Procedimientos de actuación en Incidentes

IRIS-CERT <cert@rediris.es>

Martes 14 de Noviembre 2000

Capítulo 1

El ciclo de vida de un incidente

Los incidentes de seguridad graves suelen consistir en:

1. Se produce un ataque a una máquina mal administrada
2. Desde esa máquina se ataca a otras máquinas
3. Llega un aviso (desde el exterior de los ataques) o bien el administrador "descubre" que su máquina ha sido atacada.
4. El administrador procede a solucionar los problemas que ha encontrado y volver a dejar el equipo operativo
5. Si es posible se avisa a los responsables de la institución origen del ataque

Capítulo 2

Un ataque típico

1. Se realizan escaneos para detectar vulnerabilidades en equipos
2. Mediante un exploit el atacante consigue acceso con privilegios del administrador al equipo.
3. Se instalan puertas falsas y troyanos para ocultar el ataque.
4. Se ataca a otros equipos

Capítulo 3

La “recuperación” ante un ataque

Dos opciones:

- Contactar con los servicios legales de la institución y dejar el caso en manos de las autoridades policiales
  - Si se han producido graves perjuicios
  - Lo más importante es “no tocar” el sistema.
  - Contactar con la guardia civil /policía nacional
- Solucionar el incidente y volver a funcionar
  - incidentes “leves” (equipos no críticos)
  - Seguir los pasos indicados en la guia

En cualquier caso es conveniente actuar rápidamente para evitar daños mayores y siempre comunicar a las instancias oportunas la información del ataque.

Capítulo 4

Pasos en la recuperación del incidente

- Desconectar el equipo de la red
- Realizar una copia a bajo nivel de los datos
- Recoger la información sobre el ataque
- Analizar la información
- Restaurar el sistema y aplicar medidas de seguridad
- Contactar con los responsables de los equipos implicados

Capítulo 5

Copia de Datos

- Permite analizar el estado del sistema en el momento del ataque
- En caso de que exista alguna "bomba lógica" es posible recuperar los datos
- Si se descubren evidencias de la identidad del atacante es más fácil presentarlas como pruebas
- Emplear comandos a bajo nivel para duplicación (las utilidades del S.O. modifican el S.O. dd es muy útil en estos casos

```
dd if = /dev/hda1 of =discoc
```

o

```
dd if=/dev/hda of =/dev/hdc
```

Capítulo 6

Buscar información sobre el atacante

Para buscar programas modificados:

- Idealmente: Tripwire instalado y base de datos externa, análisis a realizar en otro equipo “limpio”.
- Muchas veces: Mismo equipo (problema: rootkit en el núcleo), pero tenemos la base de datos de paquetes instalados.
  - En RedHat rpm -Va
  - En Solaris pkgchk -v
- Otras opciones: Comparación con binarios de la instalación original o con los binarios de otros equipos no atacados

- IMPORTANTE: Los comandos del S.O. pueden haber sido modificados, es conveniente utilizar binarios compilados estáticamente, de un equipo “limpio”.

Capítulo 7

Buscar información sobre el atacante II

Los atacantes suelen instalar programas en directorios ocultos, buscar:

- Directorios de configuración de usuario ".prog" demasiado grandes
- Directorios y ficheros ASCII en "/dev"
- Directorios con nombres extraños "...", " ..",
- Ficheros transferidos por ftp
- ficheros con permisos de setuid y setguid

el comando find es tu amigo (si no es un troyano ;-):

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

Capítulo 8

Buscar información sobre el atacante III

Buscar información en los ficheros de log, depende de la configuración de cada S.O. y de como este configurado el syslog (/etc/syslogd.conf), buscar:

- En los ficheros de messages "/var/log/messages", "/var/adm/messages"
- En los ficheros de accesos "wtmpx", "utmpx"
- En los mensajes del núcleo (puesta en marcha de la tarjeta en modo promiscuo"
- Emplear el coroner toolkit para buscar ficheros borrados
- Modificaciones en los ficheros de configuración, nuevos usuarios, etc.
- Ver ficheros de comandos ejecutados por los usuarios ".bash_history"

Capítulo 9

Envío de los ficheros

Para la comunidad académica IRIS-CERT puede analizar los ficheros encontrados esto permite:

- Comprobar el atacante ha podido tener acceso a otras máquinas
- Analizar las tendencias y ver los métodos empleados por los atacantes
- Comprobar que vulnerabilidades se están produciendo
- Relacionar incidentes (igualdad de procedimientos, programas,etc.)

Para esto es importante:

- Avisar a IRIS-CERT y rellenar el formulario situado en http://www.rediris.es directorio /cert/servicios/iris-cert/incidentes/formulario.txt
- Comunicar a los responsables de la institución el ataque.
- Si los ficheros son muy grandes, dejarlos en el ftp anónimo de RedIRIS.