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

Ayuda para interpretar los logs de un firewall (9318 lectures)

Per **Celso González**, ***PerroVerd*** (http://mitago.net)

Creado el 29/08/2001 10:48 modificado el 29/08/2001 10:48

> *Hemos instalado nuestro firewall y vemos que en nuestros logs aparecen muchas líneas a puertos que desconocemos y no sabemos si nos estan atacando o es una cosa normal. En este documento[1] (en inglés) nos explica de una forma muy muy muy detallada que significa cada una de estas líneas.*

El documento empieza con una descripción de los números de puertos, nos indica cuales son los que se pueden tener un tráfico normal, cuales son los programas que los suelen emplear, o que troyanos emplean ese puerto.
Esta es la parte fuerte del documento y la que mayor extensión ocupa

Aparte de esto tenemos información acerca de los paquetes ICMP, interpretar logs de algunos programas especiales (DNS, httpd, identd...), interpretar direcciones IP, descripción de los problemas que podemos tener al filtrar demasiado ;-), técnicas para filtrar correctamente y una descripción en detalle del netbios.

Resumiendo, muy interesante

Lista de enlaces de este artículo:

1. http://www.robertgraham.com/pubs/firewall-seen.html

E-mail del autor: celso _ARROBA_ mitago.net
Podrás encontrar este artículo e información adicional en: http://bulma.net/body.phtml?nIdNoticia=825