Detección de intrusos con Debian GNU/Linux

by José Salvador González Rivera
<jsgr(at)linuxpuebla.org>

About the author:

José Salvador González Rivera es miembro activo del Grupo de Usuarios Linux de Puebla en México, constantemente participa en eventos para promover el uso de Software Libre y principalmente Linux, este semestre egresó de la Licenciatura en Sistemas Computacionales, puedes contactarlo en jsgr(at)linuxpuebla.org y también en jsgr(at)tec.com.mx

Abstract:

Ahora que toda la información se almacena de manera digital en medios electrónicos es mucho más ágil acceder a ella por medio de redes de computadoras que nos permiten el paso de datos a distancia, datos de índole financiera, gubernamental, militar, industrial y comercial que lamentablemente son objetivo fácil para las personas malintencionadas que no cuenten con la ética suficiente para obtenerla o destruirla.

Debido a la falta de conciencia no existen recursos abundantes sobre este tema en diversos idiomas, en este pequeño artículo haré una revisión "básica" sobre las técnicas y herramientas que podemos utilizar para detectar a los intrusos en Linux. Procuraré no repetir información con otras palabras de manuales de usuarios por lo que me centro en puntos específicos que se presentan.

Introducción

Al seleccionar un sistema operativo Linux debemos considerar al gran número de distribuciones que existen, la mayoría se basan principalmente en RedHat, por ejemplo Conectiva (Brasil), Hispa fuentes(España), Mandrake(Francia), SuSE (Alemania), Caldera y muchas otras que utilizan el manejador de paquetes RPM. Otra distribución es Slackware, el cual busca un Unix muy tradicional al seguir utilizando únicamente archivos de instalación .tgz "Casi" todas son desarrolladas por empresas comerciales, pero Debian no es el caso. Debian tiene un manejador de paquetes (DPKG) que nos facilita la actualización de programas al buscar automáticamente las actualizaciones desde Internet y cumpliendo dependencias de archivos y librerías que un paquete requiera facilitando la administración del sistema y permitiendo siempre estar al día automáticamente con las nuevas actualizaciones de seguridad.

¿Porqué Debian GNU/Linux?

Debian también presenta algunas características sustanciales importantes:

1) Carece de fines comerciales y no obedece a urgencias mercantiles.
2) Tiene un buen seguimiento de errores, problemas son arreglados en menos de 48 horas.
3) Desde el principio su principal prioridad es desarrollar un sistema operativo completo y confiable.
4) Es desarrollado por voluntarios en todo el mundo.

Cada nueva versión soporta nuevas arquitecturas de hardware, actualmente estan soportadas: Alpha, ARM, HP PA−RISC, Intel x86, Intel IA−64, Motorola 680x0, MIPS, MIPS (DEC), Power PC, IBM S/390, Sparc y actualmente están por soportar Sun UltraSparc y SuperH de Hitachi siendo el sistema Linux que más arquitecturas soporta.

Dentro de los paquetes existentes en Debian tenemos varias herramientas para la detección de intrusiones en tiempo real que detectan comportamientos hostiles en una conexión, se suelen clasificar de 2 tipos, los que monitorean intentos de ataque a toda una red o los que solo monitorean las actividades de un host determinado.

* Herramientas de host

Utilizamos la herramienta PortSentry para detectar escaneo de puertos, TripWire para detectar modificaciones a los archivos de sistema y LogSentry para el análisis de bitácoras; siendo el primero y el último parte de la suite de herramientas llamada TriSentry de Psionic Technologies.

Detección de Escaneo de Puertos

El sistema PortSentry vigila los puertos de nuestro sistema y ejecuta una acción (generalmente un bloqueo) en caso de detectar un intento de conexión a un puerto que no queremos sea escuchado.

Su página principal se encuentra en http://www.psionic.com/products/portsentry.html y está disponible para sistemas Solaris, BSD, AIX, SCO, Digital Unix, HP−UX, y Linux.

