https://info.nodo50.org/Cuidado-con-equivocarte-demasiadas.html

Cuidado con equivocarte demasiadas veces de contraseña

- Nodo50 - Noticias Técnicas -

Fecha de publicación en línea: MiÃ©rcoles 18 de mayo de 2011

En los servidores de Nodo50 usamos un sistema de seguridad para bloquear ataques de diccionario y de fuerza bruta. Este tipo de ataques consisten en probar múltiples combinaciones de nombres de usuari@ y contraseña hasta conseguir dar con la correcta. El objetivo de los atacantes es conseguir entrar a una cuenta de administración para tomar el control de un servidor, o entrar en una cuenta de correo para usarla para enviar spam, o usar una cuenta de FTP para subir a una web virus, scripts de envío de spam, páginas webs que imiten las de bancos para hacer phishing, etc.

El sistema que usamos contra este tipo de ataques consiste en detectar las direcciones IP desde donde se producen muchos fallos de identificación y bloquear esa IP en nuestro cortafuegos durante media hora o mas tiempo.

Estos bloqueos provocan que el ataque de fuerza bruta no sea efectivo pues impide probar muchas combinaciones de nombre+contraseña en poco tiempo.

Pero a veces se produce un efecto no deseado, se trata del bloqueo de usuari@s legítimos que se confunden de contraseña varias veces seguidas en poco tiempo. A veces ocurre en locales de organizaciones desde donde trabajan varias personas con varios ordenadores, afectando el bloqueo provocado por una persona a todas las que trabajan en la misma conexión a Internet (que por tanto para nuestro servidor tienen la misma IP).

En algunas ocasiones lo que ocurre es que en algún ordenador hay una cuenta de correo mal configurada, y el programa de correo reintenta la descarga de correo cada pocos minutos provocando el bloqueo.

Si sufres estos bloqueos notarás que el servidor deja de responder durante media hora y posiblemente varias veces al día, los programas de correo, FTP o navegadores te dirán que el servidor no responde.

Escríbenos a ayuda@nodo50.org o llámanos al 915488348 y te podremos dar pistas para ver donde está el problema (que cuenta de correo lo provoca, por ejemplo), para encontrar lo que provoca esos errores repetidos de identificación. También podremos poner tu dirección IP en una lista blanca de IPs que no deben bloquearse, es útil si tienes IP fija, aunque eso no quita que debas evitar esos intentos repetidos de identificación.

Referencias

- Ataque de fuerza bruta
- Ataque de diccionario