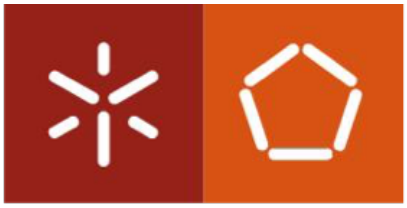

Universidade do Minho
Departamento de Informática
Mestrado Integrado em Engenharia Informática

Engenharia de Segurança: TP3

Aula 4

Diana Lopes, nº a74944
Gabriela Vaz, nº a74899

Conteúdo

Capítulo 1

TOR (*The Onion Router*)

Inicialmente, instalou-se o **tor**, **secure-delete**, **curl** e **anonsurf** na conta do utilizador *user* na máquina virtual, executando os 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

1.1 E1.1

Abrindo o *browser* e carregando a página `http://myiplocator.net/` obtém-se a informação apresentada na Figura 1.1.


Your IP Address is

193.137.92.69

[HIDE YOUR IP]

Your IP Details	
ISP:	Fundacao para a Ciencia e a Tecnologia, I.P.
City:	Braga
Region:	Braga
Country:	Portugal
Postal Code:	4700-000

Figura 1.1: Ponto 1 desta experiência.

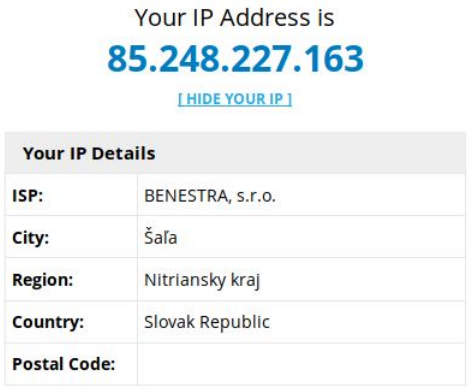

Figura 1.2: Ponto 3 desta experiência.

No terminal, executa-se o comando **sudo anonsurf start**. Fazendo *reload* da página `http://myiplocator.net/` obtém-se a informação apresentada na Figura 1.2.
No terminal, executa-se o comando **sudo anonsurf change**. Fazendo *reload* da página `http://myiplocator.net/` obtém-se a informação apresentada na Figura 1.3.

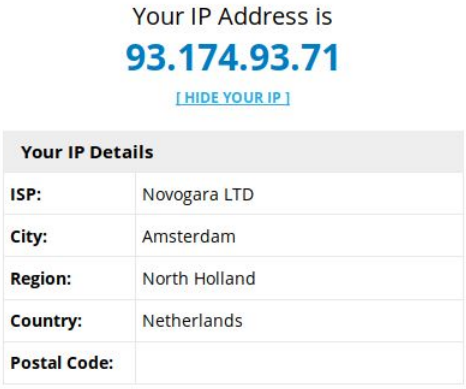

Figura 1.3: Ponto 5 desta experiência.

Por fim, executa-se o comando **sudo anonsurf stop** e faz-se **reload** da página `http://myiplocator.net/`, obtendo-se a informação apresentada na Figura 1.4, que coincide com a informação apresentada na Figura 1.1.

1.2 P1.1

Efetuando o comando **sudo anonsurf start** não conseguimos garantir que estamos localizados nos Estados Unidos. Um exemplo disso é a Figura 1.2 que é obtida após a execução deste comando. Isto deve-se ao facto de existirem três *onion routers* e não é possível escolher os *onion routers* por onde se passa. Assim, a localização muda sempre mas não pode ser escolhida.

Figura 1.4: Ponto 7 desta experiência.

1.3 E1.2

Inicialmente, instalou-se o **torbrowser-launcher** na conta do utilizador *user* na máquina virtual, executando-se os seguintes comandos no terminal:

- sudo su
- echo "deb http://deb.debian.org/debian stretch-backports main contrib» /etc/apt/sources.list.d backports.list
- exit
- sudo apt-get update
- sudo apt-get install torbrowser-launcher

No *browser* TOR acedeu-se à página `https://blog.torproject.org/italian-anti-corruption-authority-anac-adopts-onion-ser` Clicando no símbolo do Onion (cebola) do lado esquerdo da barra de URL e consegue consultar-se o circuito para este site, que pode ser consultado na Figura 1.5.

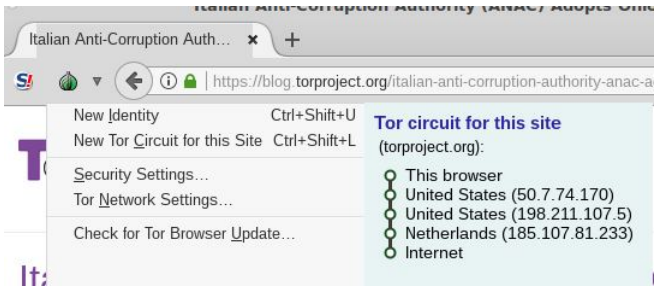

Figura 1.5: Circuito para o site `https://blog.torproject.org/italian-anti-corruption-authority-anac-adopts-onion-services`.

No mesmo *browser*, abriu-se uma nova *tab* para se aceder à página `https://www.expressvpn.com/blog/best-onion-sites-on-dark-web/`. Novamente, clicando no símbolo Onion (cebola), consultou-se o circuito para este site. Este circuito pode ser consultado na Figura 1.6.

Figura 1.6: Circuito para o site `https://www.expressvpn.com/blog/best-onion-sites-on-dark-web/`.

Em ambos os casos, o circuito passa por três *onion routers* (ORs) diferentes. Também se pode concluir que, apesar de o *browser* ser o mesmo, os circuitos são diferentes.

1.4 P1.2

Na Figura 1.7 pode consultar-se o circuito da página `http://zqktlwi4fecvo6ri.onion/wiki/index.php/Main_Page`.

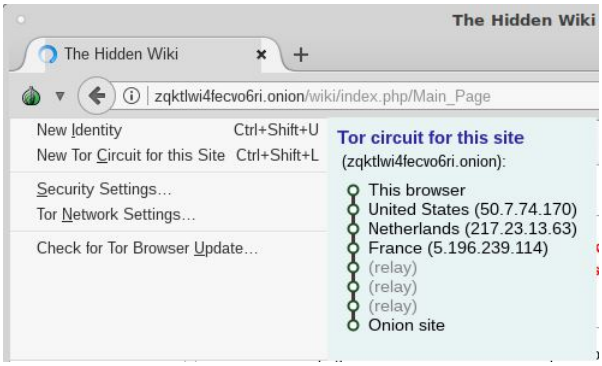

Figura 1.7: Circuito para o site `http://zqktlwi4fecvo6ri.onion/wiki/index.php/Main_Page`.

Existem seis saltos até ao Onion e três deles são de *"relay"*. As células de *"relay"* são utilizadas para garantir o anonimato quer de quem disponibiliza os serviços como de quem acede aos serviços. Deste modo, o endereço IP de quem disponibiliza um determinado serviço é anónimo, assim como o endereço IP de quem acede a esse serviço.