Wyszukiwanie ścieżki datagramu w internecie

Patryk Kaniewski

2021-01-06

Spis Treści

Patryk Kaniewski

1 Grupa wykonująca zadanie

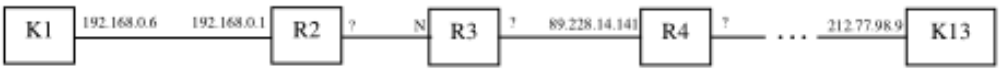
- Patryk Kaniewski

2 Wstęp

2.1 Cel ćwiczenia

Wyszukanie ścieżki datagramów w internecie

2.2 Schemat ćwiczenia



2.3 Wymagany sprzęt

- Komputer z systemem POSIX

2.4 Plan ćwiczenia

2.4.1 Część 1:

1. Wyszukujemy cel
2. Rejestrujemy ruch ICMP
3. Znajdujemy droge

2.4.2 Część 2:

1. Rejestracja ruchu ICMP i DNS
2. Znajdujemy DNS i reverse DNS

2.4.3 Część 3:

1. Znajdujemy droge do dalekiego celu
2. Czekamy
3. Znajdujemy droge do dalekiego celu
4. Porownujemy drogi

3 Ćwiczenie

3.1 Przed ćwiczeniem

3.1.1 Konfiguracja wstępna

ip a show dev enp4s0

```
2: enp4s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default ql
    link/ether b4:2e:99:e4:68:04 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.186/24 brd 192.168.0.255 scope global dynamic noprefixroute enp4s0
       valid_lft 32301sec preferred_lft 32301sec
```

Wybieramy cel (w moim przypadku skierniewice.eu)

3.2 Część 1

3.2.1 Szukanie celu

Wykonujemy ping do wybranego przez nas celu (w moim przypadku skierniewice.eu)

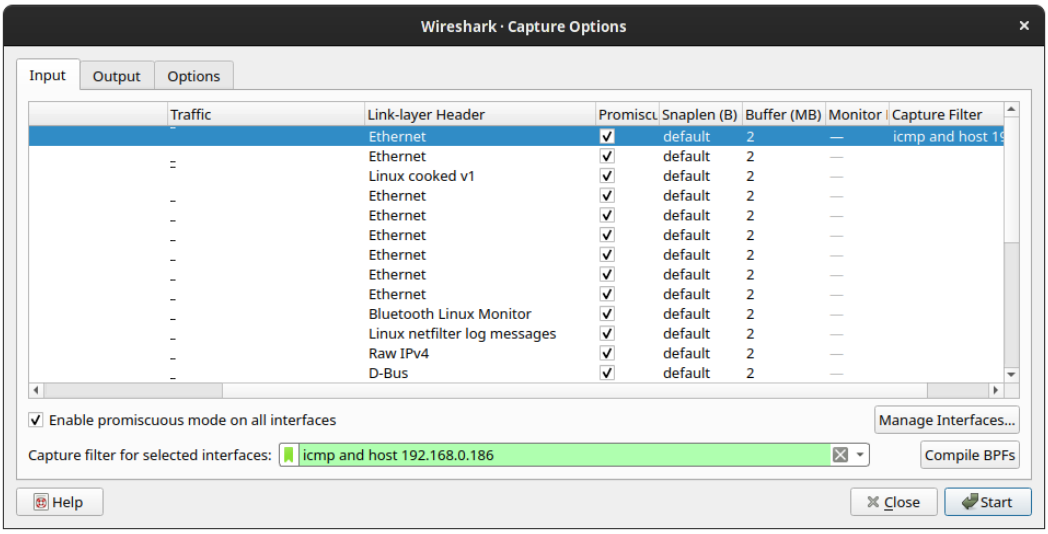
```
PING skierniewice.eu (94.152.194.219) 56(84) bytes of data.
64 bytes from 10.ires.pl (94.152.194.219): icmp_seq=1 ttl=55 time=6.41 ms
64 bytes from 10.ires.pl (94.152.194.219): icmp_seq=2 ttl=55 time=6.49 ms
64 bytes from 10.ires.pl (94.152.194.219): icmp_seq=3 ttl=55 time=6.43 ms
64 bytes from 10.ires.pl (94.152.194.219): icmp_seq=4 ttl=55 time=6.31 ms

--- skierniewice.eu ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 6.310/6.412/6.492/0.065 ms
```

