Preparación 1

- Al Investigador forense se le deberá de proporcionar acceso físico al sistema sospechoso.

- Puede ser necesario contar con una copia física del disco duro con propósitos de forensia y de evidencia. Finalmente, puede ser necesario un acceso físico para desconectar la máquina sospechosa de cualquier red.

- Se precisa de un buen conocimiento de la actividad usual de la máquina/servidor en la red. Usted debe de tener un archivo en lugar seguro donde se describa la actividad usual de puertos para poder comparar eficientemente con el estado actual.

- Puede ser de gran ayuda tener un buen conocimiento de los servicios que corren usualmente en la máquina. No dude en pedir ayuda a un experto en Unix/Linux si lo considera necesario.. Es una buena idea tener un mapa de los servicios y procesos que se ejecutan en la máquina.

- Tenga una lista actualizada de todos los archivos críticos (especialmente archivos SUID y GUID) y guárdela en un lugar seguro fuera de la red o incluso en papel. Con esta lista, usted puede fácilmente separar los archivos SUID habituales y detectar los inusuales.

- Tenga un mapa de su actividad de puertos usual así como las reglas de tráfico.

Identificación 2

Cuentas inusuales
Busque cualquier entrada sospechosa en ***/etc/passwd***, especialmente con UID 0. También vea en ***/etc/group*** y ***/etc/shadow***.
Busque los archivos huérfanos que podrían haber sido dejados al borrar una cuenta utilizada en el ataque:
 # find / \ (-nouser -o -nogroup \) -print

Archivos inusuales
- Busque todos los archivos SUID y GUID:
 # find / -uid 0 \ (-perm -4000 -o -perm 2000 \) -print
- Busque los nombres de archivos extraños, comenzando con ".", " .. " o " ".

Identificación 2

 # find / -name "*" -print
 # find / -name ".*" -print
 # find / -name "..*" -print
- Busque archivos de gran tamaño (en este caso que superen los 10 MB)
 # find / -size 10 MB -print
- Busque procesos que se ejecuten desde o hacia archivos que no estén "linkeados":
 # lsof +L1

Busque archivos inusuales en /proc y /tmp. Este último directorio es uno de los preferidos por los atacantes para almacenar datos o binarios maliciosos.

Servicios inusuales
(Sólo Linux) Ejecute ***chkconfig*** (si está instalado) para comprobar si todos los servicios están habilitados:
 # chkconfig - list

Revise los procesos en ejecución (recuerde que un rootkit puede cambiar los resultados en todo este documento, especialmente aquí!).
 # ps -aux

Utilice **lsof -p** ***[pid]*** sobre procesos desconocidos

Usted debe de reconocer los procesos habituales y ser capaz de deducir cuáles podrían haber sido añadidos por el atacante.
Preste especial atención a los procesos que se ejecutan bajo el UID 0.

Actividad inusual de red
Trate de detectar sniffers en la red mediante varias formas:
Busque en los archivos de log del kernel si hay interfaces que hayan entrado en modo promíscuo, algo así como "*kernel: device eth0 entered promiscuous mode*"

Use **# ip link** para detectar el flag "PROMISC". Prefiera este método sobre **ifconfig**, puesto que **ifconfig** no funciona en todos los kernels.
Busque actividad en los puertos: **# netstat -nap** y **# lsof -i** para obtener más información sobre los procesos que estén escuchando en los puertos.
Busque entradas MAC inusuales en su LAN:
 # arp -a
Busque direcciones IP inesperadas en la red.

Identificación 2

Tareas automáticas inusuales
Busque trabajos inusuales programados por los usuarios mencionados en ***/etc/cron.allow***. Preste especial atención a los trabajos de **cron** programado por cuentas con UID 0 (root): **# crontab -u root -l**
Busque cron inusuales que tengan como alcance todo el sistema: **# cat /etc/crontab** y **# ls -la /etc/cron.***

Entradas inusuales de log
Busque eventos sospechosos, incluyendo las siguientes:
Gran número de errores de autenticación/login local o por herramientas de acceso remoto (sshd, ftpd, etc)
Programas con Llamadas a Procedimiento Remoto (RPC) con entradas de log que incluyen gran número de caracteres extraños
Un gran número de errores en el registro de Apache
- Reinicios (de hardware)
- Reinicio de aplicaciones (reinicio Software)
Casi todos los archivos de registro se encuentran en /var/log en la mayoría distribuciones de Linux. Estas son las principales:
/var/log/message: mensajes en general y otros relacionados con el sistema
/var/log/auth.log: Registros de autenticación
/var/log/kern.log: Registros del kernel
/var/log/cron.log: Registros de crond (cron)
/var/log/maillog: Registros del servidor de correo
/var/log/httpd/: Registro de acceso y errores de Apache
/var/log/boot.log: Registro de arranque del sistema
/var/log/mysqld.log: Registro del servidor de base de datos MySQL
/var/log/secure: Entrada de autenticación
/var/log/utmp o **/var/log/wtmp**: Registro de login
Para ver los logs, las herramientas como cat y grep pueden ser útiles:
cat /var/log/httpd/access.log | grep "GET / signup.jsp"

