

Manual de instalação do programa **Spoofers** da **CAIDA** para teste de **anti-spoofing**. Esta é a ferramenta usada pelo pessoal do **MANRS** para avaliar se sua rede está bloqueando **spoofing de pacotes IPv4 e IPv6**. O **Spoofers** pode ser baixado dessa URL: <https://www.caida.org/projects/spoofers/>.

Podemos rodá-lo em interface gráfica ou de uma interface **CLI**. A vantagem de rodar em uma interface **CLI**, é que podemos configurar os testes em servidores GNU/Linux, periodicamente e de sub-redes diferentes. Importante para se manter bem nos **testes de conformidade** do **MANRS** mensalmente.

O **Spoofers** é dividido em **2 partes**, uma parte roda em background e a outra, a interface de teste que pode ser **GUI** ou **CLI**, se comunica com o serviço em background. Vamos ver primeiro a interface gráfica em um **GNU/Linux**. Em **Windows** pode ser mais simples tipo **next, next, finish**:

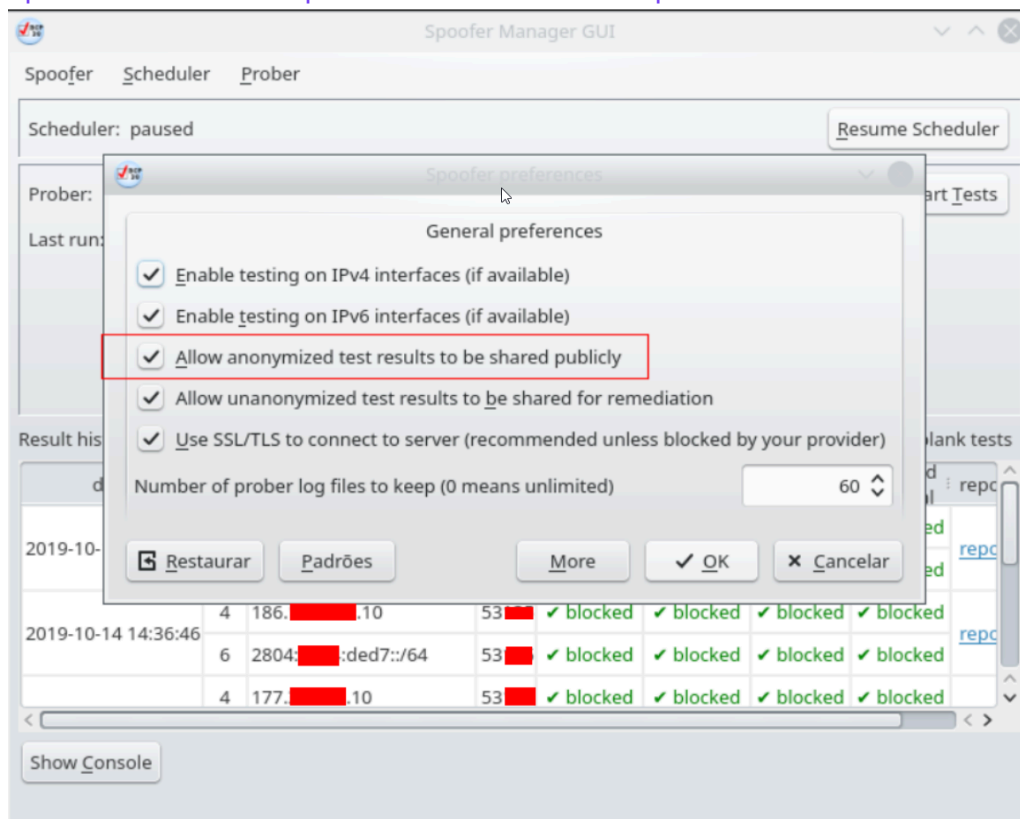
Primeiro rodamos o comando abaixo como root:

```
# spoofers-scheduler --daemon
```

Com seu usuário execute o comando abaixo:

```
$ spoofers-gui
```

Aparecerá uma tela parecida com esta e clique no **OK**:





Inicie o teste e o resultado precisa ser algo assim, com todas as colunas como **blocked**:

The screenshot shows the Spoofer Manager GUI with the following details:

- Spoofers:** Scheduler, Prober
- Scheduler:** ready (with a **Pause Scheduler** button)
- Prober:** next scheduled for 2019-10-21 15:43:31 -03 (in about 7 days) (with a **Start Tests** button)
- Last run:** 2019-10-14 14:36:46 -03
- Result history:**  Hide old blank tests

date	IPV	client address	ASN	outbound private	outbound routable	inbound private	inbound internal	report
2019-10-14 14:36:46	4	186. [redacted].10	53 [redacted]	✓ blocked	✓ blocked	✓ blocked	✓ blocked	<a href="#">report</a>
	6	2804: [redacted]:ded7::/64	53 [redacted]	✓ blocked	✓ blocked	✓ blocked	✓ blocked	
2019-10-14 14:30:36	4	177. [redacted].10	53 [redacted]	✓ blocked	✓ blocked	✓ blocked	✓ blocked	<a href="#">report</a>
	6	2804: [redacted]:ded6::/64	53 [redacted]	✓ blocked	✓ blocked	✓ blocked	✓ blocked	

O ideal é deixarmos um teste sempre rodando periodicamente e gerando relatórios no **CAIDA**. Para isso podemos pegar um GNU/Linux com IPv4 público e IPv6 global e usá-lo para gerar nossos relatórios. Estarei usando ainda um **Debian GNU/Linux** mas dentro do arquivo **INSTALL**, constam instruções de como compilar em outras distribuições GNU/Linux.

Faremos o seguinte:

```
# cd /usr/local/src/  
# wget -c https://www.caida.org/projects/spoofer/downloads/spoofer-1.4.13.tar.gz  
# tar xvfz spoofer-1.4.13.tar.gz  
# cd spoofer-1.4.13/  
# apt install build-essential libpcap0.8-dev libprotobuf-dev \  
protobuf-compiler libssl-dev qtbase5-dev scamper  
# ./configure  
# make  
# make install
```

Execute o comando:

```
# spoofer-scheduler --daemon
```

Depois edit o arquivo **/etc/xdg/CAIDA/Spoofer.conf** e na seção **[General]** adicione esses parâmetros:

```
sharePublic=true  
shareRemedy=true
```



No `/etc/crontab` adicione a seguinte linha que executará o Spoofer toda segunda-feira às 01:00:

```
00 1 * * 1 root /usr/local/bin/spoofer-prober -s1 -r1
```

Para que o daemon execute sempre que o sistema reiniciar, adicionaremos ele no `systemd`. Copie e cole comandos do bloco abaixo no shell como root:

```
cat << EOF > /etc/systemd/system/spoofer.service
[Unit]
Description=Executa o daemon spoofer
After=network.target

[Service]
Type=oneshot
ExecStart=/usr/local/bin/spoofer-scheduler --daemon
RemainAfterExit=yes

[Install]
WantedBy=multi-user.target
EOF
```

O bloco acima criará o arquivo `/etc/systemd/system/spoofer.service` e agora iremos habilitar o serviço para rodar:

```
# systemctl daemon-reload
# systemctl enable --now spoofer
```

Reinicie o sistema para verificar se tudo funcionou corretamente. Cheque fazendo um comando:

```
# ps afx|grep spoofer|grep -v grep
594722 ?        Ss      0:02  \_ spoofer-scheduler --daemon
```

Você pode procurar os resultados dos testes nessa URL passando o seu **ASN**: [https://spoofer.caida.org/recent\\_tests.php](https://spoofer.caida.org/recent_tests.php)