3.2.2 Rejestracja ruchu ICMP

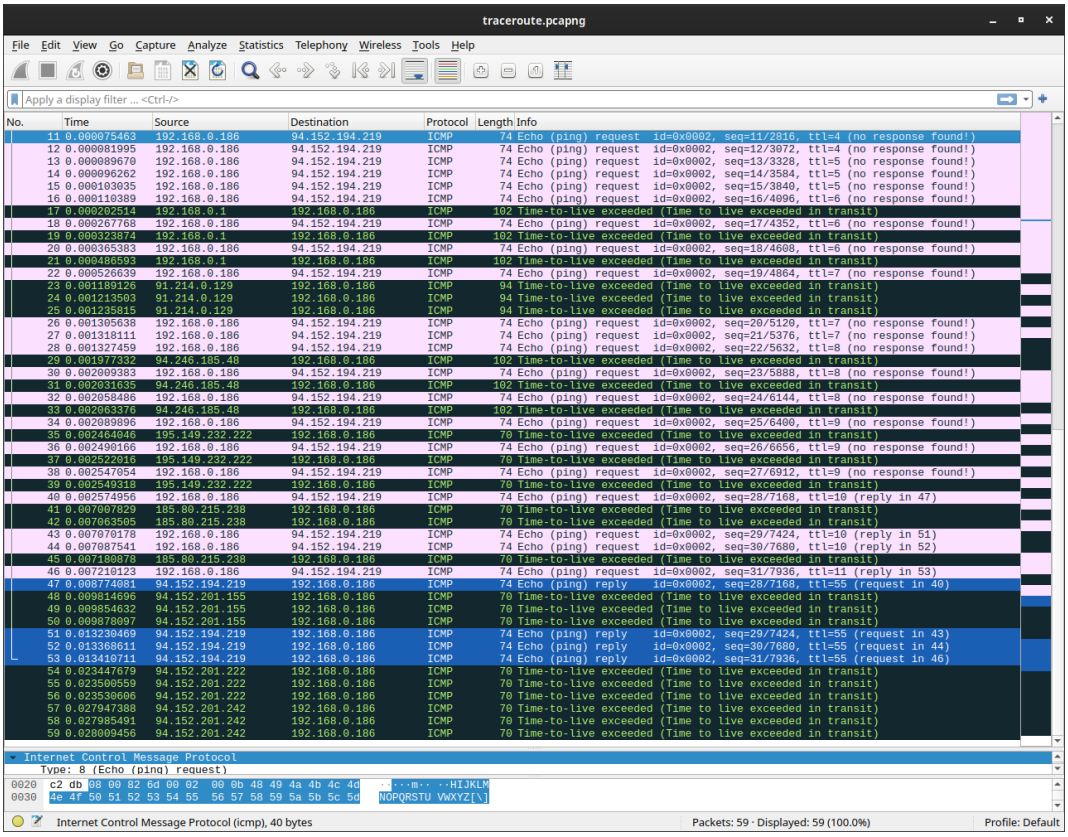
Następnie używamy otrzymanego adresu IP do polecenia `traceroute -n -I 94.152.194.219` (opcja -n wyłącza odwracanie adresów ip na adresy domenowe; opcja -I wymusza używanie icmp echo do badania celow).

Rejestrujemy sesje za pomoca programu do przechwytywania pakietów np. wireshark i filtrujemy ICMP.



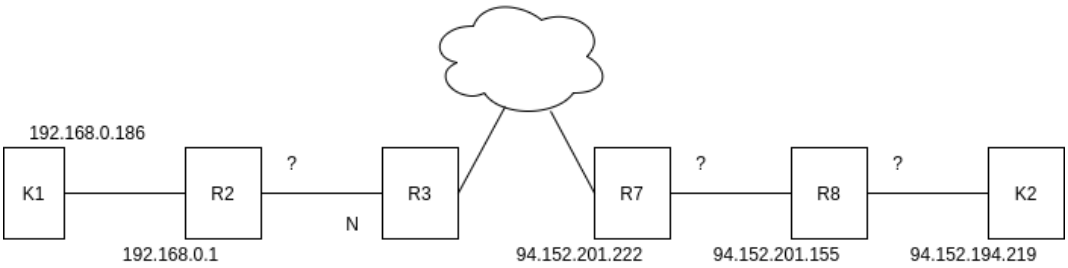

```
traceroute to skierniewice.eu (94.152.194.219), 30 hops max, 60 byte packets
 1  192.168.0.1  0.223 ms  0.318 ms  0.473 ms
 2  91.214.0.129  1.167 ms  1.184 ms  1.200 ms
 3  * * *
 4  94.246.185.48  1.913 ms  1.960 ms  1.986 ms
 5  195.149.232.222  2.379 ms  2.431 ms  2.451 ms
 6  185.80.215.238  6.902 ms  6.804 ms  6.823 ms
 7  94.152.201.242  27.428 ms  26.699 ms  26.697 ms
 8  94.152.201.222  22.125 ms  21.498 ms  21.478 ms
 9  94.152.201.155  7.770 ms  7.394 ms  7.273 ms
10  94.152.194.219  6.205 ms  6.176 ms  6.286 ms
```

