APSEI Assignment 2
Business hacking

Raquel Paradinha 102491
Miguel Matos 103341

Março 2023

Contents

1 Introdução

No âmbito da realização deste trabalho, exploramos o ecossistema *web* associado a uma dada conexão. Para este efeito, escolhemos o site Caracas Chronicles (`https://www.caracaschronicles.com/`), um *site* de notícias Venezuelano, como sendo o destinatário a que tentamos aceder.

2 Traceroute

O comando *traceroute* é utilizado para descobrir quantos dispositivos estão entre o computador que inicia a conexão e o destino da mesma, através do envio de sucessivos pacotes ICMP. No fim da execução, retorna dados como o endereço IP dos *routers* e a velocidade das conexões.

Como referido anteriormente, o site escolhido para este trabalho foi o *caracaschronicles.com*. Este é o resultado da execução do comando `traceroute -I caracaschronicles.com` dentro da rede *eduroam*, na Universidade de Aveiro.

```
mankings@pop-os:~$ traceroute -I caracaschronicles.com
traceroute to caracaschronicles.com (172.67.192.7), 64 hops max
  1   192.168.63.254  2.953ms  2.142ms  2.297ms
  2   10.1.0.118  3.849ms  2.614ms  2.194ms
  3   193.137.173.244  3.917ms  5.288ms  4.396ms
  4   193.136.4.26  6.267ms  4.036ms  4.936ms
  5   194.210.7.108  9.387ms  9.570ms  10.644ms
  6   193.136.1.8  9.711ms  9.771ms  9.878ms
  7   194.210.6.103  12.443ms  11.932ms  13.480ms
  8   83.97.88.209  16.509ms  11.442ms  11.690ms
  9   62.40.98.97  24.152ms  20.072ms  19.436ms
 10   *  *  *
 11   172.68.132.2  20.021ms  19.996ms  19.376ms
 12   172.67.192.7  21.295ms  21.850ms  21.460ms
```

Neste caso, os pacotes chegaram ao destino final no 12º dispositivo. Todos os que responderam ao pacote ICMP têm listados os seus endereços IP e o tempo que a máquina demorou a responder, nas três tentativas. No 10º salto, o *traceroute* retorna três asteriscos. Isto significa que o pacote ICMP deu *timeout*, ou seja, o processo não obteve resposta ao pacote. Quando isto acontece, o *traceroute* retorna um asterisco e passa para o próximo pacote.

3 Resultados

3.1 Informações por IP

As tabelas 1 e 2 contêm os dados obtidos utilizando ferramentas como `https://ipinfo.io/` e `https://www.infobyip.com/`, assim como o comando `whois <ip_address>` utilizado diretamete na linha de comandos, para obter mais informações acerca dos endereços fornecidos pelo comando *traceroute*.

A primeira contém dados relativos à localização física dos dispositivos, e as organizações por eles responsáveis. Já a segunda refere-se às companhias responsáveis pelos *hosting* dos serviços - vários dos *routers* por onde a conexão são operados pelas mesmas organizações, como parte de uma rede maior, identificada pelo seu *Autonomous System Number* (ASN). Este é o identificador utilizado pelo protocolo *Border Gateway Protocol* (BGP), utilizado para trocar informação de forma eficaz entre estas "super-redes" geridas por organizações diferentes.

Os endereços 1 e 2 são classificados como endereços IP *bogon*, que correspondem a endereços IP não atribuídos oficialmente por entidades responsáveis, tais como a *Internet Assigned Numbers Authority* (IANA) e *Regional Internet Registry* (RIR).

O endereço 10 retorna apenas três asteriscos, ou seja, o pedido deu *timeout* nas três vezes em que foi feito. Existem várias razões possíveis para isto, sendo as mais prováveis a interferência de uma firewall que bloqueia os pacotes ICMP, ou que o router está demasiado ocupado para responder ao pedido, tendo em conta o *Time-To-Live* (TTL) dos pacotes enviados.

3.2 Headers HTTP

Os pacotes HTTP enviados pelos dispositivos também contêm alguma informação relativa ao ecossistema onde estão inseridos. Ao utilizar uma ferramenta/website como `https://securityheaders.com/` para analisar os pacotes recebidos, conseguímos descobrir também aspetos como as tecnologias de software em que a plataforma assenta. No nosso caso, o *Caracas Chronicles* é construído em *WordPress*, um *Content Management System* (CMS), assentando na *WP Engine*, uma plataforma de *hosting* e gestão de websites construídos em *WordPress*.

