes, día de la semana y semana.).

- La siguiente línea lleva la cabeza de lectura/escritura de un dispositivo de cinta hasta el final de la cinta y realiza una copia del directorio /home.
  - Mt –f /dev/st0 eod; tar –cf /dev/st0 /home

- Debemos llevar el control sobre la cinta: llenado, deterioro, etc. Se recomienda usar varias e ir alternándolas.

- Posibilidad de usar cargadores de cintas: dispositivos hardware que van cambiando las cintas del dispositivo. El siguiente script rota las cintas (6) cada semana y copia el contenido de /home:

```
#!/bin/bash
# Selecciona el slot del cargador dependiendo de la
# semana y el número de cintas.
SLOT=$[$(date+%U)%6]
# Comprueba que no hay cinta cargada.
mtx –f /dev/changer unload
# Carga la cinta dependiendo del día de la semana.
mtx –f /dev/changer load $SLOT
# Busca el final de la cinta.
mt –f /dev//st0 eod
# Copia el directorio /home en la cinta.
Tar –cf /dev/st0 /home
```

Aplicaciones comerciales más usadas

- BRU (backup and restore utility): soporta recuperación del sistema en caso de accidentes.
- Ficheros BRU son portables a todas las plataformas que soporten dicho sistema, como Windows NT.
- Mas información en:
  - http://www.estinc.com/

- Arkeia: multiplataforma, multiprotocolo y robusto.
- Orientación cliente/servidor que puede realizar el fichero de backup y restablecer las operaciones para uno o más sistemas informáticos.
- Puede mantener cualquier conjunto de sistemas Linux y Windows en un solo dispositivo de backup en un servidor centralizado, facilitando enormemente las operaciones de recuperación de ficheros en entornos grandes de computación. Aunque los resultados obtenidos con Arkeia requieren sufrir una curva de aprendizaje importante.
- Gratis para menos de dos equipos.
- http://www.arkeia.com/

4. Recuperándonos de un ataque

- Como administradores de un sistema, debemos llevar un control sobre el mismo, con el que podamos descubrir irregularidades. Algunos indicios que nos pueden hacer sospechar si el sistema está comprometido son:
  - La presencia repentina de cuentas nuevas en etc/passwd.
  - El fallo o el comportamiento extraño de binarios.
  - Demasiado tráfico de red inexplicable, muchos puertos abiertos, muchas conexiones.
  - Una carga inexplicable de la CPU.

- En caso de que notemos que algo anda mal, lo primero es desconectar al sistema de la red (físicamente también).
- Intentar descubrir a las máquinas comprometidas y aislarlas del resto (gusanos, etc.).
- Es difícil intentar seguir el rastro de la persona que está atacando el sistema, por lo que se recomienda descartar esta opción siempre que dificulte las tareas de protección.

- Apagar el equipo:
  - Shutdown –r now

- En caso de que no podamos apagarlo como usuario root, hacer uso de la herramienta SysRq (combinación de teclas a las que el núcleo responderá sin importar qué otras cosas esté haciendo, salvo que esté completamente bloqueado). Tecleando Alt+SysRq+U hacemos que todos los ficheros sean de sólo lectura y con Alt+SysRq+s sincronizamos los discos disminuyendo el riesgo de perdida de datos para luego resetear el sistema.

- Si nada de esto funciona, reseteamos.

- Una vez reseteado, entramos en la BIOS para arrancar la placa y los controladores.

- Debemos asegurarnos que la configuración de la BIOS no ha cambiado. En caso afirmativo restauramos la configuración original.

- Si notamos algo sospechoso, apagamos el equipo y trabajamos con el disco duro como esclavo en otra máquina.

- Intentaremos determinar que datos no están contaminados para guardarlos con el objetivo de restaurarlos.
- Formatear el disco duro y reinstalar Linux.
- Cambiar las contraseñas de los usuarios al volver a crearlos.
- Restaurar los archivos desde copias de seguridad no contaminadas.

Otras herramientas

- CHKWTMP: Los archivos logs pueden ser alterados por intrusos. Esta herramienta detecta dicha alteraciones.
  - http://www.sunsite.ics.forth.gr/pub/systools/chkwmp/
- TCPLogD: Detecta rastreos silenciosos. Incluye la posibilidad de hacer logging, ignorar puertos y paquetes, además de una función que imposibilita el ahogamiento del demonio.
  - http://www.kalug.lug.net/tcplogd/
- HostSentry: Busca anomalías de login: comportamientos extraños, anomalías de tiempo y anomalías de lugar. También busca logins y crea sus propios logs, por lo que si se encuentra alguna discrepancia entre estos logs y los del sistema es por que se ha producido una intrusión.
  - http://www.psionic.com/abacus/host-sentry/

Otras herramientas

- Shadow: detecta rastreos silenciosos. Permite distribuir información sobre seguridad y detección de intrusiones entre varios hosts, lo que permite detectar ataques sofisticados en los que se mezcla y relacionan multiples atacantes y objetivos.
- MOM: herramienta de detección de intrusiones poderosa y compleja para vigilar redes enteras. Un procesos principal controla la información que le llegan de sus procesos hijos (en otros hosts)
  - http://biostat/wisc.edu/~annis/mom/
- El sistema Colibrí: semejante al MOM aunque mas potente.
  - http://www.csds.uidaho.edu/~hummer/

Otras herramientas

- AAFID: Sistema de detección y supervisión que utiliza pequeños programas independientes, llamados agentes, para realizar funciones de supervisión en los hosts de la red.
  - http://www.cs.purdue.edu/coast/projects/aafid-anounnce/

Bibliografia

- http://www.maestrosdelweb.com/editorial/snort/ Información en español sobre el programa snorf.
- http://www.zonagratuita.com/a-cursos/utilidades/50_herramientas_top.htm/ Información sobre herramientas relacionadas con la seguridad.
- http://www.tu-chemnitz.de/docs/lindocs/RH73/RH-DOCS/rhl-cg-es-7.3/ch-autotasks.html Información sobre realización de tareas periódicas.

- http://www.iec.csic.es/criptonomicon/linux/recursos.html/ recursos seguridad
- http://es.tldp.org/NuLies/web/2.2/Documentation/sysrq.txt Información sobre SysRq