3.2.3 Wyniki



- Na różowo zaznaczone są Echo Requst
- Na czarno zaznaczone sa TTL exceeded
- Na niebiesko zaznaczone sa Echo Reply

Nasza scieżka wyglada następująco:



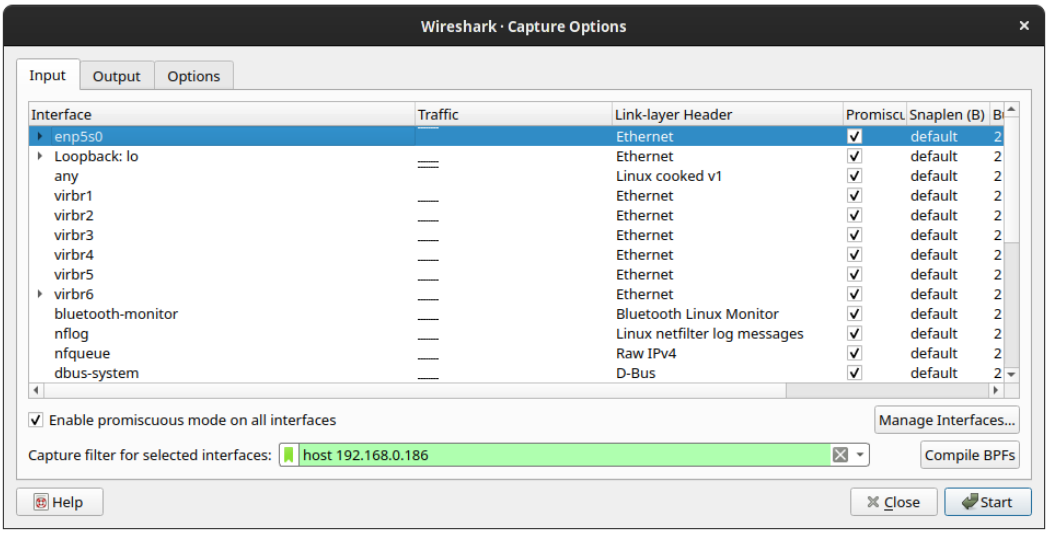
3.3 Część 2

3.3.1 Rejestracja ICMP i DNS

W częsci drugie nieco zmieniamy nasze polecenie `traceroute -I skierniewice.eu` (opcja -I wymusza używanie icmp echo do badania celow).

Bez opcji -d, traceroute bedzie probował znaleść poprzez reverse DNS lookup adresy domenowe zwiazane z adresami ip.

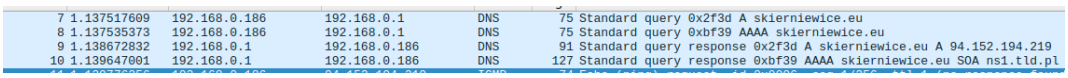
Zmieniamy również opcje przechwytywania w programie przechwytywania pakietów (np. wireshark) na host K1.



