Instrukcja laboratoryjna dla „Sieci komputerowe i Internet” – Moduł 5, Zadanie 2 *– Radosław Terelak*

1. Cele zadania laboratoryjnego:

Celem zadania laboratoryjnego jest wykorzystanie programu Wireshark do analizy ramek ethernetowych oraz protokołu ARP/Neighbour Discovery.

1. Przygotowanie środowiska do zajęć:

W ramach przygotowania środowiska do wykonania zadania laboratoryjnego, należy uruchomić aplikację Wireshark (jeżeli nie jest zainstalowana, to najpierw należy ją zainstalować z witryny <https://www.wireshark.org/download.html>).  
  
Ponadto należy w systemie operacyjnym MS Windows dodać odpowiednie wyjątki do wbudowanej w system operacyjny Windows zapory ogniowej, które umożliwią odpowiadanie na komunikaty protokołu *ICMPv4 typu Echo Request*. W tym celu należy przejść do ***Panel sterowania\System i zabezpieczenia\Zapora systemu Windows*** a następnie kliknąć na pozycję ***Ustawienia zaawansowane***, i w lewym panelu okna ***Zapora systemu Windows z ustawieniami zaawansowanymi***, należy wybrać opcję ***Reguły przychodzące***, a następnie w prawym panelu kliknąć pozycję ***Nowa reguła…***

W ramach kreatora nowej reguły należy wybrać jako typ reguły ***Niestandardowa***, a następnie kliknąć przycisk ***Dalej.***  
Następnie w lewym panelu kliknąć opcję ***Protokół i porty***, i używając rozwijanego menu, wybrać opcję ***ICMPv4***, a następnie kliknąć ***Dalej***. Następnie w lewym panelu kliknąć opcję ***Nazwa*** i w polu ***Nazwa*** wpisać jako nazwę ***Zezwól na żądania ICMPv4***. Kliknąć ***Zakończ.***Ta nowa reguła powinna umożliwić otrzymanie odpowiedzi ping dla protokołu IPv4.

Ponadto należy w systemie operacyjnym MS Windows dodać odpowiednie wyjątki do wbudowanej w system operacyjny Windows zapory ogniowej, które umożliwią odpowiadanie na komunikaty protokołu *ICMPv6 typu Echo Request*. W tym celu należy przejść do ***Panel sterowania\System i zabezpieczenia\Zapora systemu Windows*** a następnie kliknąć na pozycję ***Ustawienia zaawansowane***, i w lewym panelu okna ***Zapora systemu Windows z ustawieniami zaawansowanymi***, należy wybrać opcję ***Reguły przychodzące***, a następnie w prawym panelu kliknąć pozycję ***Nowa reguła…***

W ramach kreatora nowej reguły należy wybrać jako typ reguły ***Niestandardowa***, a następnie kliknąć przycisk ***Dalej.***  
Następnie w lewym panelu kliknąć opcję ***Protokół i porty***, i używając rozwijanego menu, wybrać opcję ***ICMPv6***, a następnie kliknąć ***Dalej***. Następnie w lewym panelu kliknąć opcję ***Nazwa*** i w polu ***Nazwa*** wpisać jako nazwę ***Zezwól na żądania ICMPv6***. Kliknąć ***Zakończ.***Ta nowa reguła powinna umożliwić otrzymanie odpowiedzi ping dla protokołu IPv6.

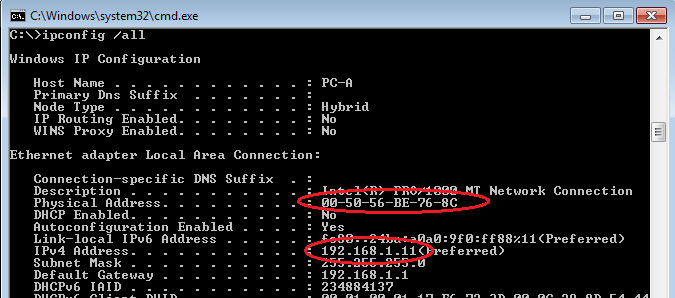
Zadania do realizacji

Krok 1:

