# Aula TP - 26/Fev/2018

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/2018. Por cada dia de atraso será descontado 0,15 valores à nota desse trabalho.

Note que estes exercícios devem ser feitos na máquina virtual disponibilizada. Caso já tenha a versão da máquina virtual utilizada na última aula, não precisa de fazer download da nova versão.

## 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
```

#### Experiência 1.1

Vamos utilizar o TOR para mudarmos a nossa localização geográfica.

1. Abra o browser e vá a http://myiplocator.net/
    - Aponte o seu endereço IP e localização
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

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

esse site.

Tires 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 símbolo do Onion (cebola) do 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.

## 2. Projeto de desenvolvimento de software

Nas duas últimas aulas teóricas falou-se sobre vários técnicas, protocolos e aplicações criptográficas, pelo que chegou a altura de iniciar os projetos de desenvolvimento de software que tinham sido apresentados:

- Projeto 1 – Leilões online
  - Leilões online, com entrega de propostas em "carta fechada";
  - Pode ser uma extensão para software open source de leilões online.
- Projeto 2 – Gestor de passwords com base em QrCodes
  - Gestor de passwords, em que com base em QrCode apresentado pelo site, o telemóvel lê o QrCode e envia o user + password para desbloquear o acesso;
  - Pode ser uma extensão para software open source de gestão de passwords.

Nesta primeira fase, os dois grupos de projeto devem definir em traços gerais o projeto e as suas funcionalidades, e pensarem de que modo serão utilizado as técnicas criptográficas no projeto.

Com output desta fase, deverão ter um primeiro draft de etapas e fluxos de comunicação / mensagens, podendo utilizar como exemplo o formato visto no segundo exemplo do voto eletrónico, na aula teórica.