METODOLOGÍA DE RESPUESTA A INCIDENTES

IRM #3 DETECCIÓN DE INTRUSIÓN DE LINUX/UNIX

Análisis en vivo en un Sistema sospechoso.

Autor IRM: CERT SG
Contribución: CERT a Dvens / Paloma Vargas
Versión del IRM: 2.0
E-Mail: cert.sg@socgen.com
Web: https://cert.societegenerale.com
Twitter: @CertSG

Traducción al Español

Paloma Amilene Vargas Alvarado
E-Mail: amilenhalvarado@gmail.com
Twitter / X: @AmileneVargas

CONTENIDO

1. ABSTRACTO

Esta metodología de respuesta a incidentes, es una hoja de consulta dedicada a los encargados que investigan un problema preciso de seguridad.

¿QUIÉN DEBE UTILIZAR HOJAS IRM?

- Administradores.
- Centro de Operaciones de Seguridad.
- CISO y adjuntos.
- CERT (Equipo de respuesta ante emergencias informáticas).

Recuerde: Si se enfrenta a un incidente, siga el IRM y tome notas. **Mantenga la calma** y, si es necesario, contacte inmediatamente con el equipo de Respuesta a Incidentes o el CERT de su línea de negocio.

2. PASOS PARA LA GESTIÓN DE INCIDENTES

SE DEFINEN 6 PASOS PARA GESTIONAR INCIDENTES DE SEGURIDAD

1. **Preparación**: prepárese para manejar el incidente
2. **Identificación**: detectar el incidente
3. **Contención**: limitar el impacto del incidente
4. **Remediación**: eliminar la amenaza
5. **Recuperación**: recuperarse a una etapa normal
6. **Lecciones aprendidas**: elaborar y mejorar el proceso

IRM proporciona información detallada para cada paso del proceso de respuesta a incidentes. Los pasos provienen de la Guía de Gestión de Incidentes de Seguridad Informática del NIST.

2.1 PREPARACIÓN

OBJETIVO: ESTABLECER CONTACTOS, DEFINIR PROCEDIMIENTOS, REUNIR INFORMACIÓN PARA AHORRAR TIEMPO DURANTE UN INCIDENTE.

Despliegue una solución EDR en endpoints y servidores.

- Esta herramienta se convirtió en una de las piedras angulares de la respuesta a incidentes en caso de ransomware o compromiso a gran escala, facilitando las fases de identificación, contención y remediación.
- Lance la Búsqueda EDR y el escaneo AV con reglas explícitas de IOC y obtenga los primeros indicadores para el seguimiento del progreso de la remediación.
- Establezca sus políticas EDR en modo de prevención.

En ausencia de EDR, se debe dar acceso físico al sistema sospechoso al investigador forense. Se prefiere el acceso físico al acceso remoto, ya que el hacker podría detectar las investigaciones realizadas en el sistema (por ejemplo, mediante el uso de un sniffer de red).

Podría ser necesaria una copia física del disco duro para fines forenses y de evidencia.
Si es necesario, podría ser necesario el acceso físico para desconectar la máquina sospechosa de cualquier red.

Se necesita un buen conocimiento de la actividad de red habitual de la máquina/servidor. Debe tener un archivo en un lugar seguro que describa la actividad de puertos habitual, para comparar de manera eficiente con el estado actual.
Se necesita un buen conocimiento de los servicios habituales. No dude en pedir ayuda a un Experto en Unix/Linux, cuando sea aplicable.

- Utilice Auditd y Logs de Linux como logs del sistema, mensajes y logs de aplicaciones (Apache, NGINX, ...).
- Utilice AppArmor, por ejemplo.

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

Tenga un mapa de su actividad de puertos/reglas de tráfico habitual.

2.2 IDENTIFICACIÓN

OBJETIVO: DETECTAR EL INCIDENTE, DETERMINAR SU ALCANCE E INVOLUCRAR A LAS PARTES APROPIADAS.

Cuentas Inusuales

- Busque cualquier entrada sospechosa en /etc/passwd, especialmente con UID 0. Revise también /etc/group y /etc/shadow.