Należy odczytać przypisane do interfejsu aktualnie dane adresowe TCP/IP, w tym celu należy:

Otworzyć okno wiersza poleceń w systemie operacyjnym, następnie wpisać polecenie   
***ipconfig /all*** i nacisnąć ***Enter***

Odczytać adres IPv4 oraz adres MAC (tzw. adres fizyczny interfejsu sieciowego) przydzielony dla interfejsu sieciowego, który jest wykorzystywany aktualnie do komunikacji z siecią Internet (w systemie Windows od 8 wzwyż, najczęściej to będzie interfejs o nazwie „Ethernet”):



Zanotuj odczytane ustawienia konfiguracyjne wykorzystywane przez interfejs sieciowy (adres IP/maska podsieci, adres bramy oraz adres MAC):

Adres IP: ***192.168.1.102***

Maska podsieci: ***255.255.255.0***

Adres bramy: ***192.168.1.1***

Adres MAC: ***08-D4-0C-1B-AE-9F***

Adres IPv6 typu link-local: ***fe80::7016:c9f8:440f:d0ce%16***

Krok 2:

W kroku 2 wykorzystany zostanie Wireshark do przechwycenia i analizy ramek Ethernetowych oraz protokołu ARP.

* + 1. Uruchomić aplikację Wireshark i włączyć przechwytywanie ruchu sieciowego na interfejsie, który system operacyjny wykorzystuje do transmisji z siecią Internet.
    2. Otworzyć okno wiersza poleceń w systemie operacyjnym (przy czym należy pamiętać, aby otworzyć tenże wiersz poleceń na uprawnieniach administracyjnych – tj. kliknąć prawym przyciskiem myszy na ikonie wiersza poleceń i wybrać „Uruchom jako administrator”), następnie wpisać polecenie ***arp -d \**** (polecenie to powoduje wyczyszczenie zawartości tablicy ARP) i nacisnąć **Enter,** a następnie polecenie **ping sekurak.pl** i nacisnąć **Enter***.*
    3. Po zakończeniu działania aplikacji ping, zakończyć przechwytywanie ruchu sieciowego w aplikacji Wireshark.
    4. Przejrzyj przechwycone dane w programie Wireshark, i znajdź pierwszą ramkę w ramach której zawarte jest żądanie ***Echo (ping) request*** skierowane na adres IP urządzenia pod adresem sekurak.pl (tenże adres IP można odczytać w wierszu poleceń gdzie wykonane zostało polecenie ping, aplikacja ta wskazuje adres IP na jaki została rozwiązana wskazana nazwa DNS). Następnie należy znaleźć dwie wcześniejsze ramki protokołu DNS znajdujące się najbliżej tegoż żądania ***Echo (ping) request***, którymi powinny być ramki zapytania i odpowiedzi protokołu ARP.
    5. Zaznacz ramkę zapytania ARP, a następnie rozwiń dla tej ramki nagłówki protokołu Ethernet, i odpowiedz na następujące pytania:

Jaki jest adres MAC źródła w pierwszej ramce? ***08-D4-0C-1B-AE-9F***

Która część adresu MAC to OUI? ***08-D4-0C***

Jaki jest producent (OUI) źródłowej karty sieciowej (NIC)? ***Intel***

Jaki jest numer seryjny źródłowej karty sieciowej (NIC)? ***1B-AE-9F***

Odczytaj adres MAC docelowy, i wskaż kto będzie odbiorcą ramki o takim adresie docelowym, jaki jest to rodzaj adresu MAC?

***FF:FF:FF:FF:FF:FF:FF – odbiorcą ramki będzie każde urządzenie.***

Dlaczego komputer PC wysyła rozgłoszenie ARP przed wysłaniem pierwszego żądania ping?