	IP	Coordenadas	País	Endereço	Organização
1	192.168.63.254	-	-	-	-
2	10.1.0.118	-	-	-	-
3	193.137.173.244	40.6310, -8.6584	PT	Campus Universitário de Santiago, 3810-193 Aveiro	Universidade de Aveiro
4	193.136.4.26	38.7591, -9.1422	PT	Av. do Brasil, 101, 1700-066 Lisboa	FCT
5	194.210.7.108	40.2056, -8.4195	PT	Rua Infantaria, 23, 3000-219 Coimbra	FCT
6	193.136.1.8	38.6910, -9.3109	PT	Rua Nossa Senhora do Egipto, 34, 2780-236 Oeiras	FCT
7	194.210.6.103	38.7167, -9.1333	PT	Largo das Olarias, 60, 1100-295 Lisboa	FCT
8	83.97.88.209	40.4165,-3.7025	ES	Apartamentos del Sol, Puerta del Sol, 2, 28012 Madrid	GEANT Vereniging
9	62.40.98.97	40.4165,-3.7026	ES	Apartamentos del Sol, Puerta del Sol, 3, 28013 Madrid	GEANT Vereniging
10	-	-	-	-	-
11	172.68.132.2	40.4165,-3.7026	ES	Apartamentos del Sol, Puerta del Sol, 3, 28013 Madrid	Cloudflare, Inc.
12	172.67.192.7	37.7621,-122.3971	US	101 Townsend Street, 94107 San Francisco	Cloudflare, Inc.

Table 1: Localização dos Dispositivos

	Host	ASN	Usage Type
1, 2	-	-	-
3, 4, 5, 6, 7	Fundação para a Ciência e Tecnologia	AS1930	(EDU) University/College/School
8, 9	GEANT Vereniging	AS20965	(DCH) Data Center/Web Hosting/Transit
10	-	-	-
11, 12	Cloudflare, Inc.	AS13335	(CDN) Content Delivery Network

Table 2: Internet Service Providers

Raw Headers

HTTP/2	200
date	Sat, 25 Mar 2023 23:13:36 GMT
content-type	text/html; charset=UTF-8
vary	Accept-Encoding
vary	Accept-Encoding
vary	Accept-Encoding
vary	Accept-Encoding,Cookie
link	<https://www.caracaschronicles.com/wp-json/>; rel="https://api.w.org/"
link	<https://www.caracaschronicles.com/wp-json/wp/v2/pages/13>; rel="alternate"; type="application/json"
link	<https://wp.me/P6PDXs-d>; rel=shortlink
x-powered-by	WP Engine
x-cacheable	SHORT
cache-control	max-age=600, must-revalidate
x-cache	HIT: 3
x-cache-group	normal
cf-cache-status	DYNAMIC
report-to	{"**endpoints**":[{"**url**":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=%2BVz8rO4bSN4o%2B1pxySZ%2F6QvnRd9TLi4acLYX9jo5FqXWDZCDyMhff8Kpf1cLCW%2BBWce%2BzkvsIZaCwR3aOOOJDAEAQf19DcRnlnYypJsw3iM8DznnAfhMyNM4W5zdnilwPgd6sHNA9IZ7XuAEr6qG%2BT4PNt9cpfoW"}],"**group**":"cf-nel","**max_age**":604800}
nel	{"**success_fraction**":0,"**report_to**":"cf-nel","**max_age**":604800}
server	cloudflare
cf-ray	7adad86a0d1dd001-SJC
content-encoding	gzip
alt-svc	h3=":443"; ma=86400, h3-29=":443"; ma=86400

4 Stakeholders e Ecossistema

4.1 Fundação para a Ciência e Tecnologia

A Fundação para a Ciência e Tecnologia (FCT) é uma organização governamental portuguesa que opera a Rede Ciência, Tecnologia e Sociedade (RCTS), uma infraestrutura que disponibliza serviços de conectividade e computação a instituições de ensino superior e não só.

4.2 GÉANT

A *GÉANT* é uma rede europeia para a investigação e educação que interconecta várias redes nacionais com o mesmo propósito. Foi fundada pela União Europeia e os seus países membros com o objetivo de fornecer serviços de conectividade *internet* a instituições de ensino e investigação na Europa.

4.3 Cloudflare

A *Cloudflare* é uma empresa norte-americana que fornece serviços de *internet*, nomeadamente, redes de distribuição de conteúdos (CDN), serviços de segurança e gestão de servidores de nomes de domínios (DNS).

Além disso, este serviço atua também como um *proxy* reverso, ou seja encaminha os pedidos dos clientes para os servidores web disponíveis, permitindo melhorar aspetos como a velocidade, disponibilidade e segurança destes.

4.4 Ecossistema

Com efeito, a conexão é roteada por duas redes de educação e investigação - uma nacional (FCT) e outra internacional (*GÉANT*) - até chegar aos servidores da *Cloudflare*, que aloja o website *Caracas Chronicles*.

5 Conclusão

Apesar desta análise se focar num *website* em particular, este é um exemplo da forma como várias organizações diferentes trabalham juntas para fornecer serviços de *internet* e conectividade.

Deste modo, conseguimos aprofundar as ligações existentes numa rede, assim como toda a comunicação que é necessária para ser feita a ligação entre dois pontos distantes no globo e conectados através da *internet*.

6 References

6.1 Tools

- https://www.infobyip.com/
- https://www.ipinfo.io/
- https://securityheaders.com/
- https://digital.com/best-web-hosting/who-is/

6.2 Sources

- https://www.apnic.net/manage-ip/apnic-services/registration-services/resource-quality-assurance/what-is-a-bogon-address/
- https://eduroam.org/eduroam-and-geant/
- https://pt.wikipedia.org/wiki/Cloudflare
- https://www.cloudflare.com/pt-br/learning/cdn/glossary/reverse-proxy/
- https://www.fct.pt/
- https://geant.org/
- https://www.cloudflare.com/