Universidade do Minho

Mestrado Integrado em Engenharia Informática

Engenharia de Segurança

Trabalho TP3

Grupo 2
Paulo Gameiro - A72067
Pedro Rodrigues - PG41092
Rafaela Soares - A79034

Braga, Portugal
9 de Março de 2020

Conteúdo

1 Exercício 1: TOR (*The Onion Router*)

1.1 Pergunta P1.1

A resposta à pergunta é não. O TOR, se for iniciado usando o comando **sudo anonsurf start**, não irá garantir que o utilizador será visto como estando localizado nos EUA.

O TOR, em si, tem como objetivo garantir anonimato quando se usa a Internet e respectivos serviços anónimos, sendo que para este fim o TOR irá utilizar *Onion Routers* (OR) e *Onion Proxy's* (OP).

O modo geral em que o TOR trabalha consiste em "saltar"de um OR para outro OR, através de uma conexão TLS, sendo que o OP irá estabelecer os circuitos através da rede e irá também gerar conexões das aplicações ao utilizador. Assim sendo, o IP do utilizador irá estar escondido de pessoas que possam estar a analisar o tráfego da rede.

No entanto, o utilizador poderá alterar o "*Exit Node*"no ficheiro torrc alterando ExitNodes para, por exemplo, ExitNodes kr,ru,sy,cn usando os *Tor Country Codes*, caso queira garantir qual será a sua localização.

1.2 Experiência 1.2

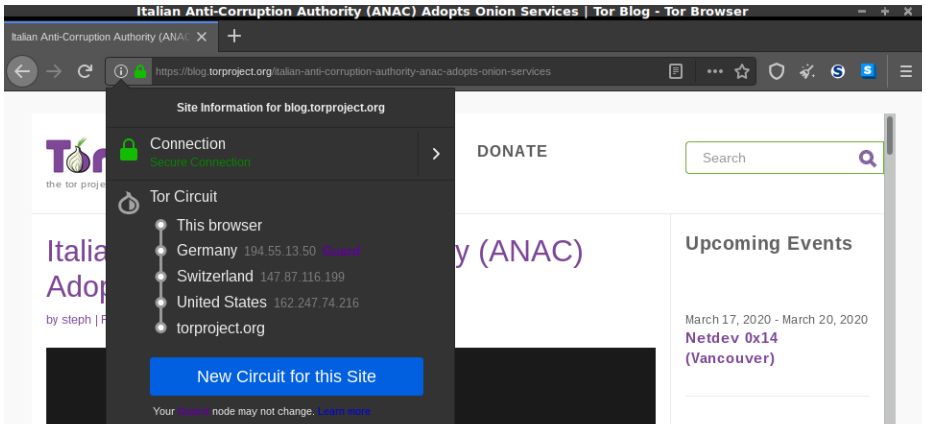

Figura 1: *Circuito TOR* no *site* **blog.torproject.org**

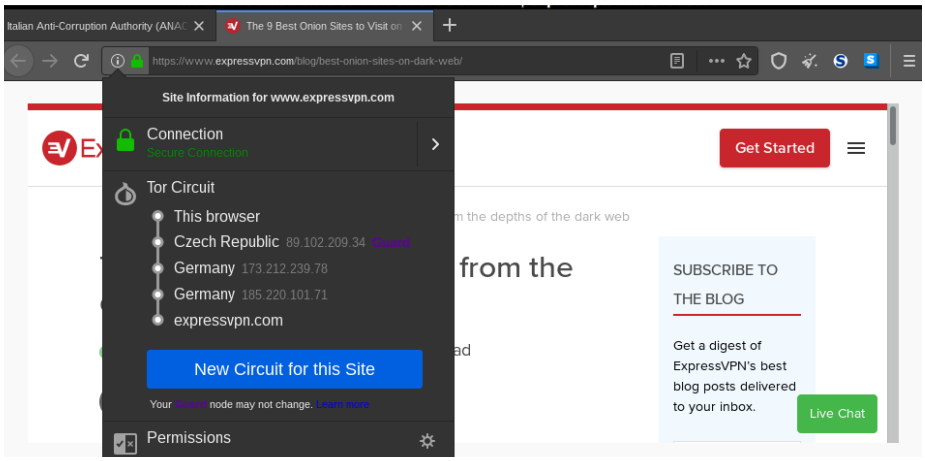

Figura 2: *Circuito TOR* no *site* **expressvpn.com**

Através dos resultados obtidos nos sites anteriormente, foi possível que o circuito difere consoante o site que esteja a ser visitado, de forma a que o utilizador se mantenha anónimo e não se torne tão fácil a conexão entre os acessos aos diversos sites.

1.3 Pergunta P1.2

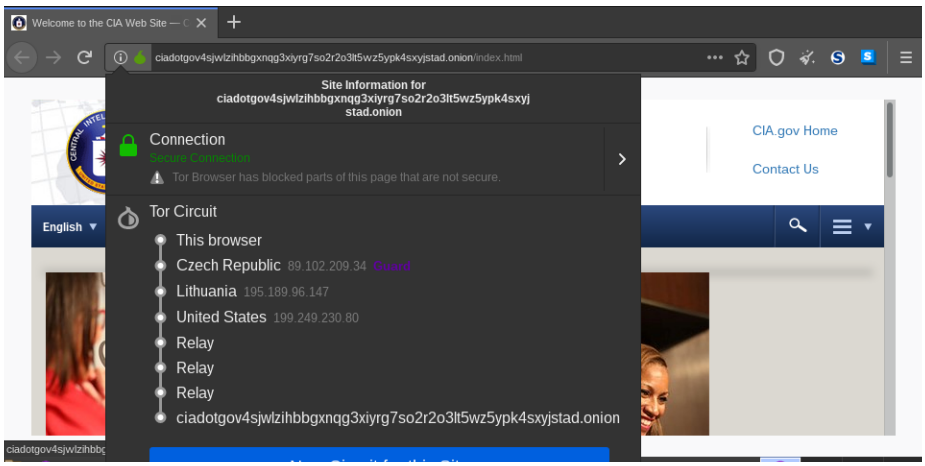

Figura 3: *Circuito TOR* no *site* da **CIA**

De forma a manter a anonimização do utilizador, garantida pelo protocolo TOR, a ligação efetuada é passada através de 6 saltos, sendo que 3 são correspondentes a ORs (Onion Routers) que se encontram no Directory Server em

que o utilizador está ligado (representados através da localização e IP), e os restantes 3 (denominados de Relay) são correspondentes aos ORs do servidor de destino, que é neste caso o servidor de armazenamento da CIA.

Cada um dos nós no circuito tem apenas conhecimento dos nós que estão imediatamente antes e depois dele próprio, e portanto o circuito é criado pelo servidor de confiança que corresponde ao Directory Server.

Entre os Onion Routers do cliente e do servidor encontra-se um ponto de ligação, denominado de **Rendezvous Point**, permitindo desta forma uma maior anonimização tendo em conta que cada uma das partes tem apenas conhecimento de 3 nós.