Routing statyczny Cisco

Sprawozdanie nr 6 z przedmiotu Sieci Komputerowe

Maciej Kaszkowiak, 151856, zadania wykonane 3 czerwca 2023

Spis treści

1 Przy pomocy programu netstat zbadaj, na jakich portach uruchamiane są serwery:

- HTTP - 80
- HTTPS - 443
- FTP - 21
- telnet - 23
- DNS - 53

Oraz kilka dodatkowych:

- ssh - 22
- PostgreSQL - 5432
- Redis - 6379
- MongoDB - 27019

Zauważyłem również, że Google Chrome jako *klient* ma losowo przydzielane porty.

2 Zadanie 3

2.1 Przeprowadzić analizę komunikacji (Wireshark) na poziomie warstwy transportowej podczas przykładowej transmisji w systemie WWW.

Załadowałem plik http.cap do programu Wireshark.

2.2 Określić adresy IPv4 i numery portów (klienta i serwera) używanych podczas transmisji.

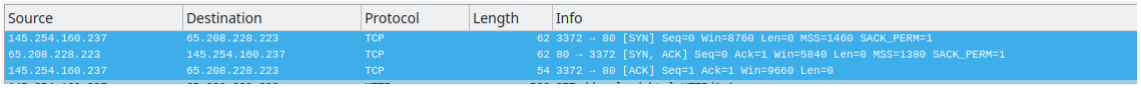
W przypadku połączenia o download.html, IPv4 serwera to 65.208.228.223, zaś IP klienta to 145.254.160.237. Port serwera to 80 (HTTP), a port klienta (przeglądarki) to 3372. Możemy zauważyć również połączenie na porcie 3371 - jest to drugie zapytanie ujęte w pliku http.cap, odpytujące o reklamy.

Source	Destination	Protocol	Length	Info
145.254.160.237	65.208.228.223	TCP	62	3372 → 80
65.208.228.223	145.254.160.237	TCP	62	80 → 3372
145.254.160.237	65.208.228.223	TCP	54	3372 → 80
145.254.160.237	65.208.228.223	HTTP	533	GET /downl
65.208.228.223	145.254.160.237	TCP	54	80 → 3372
65.208.228.223	145.254.160.237	TCP	1434	80 → 3372
145.254.160.237	65.208.228.223	TCP	54	3372 → 80
65.208.228.223	145.254.160.237	TCP	1434	80 → 3372
145.254.160.237	65.208.228.223	TCP	54	3372 → 80
65.208.228.223	145.254.160.237	TCP	1434	80 → 3372
65.208.228.223	145.254.160.237	TCP	1434	80 → 3372
145.254.160.237	65.208.228.223	TCP	54	3372 → 80
145.254.160.237	145.253.2.203	DNS	89	Standard q
65.208.228.223	145.254.160.237	TCP	1434	80 → 3372
145.254.160.237	65.208.228.223	TCP	54	3372 → 80
65.208.228.223	145.254.160.237	TCP	1434	80 → 3372
145.253.2.203	145.254.160.237	DNS	188	Standard q
145.254.160.237	216.239.59.99	HTTP	775	GET /pagea

Rysunek 1: Adresy oraz nr portów

2.3 Przeprowadzić analizę segmentów TCP przesyłanych w trakcie nawiązywania połączenia między klientem a serwerem HTTP. Określić dla każdego segmentu:

- kierunek transmisji
- numery portów (źródłowego, docelowego)
- znaczniki
- wartość pola sequence number
- wartość pola acknowledge number
- wartość pola window size
- wartości opcji



Source	Destination	Protocol	Length	Info
145.254.160.237	65.208.228.223	TCP	62	3372 → 80 [SYN] Seq=0 Win=8760 Len=0 MSS=1460 SACK_PERM=1
65.208.228.223	145.254.160.237	TCP	62	80 → 3372 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380 SACK_PERM=1
145.254.160.237	65.208.228.223	TCP	54	3372 → 80 [ACK] Seq=1 Ack=1 Win=9660 Len=0

Rysunek 2: Nawiązywanie połączenia pomiędzy klientem a serwerem HTTP

Na zrzucie ekranu możemy zaobserwować TCP handshake w postaci trzech pakietów (SYN, SYN ACK, ACK). Pakiet SYN trafia od klienta do serwera, SYN ACK od serwera do klienta, zaś ACK ponownie od klienta do serwera. Po wymianie pakietów transmisja zostaje nawiązana.