Entradas inusuales en el log del kernel

- Busque eventos sospechosos en el log del kernel usando:
 # dmesg
- Liste toda la información importante del kernel y del sistema:
 # lsmod
 # lspci
- Busque rootkits conocidos (use **rkhunter** o similares)

Hashes de archivos
Verifique que todos los binarios en /bin, /sbin, /usr/bin, /usr/sbin o cualquier otro lugar de almacenamiento correspondan con sus MD5 respectivos. (use AIDE o similar)

ATENCIÓN: esta operación podría cambiar todas las marcas de tiempo de los archivos. Esto sólo debe hacerse después que se hayan llevado a cabo todas las demás investigaciones y que sepa que puede alterar estos datos.
En los sistemas con RPM, utilice:
rpm -Va | sort
En algunos Linux, se puede utilizar un script llamado ***check-packages***.
En Solaris: # pkg_chk-vn
En Debian: debsums ac-

Contención 3

•Respalde todos los datos importantes de la máquina comprometida, si es posible con una copia física bit a bit del disco duro entero en un soporte externo. Sin cree necesario haga también una copia de la memoria (RAM) del sistema investigado..

Si la máquina no se considera crítica para la organización y se puede desconectar, apague la máquina bruscamente: desenchufe. Si se trata de una computadora portátil con una batería, sólo presione el botón "off" durante unos segundos hasta que el equipo apague.

Las investigaciones “offline” deben iniciarse inmediatamente si el paso de identificación no dio ningún resultado pero el sistema es todavía sospechoso de estar comprometido.

Trate de encontrar evidencias de todas las acciones del hacker: (usando como herramientas forenses Sleuth Kit / Autopsy por ejemplo)

•Busque todos los archivos utilizados por el atacante, incluyendo archivos borrados y vea lo que se ha hecho con ellos o al menos su funcionalidad, para evaluar la amenaza.
•Revise todos los archivos accedidos recientemente.
•Revise los logs.
•De manera más general, trate de encontrar cómo entró al sistema el atacante. Deben considerarse todas las pistas. Si no hay una prueba de la intrusión, no olvide que podría venir de un “insider”.
•Si es posible, aplique parches, para evitar el mismo tipo de intrusión, en caso que el atacante hubiera utilizado una vulnerabilidad ya arreglada.

Remedio 4

Temporalmente elimine todos los accesos a las cuentas implicadas en el incidente, y elimine todos los archivos maliciosos.

Recuperación 5

No importa lo lejos que el hacker haya penetrado en el sistema y el conocimiento que usted pueda tener sobre el compromiso, si el sistema ha sido penetrado, lo mejor es reinstalar el sistema completamente y aplicar todos los parches de seguridad.
En caso que esta solución no pueda aplicarse, usted deberá:
■ Cambiar todas las contraseñas del sistema, cuentas, y hacer que los usuarios lo hagan de manera segura: se deben usar contraseñas con mayúsculas/minúsculas, caracteres especiales, números, y por lo menos 7 caracteres.
■ Comprobar la integridad de todos los datos almacenados en el sistema, utilizando hashes MD5.
■ Restaurar todos los archivos binarios que podrían haber sido cambiados (ejemplo: /bin/su)

Repercusiones 6

Informe
Deberá de redactarse un informe de crisis que será distribuído entre todos los actores de la célula de manejo de crisis.

Deben de describirse los siguientes temas:
Causa inicial de la infección
Acciones y líneas de tiempo de cada evento importante
Qué salió bien
Qué salió mal
Costo del incidente

Capitalice
Deberán de definirse las acciones para mejorar los procesos de manejo de infecciones de gusanos para capitalizar esta experiencia.

Un aporte para:

Organización de los Estados Americanos

CICTE

IRM #3

Detección de Intrusión en Unix/Linux

Análisis en vivo sobre un sistema sospechoso

Autor IRM: CERT SG / Cedric Pernet
Versión IRM: 1.3
email: cert.sg@socgen.com
web: http://cert.societegenerale.com
Traducción: Francisco Neira
email: neira.francisco@gmail.com
Twitter: @neirafrancisco

Extracto

Esta “Metodología de Respuesta a Incidentes” (IRM, por sus siglas en inglés) es una hoja resumen dedicada a los manejadores de incidentes que investigan un asunto de seguridad específico. Quién debe de usar estas hojas IRM?

- Administradores
- Centro de Operaciones de Seguridad (SOC)
- CISOs y sus delegados
- CSIRT (equipos de respuesta a incidentes informáticos)

Recuerde: Si usted afronta un incidente, siga el IRM, tome notas y no pierda el control. Contacte su CSIRT inmediamente si es necesario.

Pasos del manejo de incidentes

Se definen 6 pasos para manejar los incidentes de seguridad:

- Preparación: Alistarse para manejar el incidente
- Identificación: Detectar el incidente
- Contención: Limitar el impacto del incidente
- Remedio: Remover la amenaza
- Recuperación: Recobrar a una etapa normal
- Repercusiones: Delinear y mejorar el proceso