***Aby dowiedzieć się do kogo konkretnie ma skierować swoje zapytanie, ponieważ nie ma wystarczającej ilości informacji (adres MAC) i szuka adresata.***

* + 1. Zaznacz ramkę odpowiedzi ARP, a następnie rozwiń dla tej ramki nagłówki komunikatu protokołu ARP, i wypełnij następującą tabelę korzystając z informacji zawartych w tym drugim przechwyconym komunikacie ARP:

|  |  |
| --- | --- |
| Pole | Wartość |
| **Adres MAC nadawcy** | ***10:C3:7B:4A:A1:FD*** |
| **Adres IP nadawcy** | ***192.168.1.13*** |
| **Docelowy adres MAC** | ***08:D4:0C:1B:AE:9F*** |
| **Docelowy adres IP** | ***192.168.1.102*** |

Krok 3:

W kroku 3 wykorzystany zostanie Wireshark do przechwycenia i analizy komunikatów ARP w celu zbadania opóźnień w sieci spowodowanych przez protokół ARP.

* + 1. Usunąć wpisy ARP w komputerze PC (z wykorzystaniem polecenia ***arp -d \****)
    2. Uruchomić aplikację Wireshark i włączyć przechwytywanie ruchu sieciowego na interfejsie, który system operacyjny wykorzystuje do transmisji z siecią Internet.
    3. Otworzyć okno wiersza poleceń w systemie operacyjnym, a następnie wydać polecenie **ping** skierowane do komputera kolegi/koleżanki (należy w tym celu uzyskać od kolegi/koleżanki adres IP jego/jej komputera PC) i nacisnąć **Enter***.*
    4. Po zakończeniu działania aplikacji ping, zakończyć przechwytywanie ruchu sieciowego w aplikacji Wireshark.
    5. Zbadaj przechwycone przez program Wireshark informacje. Ponieważ w twoim komputerze nie było żadnych wpisów ARP dla komputera kolegi/koleżanki, to najpierw zostało wysłane żądanie ARP na adres IP komputera kolegi/koleżanki z prośbą o adres MAC. Następnie można zauważyć wysłanie komunikatu *ICMP Echo request*, aczkolwiek na to żądanie *Echo request* komputer kolegi/koleżanki nie zwrócił komunikatu *ICMP Echo Reply*, za to komputer kolegi/koleżanki wysłał zapytanie ARP do naszego komputera. Po dodaniu odpowiedniego wpisu ARP do bufora ARP w obydwu komputerach, ostatnie trzy już wymiany komunikatów ICMP zakończyły się pozytywnie.

Wskaż, dlaczego pierwszy „ping” się nie powiódł, tj. dlaczego nie został przez komputer kolegi/koleżanki odesłany komunikat *ICMP Echo Reply*:

***Nie powiódł się, ponieważ w tablicy ARP drugiego komputera nie było jeszcze danych  
o naszym komputerze. Zanim komputer je uzyskał (poprzez zapytanie) czas oczekiwania na odpowiedź polecenia ping się skończył i wyświetlił się błąd.***

Dlaczego w ogóle komputer kolegi/koleżanki wysłał do nas zapytanie ARP, jeżeli wcześniej otrzymał choćby w komunikacie *ICMP Echo Request* adres MAC naszego komputera?

***Komputer wysłał do nas zapytanie, ponieważ nie miał wcześniej odpowiedniego wpisu  
w swojej tablicy ARP. Taki wpis można zrobić ręcznie bądź poprzez zapytanie. Samo wysłanie ping’a nie skutkuje zapisem odpowiednich danych na komputerze adresata.***

Jeżeli żądania ARP mogą spowodować opóźnienia w sieci, dlaczego złym pomysłem jest to, aby czas dla utrzymywania wpisów ARP był nieograniczony?

**W przypadku zmiany karty sieciowej powodowałoby to problemy z komunikacją  
z wcześniej zapisanymi danymi w tablicach. Ten sam adres IP miałby nowy adres MAC, przez co urządzenia nie mogłyby się komunikować.**

* + 1. Analizując przechwycone ramki, wskaż jaki adres MAC ma komputer kolegi/koleżanki:

***10:C3:7B:4A:A1:FD***

Krok 4:

W kroku 4 wykonana zostanie analiza zastosowania tablicy ARP w systemie operacyjnym, na przykładzie systemu MS Windows.

