Bruteblock: Um detector de bruteforce.

Autoria de Daniel Bristot de Oliveira
18/08/2006
Última Atualização 18/08/2006

O BSDnews.com , anunciou hoje uma nova ferramenta, o brutelock(8).O bruteblock(8) é um detector de ataques de brute force, o programa basicamente analisa os logs do sistema a procura de possíveis ataques. Ao encontrar um ataque, ele bloqueia o cliente mal intencionado com uma regra no ipfw(8). O brutelock(8) utiliza expressões regulares ao analisar os logs, o que torna a aplicação flexível e customizável; outro fator relevante é o programa de ser escrito em C e não depender de aplicações externas para funcionar, pois as regras de firewall são manipuladas utilizando a API do ipfw(8).

O bruteblock está disponível no ports em security/bruteblock, veja mais detalhes sobre a aplicação neste link .