En Debian puede instalarse tecleando la instrucción:

apt−get install portsentry

Se pueden especificar diferentes niveles de actividad, el modo clásico, stealth y avanzado, toda la configuración se encuentra en el archivo /usr/local/psionic/portsentry/portsentry.conf

Las principales opciones las consulte directamente de un artículo de José Torres Luque en la revista ES Linux Magazine y son las siguientes:

TCP_PORTS, aquí se ponen los puertos a logear tanto para el modo clásico como para el stealth. El autor del programa propone tres listas distintas de puertos según el grado de sensibilidad que queramos aplicar. El máximo de puertos es 64.

UDP_PORTS, este es un equivalente al anterior pero para puertos UDP.

ADVANCED_PORTS_TCP, ADVANCED_PORTS_UDP, indican el rango máximo del puerto a usar para el modo advanced. Todo puerto inferior al indicado será monitorizado salvos los que ya vimos que eran excluidos. El rango máximo puede ser definido hasta el 65535. Aunque no se recomienda exceder de mas de 1024 pues podría generar falsas alarmas.

ADVANCED_EXCLUDE_TCP, ADVANCED_EXCLUDE_UDP, son una lista de exclusión de puertos, todo los que aqui se pongan no serán tenidos en cuenta a la hora de monitorear en el modo avanzado. Se ponen puertos típicos de conexión que sean habituales por clientes remotos y en los que no se este ofreciendo un servicio real. Por ejemplo: ident

IGNORE_FILE, Aqui especificamos el archivo donde incluiremos las IPs que no tendremos en cuenta al momento de monitorear, en el también se debería poner las IP de los interfaces locales incluyendo el "lo". Se podría también incluir las IPs locales.

KILL_ROUTE, aqui podemos poner el comando a ejecutar para bloquear accesos del host atacante. p/e: iptables −I INPUT −s $TARGET$ −j DROP aqui $TARGET$ sirve para hacer referencia al host atacante.

KILL_RUN_CMD, indicamos un comando a ejecutar antes que se bloquee el acceso al host atacante.

SCAN_TRIGGER, define a los cuantos intentos hará saltar la alarma.

PORT_BANNER, muestra un mensaje en los puertos abiertos con el modo connect.

Una vez configurado tenemos que ejecutarlo en alguno de los 3 modos, para esto se puede elegir las opciones: para TCP tenemos −tcp (modo básico), −stcp (modo stealth) y −atcp (avanzado), para UDP tenemos −udp, −sudp, −audp.

Análisis de Integridad

El sistema TripWire permite monitorear la integridad de los archivos del sistema, su página principal se encuentra http://www.tripwire.org/ y está disponible para el sistema operativo Linux y de manera comercial para Windows NT, Solaris, AIX y HP−UX.

En Debian puede instalarse tecleando la instrucción:

apt−get install tripwire

Se utilizan dos claves para almacenar la información, la primera "site key" se utiliza para cifrar los archivos de políticas y configuración, la "local key" se utiliza para cifrar la información que muestra el estado de los archivos que son monitoreados.

La configuración se realiza de manera sencilla en el archivo /etc/tripwrie/twpol.txt y una vez modificado se "instala" tecleando la instrucción:

twadmin −m P /etc/tripwire/twpol.txt

Para generar la base de datos inicial con el estado actual de los archivos ejecutamos la instrucción:

tripwire −m i 2

Para verificar la integridad del sistema de archivos ejecutamos la instrucción:

tripwire −m c

El archivo de configuración puede ser borrado para que un posible intruso no pueda ver que archivos son revisados por lo que ejecutamos la siguiente instrucción:

rm /etc/tripwire/twcfg.txt /etc/tripwire/twpol.txt

Para crearlos en caso de ser necesario tecleamos la instrucción:

twadmin −m p > /etc/tripwire/twpol1.txt twadmin −m f > /etc/tripwire/twcfg.txt

Análisis de Bitácoras

El sistema LogCheck forma parte de LogSentry, nos permite hacer una revisión de bitácoras de manera más efectiva pues clasifica y genera reportes de las actividades y errores que realmente se deben consultar, lo hace en 4 niveles: ignorar, actividad no usual, violación de seguridad y ataque.

Su página principal se encuentra en http://www.psionic.com/products/logsentry.html y está disponible para sistemas Solaris, BSD, HP−UX y Linux.