Poniżej zamieściłem informacje z Wiresharka. Przykładowo, pierwszy pakiet informuje o przesyłaniu danych z adresu 145.254.160.237:3372 na adres 65.208.228.223:80, ze znacznikiem SYN, z polem sequence number o wartości 0, bez wartości acknowledge number, z polem window size równym 8760, z opcjami MSS = 1460 (maksymalny rozmiar segmentu) oraz SACK PERM = 1.

```
145.254.160.237 65.208.228.223 TCP 62 3372 → 80 [SYN] Seq=0
  Win=8760 Len=0 MSS=1460 SACK_PERM=1

65.208.228.223 145.254.160.237 TCP 62 80 → 3372 [SYN, ACK] Seq=0 Ack=1
  Win=5840 Len=0 MSS=1380 SACK_PERM=1

145.254.160.237 65.208.228.223 TCP 54 3372 → 80 [ACK] Seq=1 Ack=1
  Win=9660 Len=0
```

Rysunek 3: Przedruk z Wiresharka

Poniżej załączam przedruk z RFC odnośnie opcji SACK_PERM:

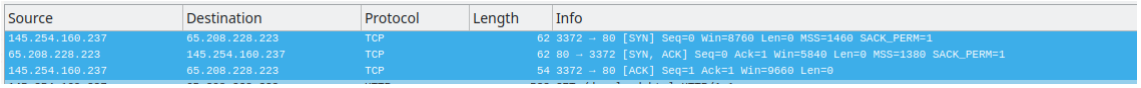
```
2.  Sack-Permitted Option
This two-byte option may be sent in a SYN by a TCP that has been
   extended to receive (and presumably process) the SACK option once the
   connection has opened.  It MUST NOT be sent on non-SYN segments.
```

Rysunek 4: RFC 2018: TCP Selective Acknowledgment Options

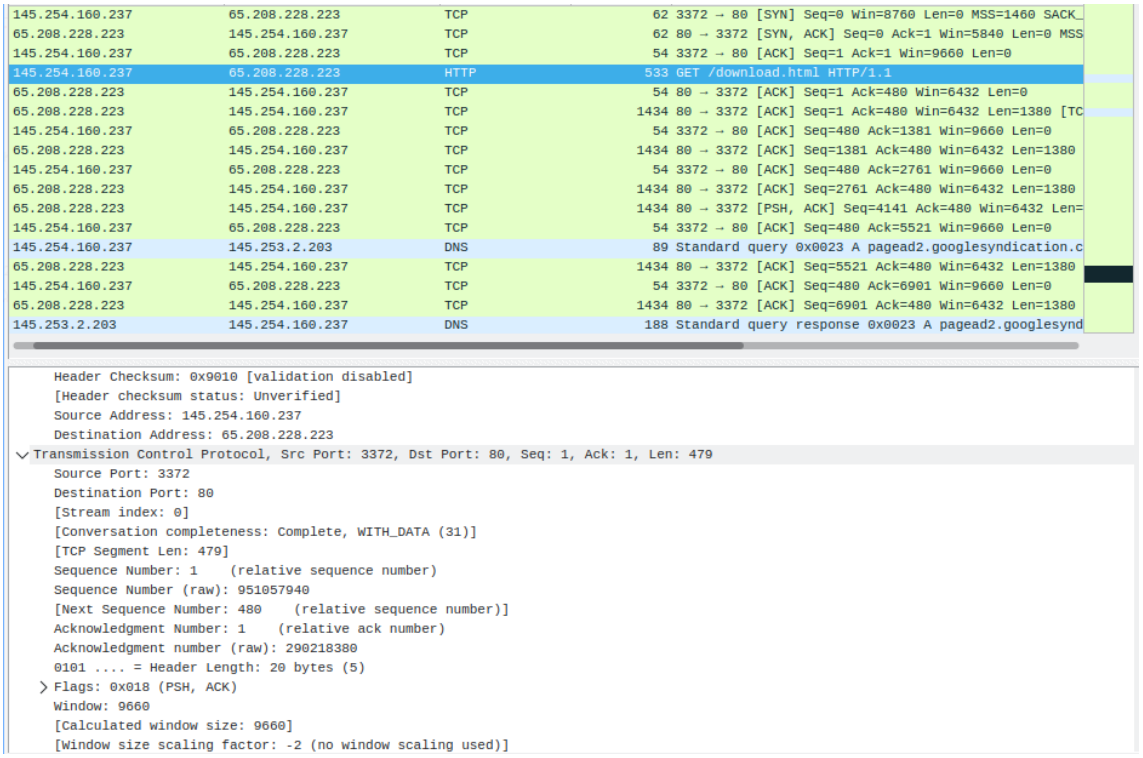
2.4 Przeprowadzić analizę segmentów TCP przesyłanych w trakcie przesyłania zawartości strony download.html między serwerem HTTP a klientem. Określić dla każdego segmentu:

- kierunek transmisji
- numery portów (źródłowego, docelowego)

- znaczniki
- wartość pola sequence number
- wartość pola acknowledgement number
- wielkość pola danych.



