Pentest com Kali Linux

Instrutor:Vitor Mazuco

http://facebook.com/vitormazuco

Email:vitor.mazuco@gmail.com

WebSite:http://vmzsolutions.com.br

Prevenção de Sockstress

A única maneira de impedir completamente ataques sockstress é ir para o whitelist o acesso de serviços TCP. Isto não é prático na maioria das situações, por isso o melhor que pode ser feito é para avaliar as conexões limite com o iptables.

Para bloquear um IP depois que se abre mais de 10 conexões para a porta X em 30 segundos, instalar as seguintes regras do iptables:

Prevenção de Sockstress

```
# iptables -I INPUT -p tcp --dport 21 -m state --state NEW -m
recent –set

# iptables -I INPUT -p tcp --dport 21 -m state --state NEW -m
recent --update --seconds 30 --hitcount 10 -j DROP
```

Prevenção de Sockstress

Note-se que os ataques de sockstress ainda são possíveis mesmo com essas regras em vigor. O atacante só precisa de mais endereços IP para montar um ataque bem sucedido.