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

SANS actualiza el top20 (6977 lectures)

Per **Javi Polo**, ***DrSlump*** (http://drslump.org)

Creado el 05/10/2001 14:12 modificado el 05/10/2001 14:12

El instituto SANS ha actualizado la lista de las 20 vulnerabilidades más críticas que hay hoy en dia en internet

El Instituto SANS[1] (System Administration, Networking and Security) actualizó el dia 2 de Octubre de 2001 la lista top20[2], que describe las que ellos consideran hoy en dia las vulnerabilidades más grandes que hay a dia de hoy joden la marrana en internet ;)

El resumen de esta lista es:

1. Vulnerabilidades comunes
   - Instalaciones por defecto de Sistemas Operativos y aplicaciones
   - Cuentas que no tienen password o el password es muy debil
   - La falta de backups (o backups incompletos)
   - Gran cantidad de puertos abiertos
   - Falta de filtrado de tráfico para comprobar que este entra/sale desde las direcciones IPs correctas
   - Falta de logs o logs incompletos
   - CGIs vulnerables
2. Fallos del mundo Windows
   - El fallo del unicode (IIS)
   - Buffer Overflows en las extensiones ISAPI de IIS
   - Exploits para Remote Data Services (RDS) de IIS
   - Falta de protección de los shares Netbios
   - Obtención de información por métodos que no requieren de autentificación
   - Hashing pobre en SAM
3. Fallos de UNIX
   - Buffer Overflows en los servicios de RPC
   - Fallos de Sendmail
   - Debilidades del DNS Bind
   - Comandos "r" (rlogin, rsh, ...)
   - Fallos en el lpd
   - sadmind y mountd
   - Uso de communitys por defecto en SNMP

De la primera parte podemos extraer que

- los fallos "de toda la vida" siguen presentes,
- que hay mucho administrador vago que deja las máquinas "out of the box", o, "así como se instala se queda",
- que la gente no se preocupa por los fallos implícitos en el protocolo IP (por ejemplo, al no comprobarse si la dirección de un paquete que viene de nuestra red tiene en la cabecera IP una IP de nuestra red, facilitamos el hecho de que se pueda usar nuestra red para hacer IP Spoofing, algo bastante malo ;))
- Una de las vias de intrusión más comunes son los CGIs mal programados

La parte de windows la obviaremos, a fin de cuentas, esto es una asociación de usuarios de linux, si los winusers tienen problemas, que se busquen la vida XD. Un buen lugar para empezar puede ser NtBugTraq[3]

Por otra parte, de los ataques típicos a UNIX podemos ver que tampoco ha cambiado mucho la cosa:

- Se atacan fallos conocidos de toda la vida (sendmail, rpc, bin, mound, lpd)
- Sigue habiendo administradores vagos que no cambian las configuraciones por defecto, no actualizan el software, siguen usando métodos de acceso remoto TOTALMENTE INSEGUROS, como los famosos "comandos r", habiendo para ellos sustitutos mucho más seguros, como ssh

En resumen, parece que aunque aparezcan fallos nuevos, el panorama sigue igual ...

Lista de enlaces de este artículo:

1. http://www.sans.org
2. http://www.sans.org/top20.htm
3. http://www.ntbugtraq.com

E-mail del autor: javipolo _ARROBA_ drslump.org
Podrás encontrar este artículo e información adicional en: http://bulma.net/body.phtml?nIdNoticia=888