- Busque archivos huérfanos, que podrían haber sido dejados por una cuenta eliminada 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 nombres de archivos extraños, que comiencen con “.“or “..“ or ““:

```
# find / --name " *" --print
# find / --name ". *"
# find / --name ".. *" --print
```

- Busque archivos grandes (aquí: más grandes que 10MB):

```
# find / -size +10MB --print
```

- Busque procesos que se ejecutan desde o hacia archivos que han sido desenlazados (unlinked):

```
# lsof +L1
```

Busque archivos inusuales en /proc y /tmp. Este último directorio es un lugar de elección para que los hackers almacenen datos o binarios maliciosos.

Servicios Inusuales

Ejecute chkconfig (si está instalado) para verificar todos los servicios habilitados:

```
# chkconfig --list
```

Mire los procesos en ejecución (recuerde: un rootkit podría cambiar sus resultados para todo en este documento, ¡especialmente aquí!):

```
# ps -aux
```

Use lsof -p [pid] en procesos desconocidos.

Debe conocer sus procesos en ejecución habituales y ser capaz de determinar qué procesos podrían haber sido añadidos por un hacker. Preste especial atención a los procesos que se ejecutan bajo UID 0.

Actividad de Red Inusual

- Intente detectar sniffers en la red utilizando varias formas:
  - Mire sus archivos de log del kernel en busca de interfaces que entren en modo promiscuo, como:
    "kernel: device eth0 entered promiscuous mode"
  - Use # ip link para detectar el indicador "PROMISC".

- Busque actividad de puertos inusual:

  # netstat -nap y
  # lsof -i

- Busque entradas MAC inusuales en su LAN:
  # arp -a

- Busque direcciones IP inesperadas o nuevas en la red:
  # netstat -ntaupe
  # netstat -ant
  # watch ss -tt

Tareas Automatizadas Inusuales.

- Busque trabajos (jobs) inusuales programados por usuarios mencionados en /etc/cron.allow. Preste especial atención a los trabajos cron programados por cuentas UID 0 (root):
  # crontab -u root -l

- Busque trabajos cron inusuales de todo el sistema:
  # cat /etc/crontab
  # ls -la /etc/cron.*

Entradas de Log Inusuales

Busque a través de los archivos de log en el sistema en busca de eventos sospechosos, incluyendo lo siguiente:

- Gran número de fallos de autenticación/inicio de sesión desde herramientas de acceso local o remoto (sshd, ftpd, etc.)
- Programas de Llamada a Procedimiento Remoto (RPC) con una entrada de log que incluye una gran cantidad de caracteres extraños...
- Un gran número de logs de Apache que mencionan "error"
- Reinicios (Reboots) (reinicio de Hardware)
- Reinicio de aplicaciones (reinicio de Software)

Casi todos los archivos de log se encuentran en el directorio /var/log en la mayoría de las distribuciones de Linux. Aquí están los principales (las rutas pueden variar según las distribuciones):

- /var/log/message: Mensajes generales y cosas relacionadas con el sistema
- /var/log/auth.log: Logs de autenticación
- /var/log/kern.log: Logs del kernel
- /var/log/cron.log: Logs de Crond (trabajo cron)
- /var/log/maillog: Logs del servidor de correo
- /var/log/httpd/: Directorio de logs de acceso y error de Apache
- /var/log/boot.log: Log de arranque del sistema
- /var/log/mysqld.log: Archivo de log del servidor de base de datos MySQL
- /var/log/secure: Log de autenticación
- /var/log/utmp o /var/log/wtmp: Archivo de registros de inicio de sesión
- /var/log/syslog: Log de cron, actividad de samba y más
- /root/.*history: Historial de comandos del usuario root
- /home/*/.*history: Historial de comandos de los usuarios

Para buscar a través de los archivos de log, herramientas como cat y grep pueden ser útiles:

```
# cat /var/log/httpd/access.log | grep "GET /signup.jsp"
```

Entradas Inusuales Del Registro del Núcleo.

- Revisa los archivos del registro del núcleo en el sistema en busca de eventos sospechosos:
  # dmesg

Enumera toda la información importante del kernel y del sistema:

```
# lsmod
# lspci
```

- Buscar rootkits conocidos (userkhunter y herramientas similares).

Hashes de archivos.

Verifica todos los hashes MD5 de tus binarios en /bin, /sbin, /usr/bin, /usr/sbin o cualquier otro lugar donde se almacenen binarios. (usa AIDE u otra herramienta similar)

ADVERTENCIA: esta operación probablemente cambiará todas las marcas de tiempo de los archivos. Esto solo debería hacerse después de que se hayan completado todas las demás investigaciones y sientas que puedes alterar estos datos.

