



Escola de Engenharia  
**Universidade do Minho**

DEPARTAMENTO DE ENGENHARIA INFORMÁTICA  
**Mestrado em Engenharia Informática**  
*Engenharia de Segurança*

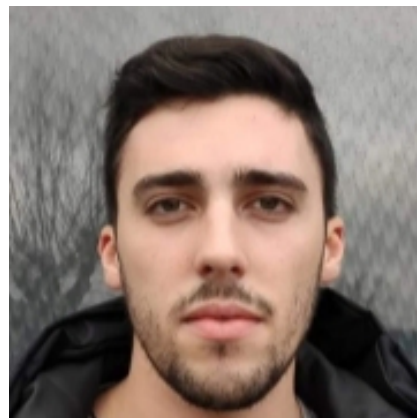
## *Aula 4*

**2 de Março de 2020**

## **Grupo 1**



Ricardo Pereira a73577



Tiago Ramires pg41101

Braga, 15 de Março de 2020

# 1. TOR (The Onion Router)

## Pergunta P1.1

1

Executando o comando *sudo anonsurf start*, não conseguimos garantir que o nodo de saída está localizado nos EUA.

2

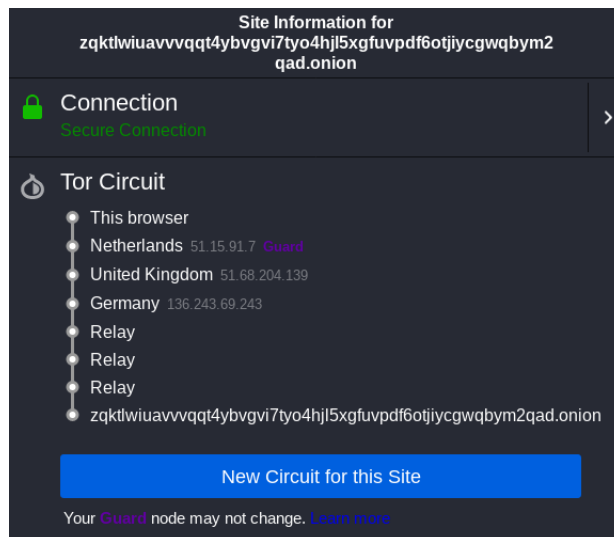
Garantir uma localização específica do nodo de saída é possível, mas através do *anonsurf*, que apenas redireciona toda a comunicação para um *proxy server tor*, torna-se impossível, pois por defeito o protocolo *TOR* mantém o anonimato do seu utilizador e para isso é criado um circuito com *Onion Routers* aleatórios que são constantemente alterados, de minuto em minuto. É possível saber as localizações geográficas onde estes circuitos se estabelecem mas a imparcialidade do *Onion Proxy* relativamente aos *Onion Routers* garante que os segundos são escolhidos de forma aleatória.

Para garantir uma localização específica utilizando o protocolo *TOR*, é necessário a utilização do próprio *TOR Browser* alterando o ficheiro *./browser/torbrowser/data/tor/torcc*, inserindo *'ExitNodes {us}'*, o que irá forçar a localização do último nodo para *USA*.

## Pergunta P1.2

1

Seguindo as instruções dadas, o circuito que se obtém é o seguinte.



**Figura 1.1:** *Tor Circuit* para [http://zqktlwi4fecvo6ri.onion/wiki/index.php/Main\\_Page](http://zqktlwi4fecvo6ri.onion/wiki/index.php/Main_Page)

## 2

Como se pode observar na figura anterior, existem 6 saltos neste circuito, sendo que os 3 primeiros são definidos pelo utilizador e os restantes definidos pelo servidor em questão. Inicialmente, o *OP* conecta-se a um *OR* na Holanda, depois a outro no Reino Unido e por fim a outro na Alemanha, havendo uma troca de chaves com os *OR*'s. Os outros três relays são nodos dos quais não se possui qualquer informação, precisamente para anonimizar aquilo que acontece do outro lado.

Faltam ainda criar pontos de *rendezvous*, sendo escolhidos determinados *introduction points* com base no *directory server*. O utilizador deve então escolher um *OR* como ponto de *rendezvous*, criando-se assim um circuito até este nodo. O utilizador envia ao *introduction point* informação acerca do ponto de *rendezvous*. Assim é criada uma ligação entre os nodos do cliente e os nodos do servidor, sendo que não é conhecida nenhuma informação de quem envia o quê.