En Debian puede instalarse tecleando la instrucción:

apt−get install logcheck

Instala el programa logtail en /usr/local/bin para mantener un registro de que logs ya han sido analizados, también instala los siguientes archivos:

Logcheck.sh,
Es un script que incluye la configuración básica.

Logcheck.hacking,
Contiene las reglas para identificar los niveles de actividad.

Logcheck.ignore,
Contiene expresiones que no deben reportarse.

Logcheck.violations,
Contiene expresiones que pueden considerarse como violaciones de seguridad.

Logcheck.violations.ignore,
Ignora las expresiones que se encuentren en este archivo.

Para programar el reporte de logs podemos crear un cron que corra el programa cada hora: 0 * * * * /bin/sh /usr/local/etc/logcheck.sh

Herramientas de red

Utilizamos la herramienta Snort para registrar los intentos de ataque a nuestra red. Su página principal se encuentra http://www.snort.org/ y está disponible para BSD, Solaris, AIX, Irix, Windows, MacOS y Linux. En Debian puede instalarse tecleando la instrucción:

apt−get install snort

Funciona en tres modos, como sniffer, packet logger y como detector de intrusos.

Tiene los siguientes parámetros:

−l directorio
Indicamos el directorio donde se almacenarán los archivos.

−h IP
Especificamos el IP de nuestra red que queramos monitorear.

−b
Captura todos los paquetes en forma binaria.

−r archivo
Procesa un archivo binario.

Modo Sniffer y Packet Logger de Snort

En modo sniffer lee todos los paquetes que pasan por la red y los muestra en consola, en modo packet logger envía los datos a un archivo dentro de un directorio.

Snort −v

Muestra el IP y las cabeceras.

Snort −dv

También muestra los datos que pasan.

Snort −dev

De manera más detallada.

Modo Detección de intrusos de Snort

En este modo nos informará de escaneos de puertos, ataques de denegación de servicio, ejecución de exploits, etc. Basándose en reglas especificadas en el archivo /usr/local/share/snort estas reglas pueden ser descargadas

de la página principal y son actualizadas del servidor cada hora aproximadamente.

Su configuración es tan sencilla como modificar el archivo snort.conf donde especificamos los detalles de nuestra red y directorios de trabajo, se modificó solamente la IP:

var HOME_NET IP

Para ejecutar snort tecleamos la instrucción:

snort −c snort.conf

Los archivos de registro se almacenan en /var/log/snort donde podemos ver las IPs atacantes. Por supuesto esta es una revisión básica de lo que podemos hacer con Snort, te recomiendo que revises más documentación ya que es una herramienta excelente que, por cierto, ha sido comparada por revistas y grupos de seguridad recomendándola como la mejor herramienta de detección de intrusos para cualquier plataforma Unix y Windows. Existe soporte comercial por empresas como Silicon Defense y Source Fire así como interfaces gráficas que empiezan a surgir para una mejor y más estética presentación de resultados.

En algunas ocasiones surgen emergencias que no fueron contempladas con anterioridad y tienen que resolverse de manera inmediata. Estos problemas generalmente son ocasionados por personas malintencionadas o intrusos que intentan acceder por algún motivo a nuestros servidores, desde robar o alterar nuestra información hasta atacar a otros equipos desde el nuestro, desde instalar un programa sniffer o algún rootkit.

Otras Herramientas Utiles

Detección de sniffers

Un sniffer es una herramienta que pone en modo promiscuo nuestra interfaz de red con la intención de capturar todo el tráfico que pasa por la red, el comando ifconfig nos muestra información completa sobre nuestra interfaz:

eth0 Link encap:Ethernet HWaddr 00:50:BF:1C:41:59
inet addr:10.45.202.145 Bcast:255.255.255.255 Mask:255.255.128.0
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:7180 errors:0 dropped:0 overruns:0 frame:0
TX packets:4774 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:100
RX bytes:8122437 (7.7 MiB) TX bytes:294607 (287.7 KiB)
Interrupt:10 Base address:0xc000

Pero si el comando ifconfig fue sustituido o el sniffer se encuentra situado en otra máquina de la red es necesario monitorear las conexiones al exterior, por ejemplo el envío de e−mail a cuentas extrañas o detectar logs del sniffer.