* + 1. Usunąć wpisy ARP w komputerze PC (z wykorzystaniem polecenia ***arp -d \****)
    2. Otworzyć okno wiersza poleceń w systemie operacyjnym, a następnie wydać polecenie **arp** i nacisnąć **Enter***.*
    3. Przeanalizuj wynik działania tego polecenia i odpowiedz na bazie wyświetlonych informacji na następujące pytania:

Które polecenie powinno być użyte do wyświetlenia wszystkich wpisów znajdujących się w buforze ARP?

***arp -a***

Jakie polecenie powinno zostać użyte do skasowania wszystkich wpisów znajdujących się w buforze ARP (opróżnienie pamięci podręcznej ARP)?

***arp -d \****

Jakiego polecenia należałoby użyć, aby usunąć wpis z bufora ARP dla np. adresu 192.168.1.11?

***arp -d 192.168.1.11***

* + 1. Otworzyć okno wiersza poleceń w systemie operacyjnym, a następnie wydać polecenie **arp -a** i nacisnąć **Enter***.* Wskaż jakie dynamicznie uzyskane wpisy znajdują się obecnie w tablicy ARP:

***192.168.1.1 d0-96-fb-50-3e-3f dynamic***

***192.168.1.11 60-32-b1-4c-13-fa dynamic***

***192.168.1.13 10-c3-7b-4a-a1-fd dynamic***

***192.168.1.15 10-4a-7d-65-e4-24 dynamic***

* + 1. Otworzyć okno wiersza poleceń w systemie operacyjnym, wydać polecenie **ping** skierowane na adres IP bramy, a następnie skierowane na adres IP komputera kolegi/koleżanki, w celu dodania dynamicznych wpisów do tablicy ARP.

Otworzyć okno wiersza poleceń w systemie operacyjnym, a następnie wydać polecenie **arp -a** i nacisnąć **Enter***.* Na bazie wyświetlonych informacji odpowiedz na następujące pytania:

Wskaż jaki jest adres fizyczny bramy?

***d0-96-fb-50-3e-3f***

Wskaż jaki jest adres fizyczny komputera kolegi/koleżanki?

***10-c3-7b-4a-a1-fd***

* + 1. Usunąć wpisy ARP w komputerze PC (z wykorzystaniem polecenia ***arp -d \****)
    2. Otworzyć okno wiersza poleceń w systemie operacyjnym, a następnie dodać statyczny wpis do bufora ARP za pomocą polecenia **arp –s *inet\_addr mac\_addr***, gdzie dla adresu IP bramy należy przyporządkować adres MAC 0c-d9-96-d2-40-40, a dla adresu IP komputera kolegi/koleżanki należy przyporządkować adres MAC 0c-d9-96-d2-40-50.

Przykładowe polecenie:

C:\windows\system32> **arp –s 192.168.1.12 0c-d9-96-d2-40-40**

* + 1. Otworzyć okno wiersza poleceń w systemie operacyjnym, wydać polecenie **ping** skierowane na adres IP bramy, a następnie skierowane na adres IP komputera kolegi/koleżanki.

Wskaż, dlaczego polecenie ping się nie powiodło:

***Polecenie się nie powiodło, ponieważ adres MAC w tablicy ARP naszego komputera różni się od faktycznego adresu na urządzeniu, do którego kierujemy zapytanie. Adresat ignoruje to zapytanie, ponieważ sądzi, że nie jest ono skierowane do niego.***

Krok 5:

W kroku 5 wykonana zostanie analiza zastosowania protokołu Neighbor Discovery, na przykładzie systemu MS Windows.

* + 1. Otworzyć okno wiersza poleceń w systemie operacyjnym, a następnie wydać polecenie **netsh interface ipv6 show address** i nacisnąć **Enter**.

