Instalando e usando o Proxychains

26 de abril de 2015 / Fnkoc

Eae galera, beleza? Hoje estarei escrevendo como instalar e utilizar o proxychains, porém não entrarei em configurações do mesmo, estaremos utilizando a configuração padrão.

O que é o Proxychains?

Proxychains permite que você utilize SSH, TELNET, VNC, FTP, e outras aplicações através de um servidor proxy HTTP(HTTPS) e SOCKS(4/5).

Qual a utilidade?

Suponhamos que você foi contratado por uma empresa para realizar uma auditoria de segurança no site da mesma. Dessa forma você irá fazer muitos testes e requisições podendo assim fazer com que o firewall te bloquei e você não tenha mais acesso ao site.
Ao utilizar um proxy mesmo que o firewall te bloqueie basta você trocar o endereço proxy para adiquirir um novo IP e prosseguir com seus testes.
No caso utilizaremos a rede TOR.

Achado uma utilidade para a ferramenta vamos ao que interessa, instalação e uso.

Utilizei uma distribuição baseada no Arch Linux, portante caso você siga os passos aqui basta você substituir o gerenciador de pacotes do Arch – Pacman – pelo gerenciador do Debian – APT – ou qualquer outra distro.

Instalação

1. Download e instalação TOR

```
pacman -S tor
```

2. Download e instalação do proxychains.

```
pacman -S proxychains
```

3. Inicialize o serviço tor

```
systemctl start tor
```

Usuários de distribuições Debian like devem utilizar o comando abaixo

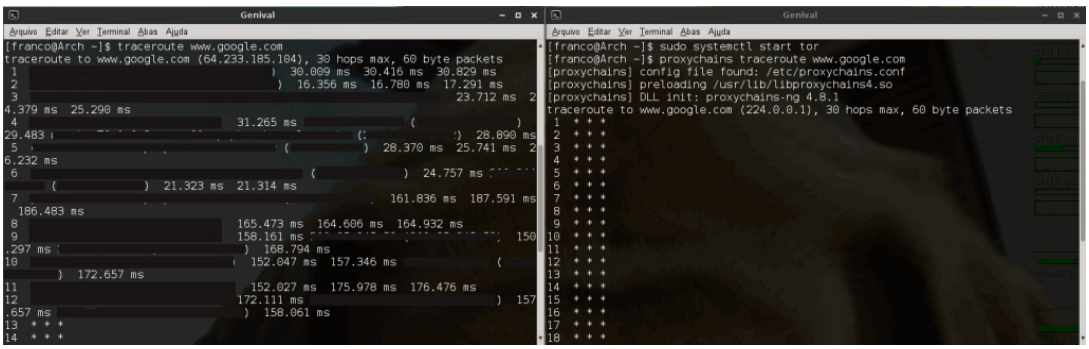
```
service tor start
```

4. Cheque o estado do serviço

```
systemctl status tor
```

Caso queira configurar o Proxychains ou o tor os arquivos se encontram em /etc/proxychains.conf e /etc/tor/torrc respectivamente.

5. Use o proxychains com alguma ferramenta, para que todo o tráfego da aplicação passe pela rede TOR. No caso utilizei o traceroute, mas vocês podem utilizar o Nmap, sqlmap, wpscan, entre outras.



Repare que quando o tráfego passa pelo TOR é impossível de se determinar o caminho percorrido até os servidores da Google (Imagem da direita).
Já com a internet limpa e sem nenhum tipo de criptografia é possível vermos todos os pulos dados até os servidores da Google

Espero que tenham gostado. Deixe sua opinião nos comentários.