Existe una herramienta llamada neped creada por un grupo de hackers españoles la cual nos informa sobre las interfaces de red que se encuentran en modo promiscuo dentro de nuestra red, no forma parte de Debian pero puede ser descargado de ftp://apostols.org/AposTools/snapshots/neped/neped.c

Nota: Estas últimas semanas ha permanecido caído su servidor.

Al ejecutar el programa obtendremos un resultado similar a lo siguiente:

```
neped eth0
−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−
> My HW Addr: 00:50:BF:1C:41:59
> My IP Addr: 192.168.0.1
> My NETMASK: 255.255.255.0
> My BROADCAST: 192.168.1.255
−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−
Scanning ....
* Host 192.168.0.2, 00:C2:0F:64:08:FF **** Promiscuous mode detected !!!
End.
```

Al enviar un paquete IP desde 191.168.0.1 hacia 192.168.0.2 necesitamos conocer su dirección MAC, para esto se envía un paquete broadcast a toda la red preguntando la dirección MAC del IP especificado, todos los equipos de la red escuchan la petición pero solo responde el host destino.

En este caso neped realiza una petición para cada IP asignada en la red pero no broadcast sino a una dirección IP inexistente. Solo los hosts con su interfaz en modo promiscuo contestarán esta petición pues son los únicas capaz de ver esos paquetes.

Este programa lo conocí por un artículo de detección de espías que encontré por la red e incluía un ejemplo similar a este, si alguien sabe el sitio Internet donde se encuentra el artículo envieme la dirección por correo electrónico porque la perdí :−)

Detección de rootkits

Los RootKits es un método para obtener más privilegios de los asignados a un usuario, generalmente sustituyen archivos binarios de nuestro sistema operativo por versiones propias para conservar el acceso posterior al sistema, por lo que es necesario verificar si tenemos los originales, para esto nos ayudamos de la herramienta chkrootkit que puede ser instalado con la instrucción:

```
apt−get install chkrootkit
```

Su página principal está ubicada www.chkrootkit.org y verifica los siguientes archivos:

aliens, asp, bindshell, lkm, rexedcs, sniffer, wted, z2, amd, basename, biff, chfn, chsh, cron, date, du, dirname, echo, egrep, env, find, fingerd, gpm, grep, hdparm, su, ifconfig, inetd, inetdconf, identd, killall, ldsopreload, login, ls, lsof, mail, mingetty, netstat, named, passwd, pidof, pop2, pop3, ps, pstree, rpcinfo, rlogind, rshd, slogin, sendmail, sshd, syslogd, tar, tcpd, top, telnetd, timed, traceroute, w, write

Esta herramienta es invocada tecleando:

```
chkrootkit
```

Haciendo la verificación de archivos y buscando posibles sniffers y paquetes de rootkits conocidos. Tiene otras herramientas que se utilizan para verificar alteración en los archivos de logs (chkwtmp y chklastlog) así

como el programa ifpromisc para verificar si nuestra interface de se encuentra en modo promiscuo.

Algunas Referencias

Te recomiendo consultes las páginas man de los programas, también te proporciono algunas referencias que consulté, por favor no dejen de mandarme sugerencias y comentarios a mi correo electrónico.

- Alexander Reelsen, Securing Debian How To, version 1.4, 18 Febrero 2001
- Anónimo, Linux Máxima Seguridad, Pearson Educación, Madrid 2000
- Brian Hatch, Hackers en Linux, Mc Graw Hill 2001
- Jim Mellander, A Stealthy Sniffer Detector, Network Security
- Antonio Villalón Huerta, Seguridad en Unix y redes, Open Publication License, octubre 2000
- CSI FBI Computer Crime and Security Survey, CSI Issues&Trends, Vol.7
- Who's Sniffing Your Network?, www.linuxsecurity.com/articles/intrusion_detection_article−798.html

---

2005−01−10, generated by lfparser_pdf version 2.51