Analiza ruchu na lokalnej karcie sieciowej z użyciem analizatora Wireshark

Symbol A oznacza stację lokalną z Wireshark na Windows, a symbol B – stację zdalną.

1. Analiza ramek generowanych przez protokół ARP

Filtr przechwytywania:

host <adres stacji A> and host <adres stacji B> and arp

Polecenie wydane na stacji B (Linux):

arping –c1 <adres stacji A>

2. Analiza ramek generowanych przez polecenia śledzenia trasy pakietów

Filtry przechwytywania dla polecenia tracert (polecenie systemu Windows generujące komunikaty echo request, po 3 komunikaty na każde TTL):

Polecenie wydane na stacji A (Windows):

tracert –d –4 fedora.pl

Filtr przepuszczający tylko komunikaty "echo request" wysyłane ze stacji A do stacji B:

src host <adres IP stacji A> and dst host <adres IP stacji B> and icmp[0:1]=0x08

Filtr przepuszczający tylko komunikaty "TTL exceeded"
wysyłane z kolejnych routerów (adresy nieznane) do stacji A
i komunikaty "echo reply" wysyłane ze stacji B do stacji A:

(dst host <adres stacji A> and icmp[0:1]=0x0b) or
(src host <adres stacji B> and dst host <adres stacji A> and icmp[0:1]=0x00)

Filtr przechwytywania dla polecenia ping –r 9 –n 1 (polecenie systemu Windows generujące jeden komunikat echo request z opcją zapisu 9 etapów trasy tam i z powrotem):

host <adres stacji A> and host fedora.pl and (icmp[0:1]=0x08 or icmp[0:1]=0x00)

3. Analiza fragmentacji

Na stacji B (Linux) przestawiamy MTU na 296:
ip link set mtu 296 dev <nazwa interfejsu sieciowego>

Na stacji B (Linux) wydajemy polecenie generujące komunikat "echo request",
w którym za nagłówkiem ICMP jest 1000 oktetów danych:
ping -c1 -s1000 <adres stacji A>

Filtr przepuszczający pofragmentowane komunikaty "echo request"
wysłane ze stacji B (Linux) do stacji A:
src host <adres stacji B> and dst host <adres stacji A> and ip[9:1]=1

Przy analizowaniu przechwyconych ramek należy zwrócić uwagę na to, że w polu Protocol nagłówka IP każdego fragmentu jest kod protokołu ICMP, czyli liczba 1, natomiast nagłówek ICMP znajduje się tylko w pierwszym fragmencie. Z tego względu w wyrażeniu filtrującym jest warunek, aby 10 oktet nagłówka IP (pole „protokół”) miał wartość 1, ale nie ma warunku, aby w ramce był komunikat ICMP „echo request”, bo taki filtr przepuściłby tylko pierwszy fragment, a zatrzymał pozostałe.

Uwaga: opcja Edit -> Preferences -> Protocols -> IPv4 -> Reassemble fragmented IPv4 datagrams ma być niezaznaczona! W przeciwnym przypadku do ostatniego fragmentu zostanie dołączony cały pakiet, co znacznie utrudni analizę tego fragmentu.