

Engenharia de Segurança

Trabalho Prático 3

Afonso Fontes

(pg35389)

Bruno Carvalho

(a67847)

Mariana Carvalho

(a67635)

27 de Fevereiro de 2018

Universidade do Minho

TOR (The Onion Router)

Pergunta P1.1

Efetuada o comando `sudo anonsurf start` consegue garantir que está localizado nos EUA?

Não, apenas conseguimos, através do comando `sudo anonsurf change` obrigar o calculo de um novo circuito que muito provavelmente tem um novo **OR** de saída, no entanto, utilizando o **anonsurf** é impossível garantir que este esteja localizado nos EUA.

Porquê? Utilize características do protocolo TOR para justificar.

Isto acontece devido à forma como são seleccionados os três **ORs** fornecidos ao **OP** pelo **Directory Server**, que devem ser sempre alterados uma vez por minuto. Através do software utilizado é impossível garantir que os **ORs** seleccionados se encontram nos EUA, no entanto caso o software fosse implementado por nós, o protocolo prevê a possibilidade de utilizar circuitos escolhidos de forma não aleatória, sendo que poderíamos escolher a utilização de **ORs** localizados nos EUA para formação do nosso circuito.

Pergunta P1.2

Clique no símbolo do Onion(cebola) do lado esquerdo da barra de URL e verifique qual é o circuito para esse site.

Podemos visualizar na fig1 e fig2 o resultado obtido aquando da consulta do circuito para os sites correspondentes.

Tor circuit for this site

(zqktlwi4fecvo6ri.onion):


- 
- This browser
 - Canada (158.69.30.132)
 - United States (100.16.220.246)
 - France (62.210.78.235)
 - (relay)
 - (relay)
 - (relay)
 - Onion site

Figura 1: *TOR circuit* para o primeiro site

Tor circuit for this site

(facebookcorewwwi.onion):



Figura 2: *TOR circuit* para o segundo site

Porque existem 6 "saltos" até ao site Onion, sendo que 3 deles são "relay"? Utilize características do protocolo TOR para justificar.

Na rede TOR, a disponibilização de serviços anónimos permite a um OP disponibilizar serviços TCP sem revelar o seu endereço IP, isto é feito pela rede TOR através de pontos de rendezvous. Em suma o que acontece é que a entidade que deseja prestar o serviço (identificada pela sua chave pública) cria um circuito cujo último(s) OR(s) denominam-se por *introduction points* e são anunciados no *Directory Server*. Quando nós (cliente) tentamos aceder ao serviço, obtemos informação sobre os *introduction points* para o mesmo, mantendo total anonimato do serviço ao qual pretendemos aceder, ao mesmo tempo criamos um circuito até a um OR que vai ser utilizado como o nosso *Rendezvous Point*. De seguida o cliente entrega um segredo a um dos *introduction points* para o serviço requisitando o mesmo através do *Rendezvous Point* estabelecido, finalmente o serviço conecta-se ao RP do cliente fornecendo o respetivo segredo. A partir de agora o cliente

utiliza o circuito conhecido que acaba no RP respetivo, garantindo anonimato até a um ponto de introdução para um circuito *relay*, que proporciona anonimato ao serviço Onion que pretendemos utilizar.