- En sistemas con RPMinstaled, use:
  # rpm–Va|sort

- En algunas distribuciones de Linux, se puede usar un script llamado check-packages.

- En Solaris:
  # pkg_chk–vn

- En Debian:
  # debsums–ac

- En OpenBSD (no realmente esto pero de todos modos):
  # pkg_delete-vnx

2.3 CONTENCIÓN

OBJETIVO: MITIGAR LOS EFECTOS DEL ATAQUE EN EL ENTORNO.

Realizar una copia de seguridad segura de la información crítica del equipo comprometido, siempre que sea posible, utilizando una copia física bit a bit del disco duro completo en un medio externo. Asimismo, generar una copia de la memoria (RAM) del sistema, la cual podrá ser analizada posteriormente si resulta necesario.

▪ Aislar el equipo comprometido mediante la solución EDR y proceder a la inspección de otros equipos y redes.

O bien

▪ Aislar el equipo utilizando el firewall o los switches de red.

Si el equipo no se considera crítico para la operación de la empresa y puede ser desconectado, deberá apagarse de forma forzada retirando el cable de alimentación. En el caso de una computadora portátil con batería, mantener presionado el botón de encendido durante algunos segundos hasta que el equipo se apague por completo.

Las investigaciones fuera de línea deberán iniciarse de inmediato si, durante la fase de identificación, no se obtuvo ningún resultado concluyente, pero el sistema continúa siendo sospechoso de estar comprometido.

Intentar identificar evidencias de todas las acciones realizadas por el atacante (utilizando herramientas forenses como Sleuth Kit / Autopsy, por ejemplo):

- Identificar todos los archivos utilizados por el atacante, incluyendo archivos eliminados, y analizar qué acciones se realizaron sobre ellos o, al menos, su funcionalidad, con el fin de evaluar el nivel de amenaza.
- Revisar todos los archivos accedidos recientemente.
- Analizar los archivos de registro (logs).
- De manera general, intentar determinar cómo el atacante obtuvo acceso al sistema. Todas las posibles líneas de investigación deben ser consideradas. Si no se encuentra evidencia técnica de la intrusión, no debe descartarse la posibilidad de que el incidente haya sido provocado por un usuario interno.
- Aplicar las correcciones necesarias cuando sea posible, para prevenir incidentes similares en el futuro, especialmente si el atacante explotó una vulnerabilidad conocida que ya cuenta con una solución disponible.

2.4 REMEDIACIÓN

OBJETIVO: TOMAR ACCIONES PARA ELIMINAR LA AMENAZA Y EVITAR FUTUROS INCIDENTES.

ADVERTENCIA. SOLO COMIENCE LA REMEDIACIÓN UNA VEZ QUE ESTÉ 100% SEGURO DE HABER DEFINIDO BIEN EL ALCANCE Y CONTENIDO EL PERÍMETRO, A FIN DE EVITAR QUE EL ATACANTE LANCE ACCIONES DE REPRESALIA.

Elimine temporalmente todos los accesos de las cuentas involucradas en el incidente y elimine los archivos maliciosos.

2.5 RECUPERACIÓN

OBJETIVO: RESTAURAR EL SISTEMA A SUS OPERACIONES NORMALES.

Sin importar qué tanto haya penetrado el atacante en el sistema ni el conocimiento que usted pueda tener sobre el compromiso, siempre que un sistema haya sido vulnerado, la mejor práctica es **reinstalar el sistema por completo y aplicar todas las correcciones de seguridad.**

En caso de que esta solución no pueda aplicarse, usted debería:

- Cambiar todas las contraseñas de las cuentas del sistema y hacer que sus usuarios lo hagan de manera segura.
- Verificar la integridad de todos los datos almacenados en el sistema, utilizando hashes de archivos (por ejemplo, $SHA\text{-}256$).
- Restaurar todos los binarios que pudieran haber sido modificados (Ejemplo: /bin/su).
- Reemplazar todos los paquetes comprometidos por versiones seguras.