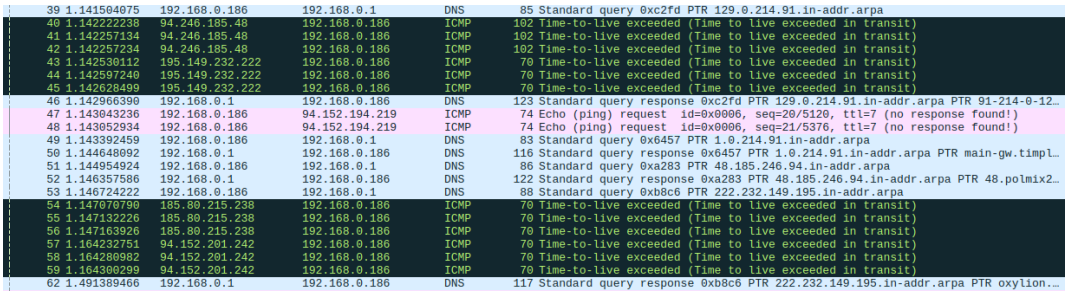

```
traceroute to skierniewice.eu (94.152.194.219), 30 hops max, 60 byte packets
 1  _gateway (192.168.0.1)  0.247 ms  0.313 ms  0.481 ms
 2  91-214-0-129.timplus.net (91.214.0.129)  1.387 ms  1.379 ms  1.415 ms
 3  main-gw.timplus.net (91.214.0.1)  1.469 ms  1.490 ms  1.505 ms
 4  48.polmix2.epix.net.pl (94.246.185.48)  2.370 ms  2.397 ms  2.389 ms
 5  oxylion.tpix.pl (195.149.232.222)  2.654 ms  2.714 ms  2.739 ms
 6  185.80.215.238 (185.80.215.238)  7.172 ms  6.814 ms  6.805 ms
 7  5E98C9F2.static.tld.pl (94.152.201.242)  23.860 ms  21.250 ms  21.252 ms
 8  5E98C9DE.static.tld.pl (94.152.201.222)  25.080 ms  25.089 ms  25.100 ms
 9  5E98C99B.static.tld.pl (94.152.201.155)  14.678 ms  14.714 ms  14.730 ms
10  10.ires.pl (94.152.194.219)  6.568 ms  6.598 ms  6.619 ms
```

3.3.2 Wyniki

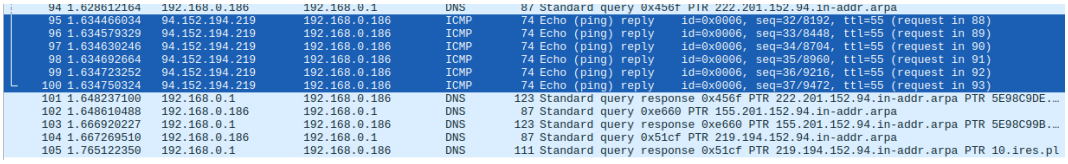
Aby ułatwić analizę packetdump możemy uzyć w wireshark display filter `icmp or dns`.



Pierwsze nasze zapytanie DNS jest typu A(AAA), aby przekonwertować nazwe domeny który przekazalismy traceroute (skierniewice.eu) na adres IPv4.



Każde kolejne zapytanie bedzie typu PTR, aby przekonwertować adres IP na nazwe domeny. Warto zwrócić uwage na to że adres IP który został wysłany w zapytaniu PTR mial oktety odwrócone i `.in-addr.arpa` dodane na końcu.



Dokładnie tak samo wygląda zapytanie na ostateczny adres na który jest związany z domeną która testowaliśmy. Ciekawym spostrzeżeniem może być że zapytanie PTR na ten sam adres który dostaliśmy z zapytania A `skierniewice.eu` ma inna nazwe domeny (`10.ires.pl`).

Można to zweryfikować za pomocą innych narzędzi (np. linux `dig` i `dig -x`).

```
;; QUESTION SECTION:
;skierniewice.eu.                IN      A

;; ANSWER SECTION:
skierniewice.eu.         3599    IN      A

;; QUESTION SECTION:
;219.194.152.94.in-addr.arpa.    IN      PTR

;; ANSWER SECTION:
219.194.152.94.in-addr.arpa. 3600 IN    PTR     10.ires.pl.
```

3.4 Część 3

3.4.1 Odległy cel

Znalezienie odległego celu w dzisiejszych czasach może okazać sie problemem ze wzgledu na powszechność usług takich jak cloudflare, aws oferujacych wszelakie usługi proxy/cache.

Wybralem cel `theindependent.sg` znajdujący sie w azji południowo-wschodniej:

```
PING theindependent.sg (34.87.85.150) 56(84) bytes of data.
64 bytes from 150.85.87.34.bc.googleusercontent.com (34.87.85.150): icmp_seq=1 ttl=60 time=265
64 bytes from 150.85.87.34.bc.googleusercontent.com (34.87.85.150): icmp_seq=2 ttl=60 time=266
64 bytes from 150.85.87.34.bc.googleusercontent.com (34.87.85.150): icmp_seq=3 ttl=60 time=265
64 bytes from 150.85.87.34.bc.googleusercontent.com (34.87.85.150): icmp_seq=4 ttl=60 time=265
```

```
--- theindependent.sg ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 265.312/265.624/266.329/0.410 ms
```

