Sieci komputerowe - analiza ruchu sieci

Marcin Kostrzewski, 444409

7 stycznia, 2020r

Spis treści

1 Opis projektu

Celem tego dokumentu jest przedstawienie wyników mojej analizy ruchu sieci w formie projektu. Analiza została wykonana na bazie plików pobranych z linków:

- `http://marcing.faculty.wmi.amu.edu.pl/DSIK/0.tcpd`
- `http://marcing.faculty.wmi.amu.edu.pl/DSIK/3.tcpd`

2 Analiza zrzutu 0.tcpd

2.1 Przebieg

Zrzut przedstawia dwa pakiety z usługi **DHCP**, dokładniej pakiet *DHCPDISCOVER* i *DHCPREQUEST*. Możemy wywnioskować zatem, że są to pakiety wysłane przez nowego połączonego z siecią LAN klienta, który chce skorzystać z tej usługi i otrzymać lokalny adres IP. Nie widzimy w ruchu pakietów odsyłanych przez serwer, lecz możemy wywnioskować, że zostały takowe wysłane; gdyby serwer nie odpowiedział, klient nie wysłałby drugiego pakietu. Nie jesteśmy w stanie stwierdzić, czy usługa rzeczywiście osiągnęła rezultat - klient otrzymał adres IP; nie został zarejestrowany ostatni pakiet z usługi DHCP - *DHCPACK*, który wysyła serwer sygnalizując finalizacje usługi. Możemy jednak oszacować, że usługa ta zakończyła się pomyślnym przydzieleniem adresu IP klientowi; żądany adres IP z pakietu DHCPDISCOVER pojawia się także w pakiecie DHCPREQUEST, co oznacza, że serwer odpowiedział pakietem *DHCPOFFER*, w którym znajdował się żądany adres IP. Transakcja mogłaby zakończyć się niepowodzeniem jedynie w przypadku zerwania połączenia po wysłaniu ostatniego przechwyconego pakietu, lub w przypadku awarii serwera DHCP, co jest mało prawdopodobne.

2.2 Adresy i protokoły

Usługa DHCP korzysta z protokołu o tej samej nazwie, zaten widzimy tutaj pakiety protokołu **DHCP**. Widzimy jedynie pakiety wysłane na adres rozgłoszeniowy (255.255.255.255). Adres klienta nie jest nam znany; nie został mu jeszcze żaden przydzielony. W ramce Ethernet znajdziemy adres MAC karty sieciowej, z której wysłane zostały pakiety (**00:13:46:9a:bf:c4**), a w pakiecie DHCP znajdziemy pewne dwa adresy IP: żądane przez klienta IP **192.168.1.2** i adres IP routera, do którego przynależy klient: **192.168.1.1**(w pakiecie *DHCPREQUEST*).

2.3 Systemy

Nie jesteśmy w stanie określić w żadnym stopniu danych o serwerze DHCP, znamy jedynie jego adres IP. O kliencie wiemy jedynie tyle, że korzystał z karty sieciowej D-Link (na podstawie adresu MAC).

2.4 Czas wykonania zrzutu

W ramce Ethernet możemy znaleźć datę wysłania pierwszego pakietu: **3 grudnia 2007r, godz. 15:05 CEST**. Długość zrzutu, czyli różnica między czasem wysłania pierwszego pakietu i drugiego pakietu to **33,70ms**.

2.5 Lokalizacja skanera

Skaner mógł zostać uruchomiony na dowolnym urządzeniu w sieci LAN, w której znajdował się klient, bo wszystkie takie urządzenia otrzymają pakiety wysłane na adres rozgłoszeniowy.

2.6 Konfiguracja LAN

- Adres routera: **192.168.1.1**
- Adres MAC klienta: **00:13:46:9a:bf:c4**

Na routerze uruchuomiony jest serwer DHCP, który przydziela adresy IP z zakresu od **192.168.1.2**.

2.7 Odtworzenie zrzutu

Uruchamiamy program Wireshark z filtrem **ip.addr == 255.255.255.255**. Tworzymy nowe połączenie z dowolnego urządzenia do sieci LAN. Jeżeli chcemy, aby serwer DHCP przydzielił taki sam adres jak w zrzucie, możemy wcześniej ręcznie przypisać mu adres 192.168.1.2. Jeżeli odłączymy urządzenie od sieci i połączymy je ponownie, jeżeli żadne urządzenie nie zajęło tego adresu, to urządzeniu prawdopodobnie zostanie przydzielony ten sam adres. Przykładowe odtworzenie zrzutu w załączniku **example1.pcap**

3 Analiza zrzutu 3.tcpd

3.1 Przebieg

Podany zrzut przedstawia jakąś sesję **SSH**. Klient łączy się z samym sobą za pomocą SSH, autentykuje się i wykonuje jakieś działania korzystając z tego protokołu. Nie jesteśmy w stanie stwierdzic, jakie są wiadomości pakietów, ponieważ protokół SSH jest szyfrowany.

3.2 Adresy i protokoły

Wykorzsystywany jest protokół **SSHv2**. Klient znajduje się na tym samym komputerze co serwer, zatem klient łączy się sam ze sobą korzystając z adresu loopback (**127.0.0.1**). Serwer SSH działa na porcie **22**, i z tym portem faktycznie klient łączy się, korzystając z losowego portu, w tym przypadku **47751**. Nieznamy jego adresu klienta/serwera.

3.3 Lokalizacja skanera

Skaner był uruchomiony na komputerze, który łączył się sam ze swoim serwerem SSH.

3.4 Czas wykonania zrzutu

Zrzut został wykonany **3 grudnia, 2007r, godz. 20:46 CEST**. Sesja trwała **2 sekundy**.

3.5 Odtworzenie zrzutu

Uruchamiamy program Wireshak nasłuchujący na urządzeniu *loopback*. Na komputerze działa zarówno serwer jak i klient SSH. Za pomocą konsoli łączymy się z serwerem SSH na adresie 127.0.0.1. Autentykujemy się i kończymy sesję. Przykładowy zrzut załączony w pliku **example2.pcap**.