Resumen Reunión FIRST 1999

IRIS-CERT <cert@rediris.es>

8 de septiembre de 1999

Resumen

Resumen de las reunión de 11 Reunión de FIRST, sobre todo resumen de las charlas y exposiciones que se realizaron durante la conferencia.

Índice General

La documentación de la reunión del FIRST impresa es muy extensa, sin embargo de algunas de las sesiones dejaron enlaces a las URL donde se podría obtener la información, que en este caso iré comentando.

La reunión duro cinco días, los temas que se trataron en cada uno de ellos son:

1 Lunes 14

Hubo dos sesiones paralelas, una sobre "inseguridad informática (Blak Hat session) y otra sobre peritaje informático y actuación en temas judiciales ("computer Forensic'.

El tutorial de "Black Hat", vino a ser una un tutorial de "hacking" y como se suelen explotar las vulnerabilidades en las configuraciones de los sistemas a la hora de conseguir acceso a estos. Fue bastante largo, las transparencias se pueden obtener de La página del autor[1] en formatos ps y pdf.

La sesión de "computer Forensic" estuvo centrada en la legislación Americana/inglesa, centrándose por parte de los ponentes en casos legales ocurridos en Australia, tratando otros aspectos de la recuperación de datos no relacionados precisamente con la seguridad en redes, recuperación de ficheros borrados (¡¡utilizando las utilidades Norton!!), etc..

A ultima hora de la tarde hubo dos sesiones más, una sobre nuevos enfoques en los virus en código móvil por parte de la empresa finjan soft[2] y el ciac[3]. En las páginas web de estas entidades hay información sobre virus, aunque no están estas exposiciones.

La otra conferencia fue impartida por miembros del CERT/CC sobre como averiguar quien es el responsable de una determinada dirección IP, siguiendo el documento que el propio CERT/CC tiene sobre como averiguar los puntos de contacto[4]. Por ultimo se trataron los distintos problemas que están surgiendo con el uso de nuevas tecnologías como ip móvil e IP sin cable, la venta de dominios/rangos etc. a la hora de comprobar a quien pertenece una determinada dirección IP

2 Martes 15

Esta jornada empezó con la inaguración oficial de la reunión, discursos de políticos y los organizadores locales, después hubo durante todo el día varias exposiciones sobre los siguientes temas:

- La autoridad de certificación DFN-PCA[5] y SurNet-PCA[6].
- Panel (exposición) sobre los grupos de seguridad en Asia.
- "Asegurar redes e instalaciones informáticas", en el sentido de compañía de seguros que te asegura por cierto valor tus instalaciones contra

[1] http://www.belgers.com/walter/first
[2] http://www.finjan.com
[3] www.ciac.org
[4] http://www.cert.org/tech_tips/finding_site_contacts.html
[5] http://www.pca.dfn.de/dfnpca
[6] http://www.surfnet.nl/pca

ataques externos.

- Comentarios de Wietse Venema estadísticos sobre el porcentaje de errores en código fuente que siguen apareciendo y a que son debidos, etc.

- Por la tarde una una sesión en la que se comento la evolución de los incidentes de seguridad del año pasado relativos a los ataques contra servidores DNS con Linux, haciendo una exposición cronológica de los hechos.

Por ultimo en la reunión que hubo de "tormenta de ideas"estuvimos tratando varios grupos académicos Europeos la posibilidad de presentar un proyecto a la Unión Europea sobre seguridad.

3 Miercoles 16

Durante este día se desarrollaron mesas redondas y exposiciones, los temas que se trataron en las mesas redondas fueron:

- ¿ Que necesitan saber el personal encargado de responder a incidentes de seguridad sobre el mundo de los hackers, cultura,etc.

- Evolución de los equipos de atención de incidentes en los últimos 10 años.

En cuanto a las exposiciones, los temas fueron:

- Manejo de las vulnerabilidades, como indicárselas a los fabricantes, etc.

- Empleo del SAINT (Satan actualizado)[7].

- Problemas de seguridad en los modem ASDL y equipos de usuario que están continuamente conectados a internet.

- Agentes inteligentes para la detección de ataques, intrusiones y obtención de la información tras un ataque. por parte del CERT-KR[8].

[7]http://www.wwdsi.com
[8]http://certcc.or.kr

4 Jueves 17

Como el día anterior, exposiciones y mesas redondas, los temas tratados:

- Gestión de incidentes de seguridad.
- Software automático para informar de incidentes de seguridad.
- Mesa redonda sobre seguridad en general.
- Tutorial sobre SSH
- Tutorial sobre Gestión de riesgos, problemática de seguirad,etc.

Por la tarde fue la asamblea del FIRST donde se aprobaron las actas de las reuniones anteriores, y sobre todo:

- Se aprobó una cuota anual de 500 dolares por grupo de seguridad, destinada a pagar una secretaría permanente que gestione las tareas administrativas del FIRST, con una pequeña rebaja posterior a dos miembros de cada organización que acudan a las reuniones.
- Se Renovó la junta directiva, aunque prácticamente quedo como estaba, entrando Roger Safian de la Northwestern University en lugar de Stephen Hansen.
- Después en la reunión posterior se produjo el cambio de "chairman/presidente"de la organización, quedando de presidente Miguel Sanchez de SGI, que se estaba ocupando antes de los temas economicos.

5 Viernes 18

Prosiguieron los tutoriales sobre SSH y gestión de riesgos, además hubo un tutorial sobre la creación de equipos de respuesta a incidentes de seguridad (IRT) por parte de miembros del Grupo de incidentes del Departamento de Energía Americano[9]

[9]http://ciac.llnl.gov