2.6 LECCIONES APRENDIDAS

OBJETIVO: DOCUMENTAR LOS DETALLES DEL INCIDENTE, DISCUTIR LAS LECCIONES APRENDIDAS Y AJUSTAR LOS PLANES Y LAS DEFENSAS.

Informe

Se debe redactar un informe de crisis y ponerlo a disposición de todos los actores del incidente.

Se deberán describir los siguientes temas:

- Causa inicial de la infección
- Acciones y cronogramas de cada evento importante
- ¿Qué salió bien?
- ¿Qué salió mal?
- Costo del incidente
- Indicadores de compromiso

Capitalizar

Se deben definir acciones para mejorar los procesos de gestión de detección de intrusiones en Unix/Linux para capitalizar esta experiencia.

3. DEFINICIONES

CONCEPTO	DESCRIPCIÓN
IRM	Metodología de Respuesta a Incidentes
CISO	Chief Information Security Officer (ejecutivo responsable de la seguridad de la información)
CERT	Equipo de Respuesta a Emergencias Informáticas.
EDR (Endpoint Detection and Response)	Solución que debe desplegarse en puntos finales y servidores, facilitando las fases de identificación, contención y remediación en casos de ransomware o compromisos a gran escala.
IOC (Indicators of Compromise)	Reglas explícitas utilizadas para la búsqueda EDR y el escaneo AV para obtener los primeros indicadores y seguir el progreso de la remediación.
Acceso Físico	El método de acceso preferido para el investigador forense en un sistema sospechoso, ya que el acceso remoto permite que el atacante detecte las investigaciones (por ejemplo, mediante un sniffer de red).
Auditd y AppArmor	Herramientas recomendadas para usar en la fase de Preparación; Auditd se utiliza para recopilar registros de Linux (sistema, mensajes y aplicaciones).
SUID (Set-User-ID) y GUID (Set-Group-ID) files	Archivos críticos cuya lista actualizada debe almacenarse en un lugar seguro para facilitar la detección de archivos SUID inusuales. Su búsqueda es una tarea de identificación.
UID 0 (User ID 0)	El identificador de usuario root (administrador), que implica el nivel más alto de privilegios. Se debe prestar especial atención a las entradas en /etc/passwd y a los procesos o trabajos cron que se ejecuten con este UID.
Archivos huérfanos	Archivos que podrían haber sido dejados por una cuenta eliminada utilizada en el ataque.
/proc y /tmp	Directorios que deben revisarse en busca de archivos inusuales; /tmp es un lugar común para

	que los hackers almacenen datos o binarios maliciosos.
Rootkit	Software malicioso capaz de alterar los resultados de herramientas de identificación (como ps –aux) para ocultar la actividad del atacante en el sistema.
Sniffers (de red)	Herramientas utilizadas para intentar detectar tráfico malicioso. Se detectan observando los registros del kernel en busca de interfaces que entren en modo promiscuo.
Modo promiscuo	Un estado del dispositivo de red que indica que está escuchando todo el tráfico que pasa por él. Su detección (PROMISC flag en # ip link) es un indicador de actividad inusual.
RPC (Remote Procedure Call)	Programas de Llamada a Procedimiento Remoto, cuya actividad inusual en los registros, como entradas con un gran número de caracteres extraños, puede ser una señal de alerta.
/var/log	Directorio principal donde se ubican casi todos los archivos de registro en la mayoría de las distribuciones de Linux.
Hashes MD5/SHA256	Valores de verificación de integridad de archivos. Se utilizan para verificar que los binarios del sistema (como los de /bin, /sbin, etc.) no hayan sido modificados.
AIDE	Herramienta recomendada para verificar los hashes MD5 de los binarios del sistema.
RPM (Red Hat Package Manager)	Sistema de gestión de paquetes. El comando `# rpm –Va.
Copia física bit a bit del disco duro/Memoria (RAM)	Tareas de contención crítica. Se realiza una copia de seguridad segura de los datos importantes y una copia forense de la memoria (RAM) del sistema para investigaciones posteriores.
Sleuth Kit/Autopsy	Herramientas forenses que se utilizan para investigaciones fuera de línea (una vez contenido el sistema) para encontrar evidencias de las acciones del atacante, incluidos los archivos eliminados.

Reinstalación completa del sistema	La mejor práctica recomendada para la Recuperación si un sistema ha sido comprometido, junto con la aplicación de todas las correcciones de seguridad.