Bisoños Usuarios de GNU/Linux de Mallorca y Alrededores | Bergantells Usuaris de GNU/Linux de Mallorca i Afegitons

Los principales incidentes de seguridad segun el CERT. (10337 lectures)

Per **Carlos Cortes Cortes**, ***carcoco*** (http://bulma.net/~carcoco/)

Creado el 27/09/2001 11:07 modificado el 27/09/2001 11:07

> Cada trimestre el **CERT**, publica un informe sobre los principales ataques, que son reportados al equipo de respuesta ante incidentes del propio CERT. Acaban de sacar el correspondiente al 3 trimestre del 2001 ...

En el mismo podemos encontrar los que se consideran los **7 incidentes** mas destacados, dando al mismo tiempo enlaces para solucinar estos problemas. Como podeis ver la mayoria relacionado con los **inseguros sistemas windows**. Aunque a mi se me ocurren otras opciones, para solucionar de una vez por todas los problemas con estos *sistemas*.

"Since the last regularly scheduled **CERT summary**, issued in May 2001 (CS-2001-02), we have seen several self-propagating worms, as well as active exploitation of vulnerabilities in Solaris in.lpd, BSD telnet daemon and Microsoft IIS by intruders. In addition, we have seen an increase in intruder activity directed at home users."

1. "Code Red" / "Code Red II" worms
2. "Code Red" Worm Crashes IIS 4.0 Servers with URL Redirection Enabled
3. W32/Sircam Malicious Code
4. Buffer Overflow in telnetd
5. Buffer Overflow in Sun Solaris in.lpd Print Daemon
6. Continuing Threats to Home Users
7. W32/Leaves Exploitation of previously installed SubSeven Trojan Horses

Una posible y razonable solucion a estos problemas:

- 1,2,3,7 -> Usar Linux/BSD/Unix's/Mac OS X
- 4 -> Usar OpenSSH
- 5 -> Usar lpr-ng, cups o actualizar lpd
- 6 -> Iptables/Ipchains/IP Filter

Sumario del 3 trimestre del año 2001 del CERT:
http://www.cert.org/summaries/CS-2001-03.html[1]

¿Que es el CERT?
CERT significa **Equipo de Respuesta para Emergencias Informáticas** (Computer Emergency Response Teams) y es una institución de la Universidad **Carnegie Mellon**, dedicada a recibir y transmitir información sobre situaciones de riesgo en sistemas de computadoras, tales como agujeros de seguridad, técnicas de ataques de hackers, etc. Proporciona tambien asistencia para reestablecerse y rastrear los pasos de un hacker después de un ataque. Siendo el CERT, un autentico punto de referencia en temas de seguridad a nivel mundial.
"The CERT is a center of Internet security expertise, at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University. We study Internet security vulnerabilities, handle computer security incidents, publish security alerts, research long-term changes in networked systems, and develop information and training to help you improve security at your site."
Más información en http://www.cert.org[2]

2 articulos relacionados con **unix**, aunque existe abundante e interesante documentacion en la web del CERT:
http://www.cert.org/tech_tips/unix_configuration_guidelines.html[3]
http://www.cert.org/tech_tips/win-UNIX-system_compromise.html[4]

La version **española** del **CERT**, parece que se ha quedado sin subvenciones y subsiste como puede: http://escert.upc.es/[5]

--
Carlos Cortes (aka carcoco)
http://bulma.net/todos.phtml?id_autor=132 [6]

Lista de enlaces de este artículo:

1. http://www.cert.org/summaries/CS-2001-03.html
2. http://www.cert.org
3. http://www.cert.org/tech_tips/unix_configuration_guidelines.html
4. http://www.cert.org/tech_tips/win-UNIX-system_compromise.html
5. http://escert.upc.es/
6. http://bulma.net/todos.phtml?id_autor=132

E-mail del autor: carcoco _ARROBA_ gmail.com