# Pentest com Kali Linux

**Instrutor:Vitor Mazuco**

**http://facebook.com/vitormazuco**

**Email:vitor.mazuco@gmail.com**

**WebSite:http://vmzsolutions.com.br**

## Ataque de Sockstress

O Sockstress é um método que é usado para atacar servidores na Internet e outras redes que utilizam as portas TCP, incluindo Windows, Mac, Linux, BSD e qualquer roteador ou outro aparelho de internet que aceita conexões TCP. O método faz isso por tentar usar os recursos locais, a fim de travar um serviço ou toda a máquina, essencialmente um ataque de negação de serviço consumindo muita memória RAM. Nosso alvo será o Metasploitable2, mas pode ser qualquer outro tipo de sistema Linux!

## Ataque de Sockstress

Criamos um script python, *sock_stress.py*, para executar um ataque de DoS de Sockstress. Para executar, faça o seguinte:

```
# python sock_stress.py 192.168.1.196 21 20
```

Agora, compare em um outro terminal a diferença de consumo de RAM que esse script faz antes e depois de sua aplicação.

```
~$ free -m
```

## Ataque de Sockstress

Esse programa, envia porções de 16 bits de comprimento. Cada bit pode ter um valor de 1 ou 0, a ser enviado pela porta TCP que está aberta, fazendo assim o servidor guardar na sua memória RAM, e podendo assim travar sua máquina por completo ou sua aplicação.

## Ataque de Sockstress

Depois de todos os recursos no sistema local foram esgotados, o sistema vai finalmente falhar. A quantidade de tempo necessário para completar este processo irá variar, dependendo da quantidade dos recursos locais disponíveis.

## Ataque de Sockstress

O programa é escrito para pegar o sinal de término transmitida como resultado ao pressionar Ctrl + C, e ele irá reparar as regras de iptables locais removendo as que foi gerado antes de matar a sequência de execução do script.