Resumen de Operaci'on de IRIS-CERT

- Estad'isticas y tendencias de ataques.
  - Estad'isticas.
  - Formulario de incidentes.
  - Descripción de ataques.
    * Accesos a root
    * Ataques distribuidos.
- Resumen de reuniones
  - FIRST
  - Coordinación Europea (Cert Coord)

Estadisticas

Aumento muy significativo del número de incidentes reportados, con respecto al año pasado.

1. Incidentes totales desde Enero de 2000: 257

2. Incidentes por máxima prioridad alcanzada:

    - Informativos: 40
    - Baja: 90
    - Normal: 98
    - Alta:29
    - Emergencia 0

Tipos de incidentes

- Escaneos: 82
- SPAM: 54
- Accesos a root: 24
- Denegaciones de servicio: 10
- Intentos de acceso, controles remotos: 32
- Otros (abusos, falsificaciónes, etc..): 55

Gr’afica

Gestión de Incidentes. Problemas

Falta de puntos de contacto.

Rapidez en la actuación.

Obtención de la información del incidente y envio de la misma.

Tiempo medio incidente: más de una semana.

Formulario de incidentes

En “http://www.rediris.es/cert/formulario.txt” esta un formulario a rellenar en caso de incidente.

Las acciones a realizar suelen ser:

- Parar el ataque.
- Comprobar como se ha producido
- Comprobar que ha modificado el atacante
- Restablecer el sistema.

Es Vital el contactar cuanto antes y responder r’apidamente a los mensajes, para localizar a mas equipos “atacados”.

Como detectar binarios modificados

De mayor a menor fidelidad:

- Comprobación en equipo externo con base de datos previa externa (Tripwire)
- Comprobar base de datos externa en el mismo equipo (Tripwire)
- Comprobar base de datos interna (si la hay).(rpm en Linux, pkg en Solaris): rpm -Va
- Ver cadenas en binarios "clave".
- Comparar tamaños con otros binarios del mismo S.O.

¿Que enviar?

- Información del equipo.
  - ¿Para que se usa ?
  - Sincronismos de fecha.
- Logs.
- Binarios encontrados y/o modificados.
- Ficheros de history de comandos, logs de los ataques,etc.

Si la información es mayor de 1MB, dejar los ficheros en

Incidente A

Equipos empleado en ataques de denegación de servicio.

Incidente producido tras el “BOOM” de las noticias sobre este tipo de ataques.

Dificil de detectar (falsificación de Dirección origen)

Incidente B

Servidor empleado para ataques DOS.

- Equipo “multiproposito”.
- Imposible de Apagar.
- Saturación de troncal

Incidente C

- Varios accesos root en poco tiempo a diversas máquinas.
- Procedencia y métodos de entrada distintos.
- Detección externa e interna.
- Equipos sin mantener!!!, estaciones de trabajo.

sniffit

```
-----------------------------------------------
 Origen   : Equipo1.organización,es (XX.XX.XX.XX ][
 Destino  : equipo2. (YYY.YYY:YYY:YYY) [110]
 Sesion   : pop-3
 Inicio   : Fecha   2000
 Duracion : 0:00:02 secs.
 Datos    : 96 bytes Conexiones activas: 1
-----------------------------------------------
+OK QPOP (version 2.52.C) at YYY.YYY.YYY.YYY starti
USER usaurio
PASS clave
STAT
LIST

-----------------------------------------------
....
```

Problema con las claves

1. NO DEBE HABER PASSWD EN CLARO POR LA RED.

2. NO DEBE HABER PASSWD EN CLARO POR LA RED.

3. EXISTE EL SSH (ahora ya lo tienen hasta los router cisco ;-) www.ssh.net

4. CASI CUALQUIER TIPO DE CONEXI'ON SE PUEDEN "TUNELIZAR"

5. EXISTEN OTROS MECANISMOS DISTINTOS DEL POP

6. SEGMENTAR LA RED.

En Resumen

- ¿Por qué no se actualizan las máquinas ?, ¿Que hace falta ?

- ¿Donde esta la información al usuario sobre como configurar su máquina ?

- ¿Quien es el responsable de lo que ocurra en una máquina ?, ¿Lo sabe el usuario que usa esa dirección IP ?, ¿Qué medidas se toman ?

Reunión Tecnica de FIRST

FIRST: Forum of Incident Response and Security Team.

Temas tratados:

- Estado de los Cert en Europa.
- Seguridad en NT
- Problemas del fraude telefónico.

Cordinación Europea

Problemas de coordinación en Europa:

- Muchos paises/lenguas/legislaciones
- Diversos tipos de grupos Redes Academicas/ISP
- Escaso interes oficial.

Desde 1991 hay intentos de coordinación

EuroCert

Duración: 1997-1999

tres fases:

- Marzo 97: Soporte grupos de seguridad.
- Mayo 98: Coordinación (reenvio) de incidentes.
- Coordinación de incidentes completa 8-(no realizada).

Financiado por 11 Redes acad'emicas.

Coordinación de CERTs

Inicio en Septiembre de 1999.

Auspiciado por Terena, pero con participación de ISP. http://www.terena.nl/projects/cert

Mision Fundamental: Conservar y mantener las relaciones de seguridad ("Web of Trust") existentes, categorizados en niveles.

Encargo a de un "validador externo" de mantener y revisar estos niveles.

Otros proyectos de CERT-Coord

Otras iniciativas presentadas han sido:

- Clasificación de incidentes de seguridad.
  - ¿Que es un incidente de seguridad ?
  - ¿Que tipos hay? : Taxonomia
  - ¿Como poder intercambiar estadisticas ?
- Base de datos de contactos (whois de RIPE)