Rysunek 5: Połączenie HTTP pomiędzy klientem a serwerem HTTP

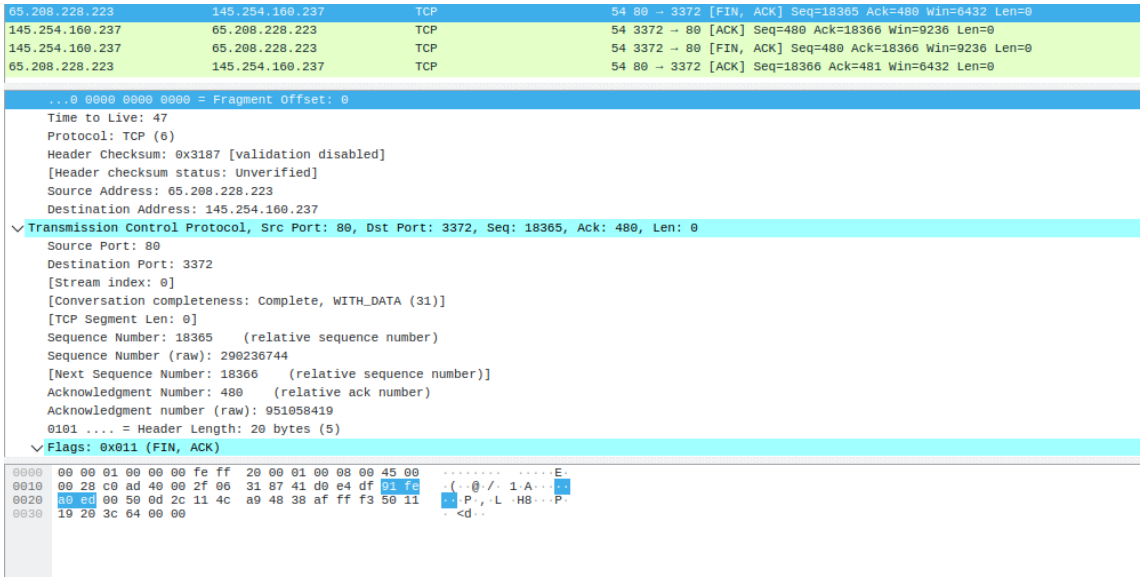


Rysunek 6: Żądanie HTTP

Na zrzutach ekranu możemy zaobserwować, że początkowo przesyłany jest pakiet z flagami PSH/ACK z żądaniem GET o pobranie pliku. W odpowiedzi serwer wysyła pakiety z danymi oraz flagą ACK. Klient zaś potwierdza każdy pakiet odpowiadając pakietem ACK bez danych. Wartości sequence number rosną wraz z przesyłem danych, a acknowledgement number odpowiada odpowiednim polom sequence number. Adresy IP oraz numery portów pozostają bez zmian. IPv4 serwera WWW to 65.208.228.223, zaś IP klienta (przeglądarki) to 145.254.160.237. Port serwera to 80, a port klienta to 3372.

2.5 Przeprowadzić analizę segmentów TCP przesyłanych w trakcie rozłączania. Określić dla każdego segmentu:

- kierunek transmisji
- numery portów (źródłowego, docelowego)
- znaczniki
- wartość pola sequence number
- wartość pola acknowledge number.



Rysunek 7: Segmenty TCP

Możemy zaobserwować, że koniec transmisji odbywa się zgodnie z następującym schematem: Klient przesyła do serwera pakiet FIN ACK, na co serwer odpowiada pakietem ACK. Następnie serwer również potwierdza zakończenie transmisji, przesyłając pakiet FIN ACK, na co klient odpowiada pakietem ACK. Adresy IP oraz numery portów pozostają bez zmian. IPv4 serwera WWW to 65.208.228.223, zaś IP klienta (przeglądarki) to 145.254.160.237. Port serwera to 80, a port klienta to 3372.