Traceroute o godzinie 11:01

```
traceroute to theindependent.sg (34.87.85.150), 30 hops max, 60 byte packets
 1  192.168.0.1  0.249 ms  0.352 ms  0.453 ms
 2  91.214.0.129  1.140 ms  1.146 ms  1.155 ms
 3  * * *
 4  94.246.185.48  1.893 ms  1.928 ms  2.005 ms
 5  195.149.233.101  2.436 ms  2.482 ms  2.673 ms
 6  188.47.253.245  2.565 ms  2.620 ms  2.547 ms
 7  * * *
 8  108.170.248.178  265.680 ms  265.580 ms  265.623 ms
 9  108.170.225.145  262.537 ms * *
10  209.85.243.180  263.452 ms  263.414 ms  263.415 ms
11  108.170.233.49  266.235 ms  265.706 ms  265.734 ms
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  34.87.85.150  265.372 ms  265.358 ms  265.202 ms
```

3.4.2 Ponowienie szukania drogi

3.4.3 Różnice w drodze

Aby porownać różnice odrzuciłem pingi z traceroute za pomoca polecenia `awk '{print $1 "\t" $2}' traceroute1.txt > trace1.txt` a następnie polecenia `diff` aby porównać te pliki

4 Wnioski

4.1 Routing

4.2 Napotkane problemy

4.2.1 traceroute -I

traceroute na systemie na ktorym przeprowadzane jest ćwiczenie (Archlinux) domyślnie nie używa ICMP echo (ping) do przeszukiwania drogi ze wzgledu na to że w dużej ilości sieci pakiety ICMP sa filtrowane

1	0.000000000	192.168.0.1	192.168.0.186	ICMP	102 Time-to-live exceeded (Time to live exceeded in transit)
2	0.000136079	192.168.0.1	192.168.0.186	ICMP	102 Time-to-live exceeded (Time to live exceeded in transit)
3	0.000226510	192.168.0.1	192.168.0.186	ICMP	102 Time-to-live exceeded (Time to live exceeded in transit)
4	0.001413974	91.214.0.129	192.168.0.186	ICMP	94 Time-to-live exceeded (Time to live exceeded in transit)
5	0.001503333	91.214.0.129	192.168.0.186	ICMP	94 Time-to-live exceeded (Time to live exceeded in transit)
6	0.001543339	91.214.0.129	192.168.0.186	ICMP	94 Time-to-live exceeded (Time to live exceeded in transit)
7	0.001571543	91.214.0.1	192.168.0.186	ICMP	94 Time-to-live exceeded (Time to live exceeded in transit)
8	0.001595959	91.214.0.1	192.168.0.186	ICMP	94 Time-to-live exceeded (Time to live exceeded in transit)
9	0.001621888	91.214.0.1	192.168.0.186	ICMP	94 Time-to-live exceeded (Time to live exceeded in transit)
10	0.002210425	195.43.72.106	192.168.0.186	ICMP	102 Time-to-live exceeded (Time to live exceeded in transit)
11	0.002242596	195.43.72.106	192.168.0.186	ICMP	102 Time-to-live exceeded (Time to live exceeded in transit)
12	0.002268215	195.43.72.106	192.168.0.186	ICMP	102 Time-to-live exceeded (Time to live exceeded in transit)
13	0.002726585	195.182.219.60	192.168.0.186	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
14	0.002763815	195.182.219.60	192.168.0.186	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
15	0.002789204	195.182.219.60	192.168.0.186	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
16	0.007341162	185.80.215.238	192.168.0.186	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
17	0.007371620	185.80.215.238	192.168.0.186	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
18	0.007419501	185.80.215.238	192.168.0.186	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
19	0.008670886	94.152.194.219	192.168.0.186	ICMP	102 Destination unreachable (Host administratively prohibited)
20	0.009075273	94.152.194.219	192.168.0.186	ICMP	102 Destination unreachable (Host administratively prohibited)
21	0.009102445	94.152.194.219	192.168.0.186	ICMP	102 Destination unreachable (Host administratively prohibited)
22	0.009170805	94.152.194.219	192.168.0.186	ICMP	102 Destination unreachable (Host administratively prohibited)
23	0.009209729	94.152.194.219	192.168.0.186	ICMP	102 Destination unreachable (Host administratively prohibited)
24	0.009234335	94.152.194.219	192.168.0.186	ICMP	102 Destination unreachable (Host administratively prohibited)

Rozwiązaniem tego było wyszukanie w manpage (`man traceroute`) o traceroute opcji -I która zmusza program do używania ICMP ping