Aula TP - 25/Fev/2019

Cada grupo deve colocar a resposta às perguntas dos seguintes exercícios na área do seu grupo no Github até ao final do dia 05/Mar/2019. Por cada dia de atraso será descontado 0,15 valores à nota desse trabalho.

Note que a máquina virtual disponibilizada pode ser utilizada para fazer estes exercícios.

Exercícios

1. TOR (The Onion Router)

Para este ponto necessita de instalar o tor, secure-delete, curl e anonsurf na conta do utilizador *user* na máquina virtual. Sugere-se que efetue a seguinte sequência de comandos:

```
sudo apt-get install tor secure-delete curl
```

```
cd ~/Tools
```

```
git clone https://github.com/Und3rf10w/kali-anonsurf.git
```

```
cd kali-anonsurf
```

```
sudo ./installer.sh
```

Note que se estiver a utilizar a máquina virtual disponibilizada para esta UC, é possível que estas ferramentas já estejam instaladas.

Experiência 1.1

Vamos utilizar o TOR (através do comando linha `anonsurf`) para mudarmos a nossa localização geográfica.

1. Abra o browser e vá a http://myiplocator.net/
    - Aponte o seu endereço IP e localização (também o pode obter através do comando `sudo anonsurf myip`)
2. Na linha de comando execute `sudo anonsurf start`
3. Faça reload (shift-reload) da página web onde se encontrava
    - Aponte o seu endereço IP e localização (note que se não mudou, é porque existiu algum erro)
4. Na linha de comando execute `sudo anonsurf change`
5. Faça reload (shift-reload) da página web onde se encontrava

- Aponte o seu endereço IP e localização (note que se não mudou, é porque existiu algum erro)

6. Na linha de comando execute `sudo anonsurf stop`
7. Faça reload (shift-reload) da página web onde se encontrava
   - Aponte o seu endereço IP e localização (note que se não é o inicial, é porque existiu algum erro)

Pergunta P1.1

Para aceder a alguns sites nos EUA tem que estar localizado nos EUA.

1. Efetuando o comando `sudo anonsurf start` consegue garantir que está localizado nos EUA?
2. Porquê? Utilize características do protocolo TOR para justificar.

Experiência 1.2

Vamos utilizar o "TOR Browser" para navegarmos anonimamente na rede. Para isso necessita de instalar o torbrowser-launcher na conta do utilizador *user* na máquina virtual.

Sugere-se que efetue a seguinte sequência de comandos:

> `sudo su`

> ```
> echo "deb http://deb.debian.org/debian stretch-backports main contrib" >
> /etc/apt/sources.list.d/stretch-backports.list
> ```

> `exit`

> `sudo apt-get update`

> `sudo apt-get install torbrowser-launcher`

> Na barra superior de menus da máquina virtual, vá a Applications / Internet / Tor Browser, de modo a finalizar a instalação do browser

> Se após finalizar a instalação o browser não abrir logo, volte a selecionar Applications / Internet / Tor Browser

Note que se estiver a utilizar a máquina virtual disponibilizada para esta UC, é possível que esta ferramenta já esteja instalada.

A. No browser TOR aceda à página https://blog.torproject.org/italian-anti-corruption-authority-anac-adopts-onion-services. Clique no lado esquerdo da barra de URL e verifique qual é o circuito para esse site.

B. Abra outro tab/pestana no browser TOR e aceda à página https://www.expressvpn.com/blog/best-onion-sites-on-dark-web/. Clique no lado esquerdo da barra de URL e verifique qual é o circuito para esse site.

Tire as suas conclusões.

Pergunta P1.2

No seguimento da experiência anterior, aceda a http://zqktlwi4fecvo6ri.onion/wiki/index.php/Main_Page ou https://www.facebookcorewwwi.onion/.

1. Clique no lado esquerdo da barra de URL e verifique qual é o circuito para esse site.
2. Porque existem 6 "saltos" até ao site Onion, sendo que 3 deles são "*relay*"? Utilize características do protocolo TOR para justificar.

Projeto de Engenharia de Segurança

Pode utilizar o resto da aula para o projeto de Engenharia de Segurança