Bazując na wyniku wykonania w/w polecenia, wskaż jaki adres/adresy są aktualnie skonfigurowane na interfejsie, jaki twój komputer wykorzystuje do komunikacji z siecią Internet:

***fe80::7016:c9f8:440f:d0ce%16***

* + 1. Otworzyć okno wiersza poleceń w systemie operacyjnym, a następnie wydać polecenie **netsh interface ipv6 show neighbor** i nacisnąć **Enter***.* Wskaż jakie dynamicznie uzyskane wpisy znajdują się obecnie w tablicy sąsiedztwa na interfejsie, jaki twój komputer wykorzystuje do komunikacji z siecią Internet:

***fe80::43:cde2:62d0:f867 10-C3-7B-4A-A1-FD Stale***

* + 1. Otworzyć okno wiersza poleceń w systemie operacyjnym, wydać polecenie **ping** skierowane na adres IPv6 komputera kolegi/koleżanki, w celu dodania dynamicznych wpisów do tablicy sąsiedztwa.

Otworzyć okno wiersza poleceń w systemie operacyjnym, a następnie wydać polecenie **netsh interface ipv6 show neighbor** i nacisnąć **Enter***.* Na bazie wyświetlonych informacji tablicy sąsiedztwa dla interfejsu, jaki twój komputer wykorzystuje do komunikacji z siecią Internet odpowiedz na następujące pytania:

Wskaż jaki jest adres fizyczny komputera kolegi/koleżanki?

***10-c3-7b-4a-a1-fd***

* + 1. Otworzyć okno wiersza poleceń w systemie operacyjnym (przy czym należy pamiętać, aby otworzyć tenże wiersz poleceń na uprawnieniach administracyjnych – tj. kliknąć prawym przyciskiem myszy na ikonie wiersza poleceń i wybrać „Uruchom jako administrator”), a następnie wydać polecenie **netsh interface ipv6 delete neighbors** i nacisnąć **Enter** (polecenie czyści tablicę sąsiedztwa z uzyskanych dynamicznie wpisów)*.*

Następnie w oknie wiersza poleceń w systemie operacyjnym wydać polecenie **netsh interface ipv6 show neighbor** i nacisnąć **Enter**. Na bazie wyświetlonych informacji tablicy sąsiedztwa dla interfejsu, jaki twój komputer wykorzystuje do komunikacji z siecią Internet odpowiedz na następujące pytania:

Wskaż czy w tablicy sąsiedztwa na interfejsie, jaki twój komputer wykorzystuje do komunikacji z siecią Internet, nadal widnieje adres fizyczny komputera kolegi/koleżanki:

***Został usunięty (Unreachable).***

* + 1. Uruchomić aplikację Wireshark i włączyć przechwytywanie ruchu sieciowego na interfejsie, który system operacyjny wykorzystuje do transmisji z siecią Internet.
    2. Otworzyć okno wiersza poleceń w systemie operacyjnym, następnie wykonać polecenie **ping** na adres IPv6 typu link-local komputera kolegi/koleżanki i nacisnąć **Enter***.*
    3. Po zakończeniu działania aplikacji ping, zakończyć przechwytywanie ruchu sieciowego w aplikacji Wireshark.
    4. W ramach przechwyconego ruchu, należy znaleźć dwie ramki odpowiedzialne za rozwiązanie adresów IPv6 na adresy MAC, i na bazie informacji w nich zawartych odpowiedzieć na pytania:

Wskaż jaki protokół został wykorzystany do przesłania komunikatów *Neighbor Solicitation* oraz *Neighbor Advertisement*:

***ICMPv6***

Wskaż zawartość pola typ oraz pola kod zapytania *Neighbor Solicitation*:

***Typ: Neighbor Solicitation (135)***

***Kod: 0***

Wskaż adres IPv6 oraz adres MAC na jaki zostało wysłane zapytanie *Neighbor Solicitation*, jak również jaki to jest typ adresu:

***IPv6: ff02::1:ff4e:822d MAC: 33:33:ff:4e:82:2d***

Wskaż zawartość pola typ oraz pola kod odpowiedzi *Neighbor Advertisement*:

***Typ: Neighbor Advertisement (136)***

***Kod: 0***

Wskaż adres IPv6 oraz adres MAC na jaki została wysłana odpowiedź *Neighbor Advertisement*, jak również jaki to jest typ adresu:

***IPv6: fe80::655b:25a:76ff:9bc9 MAC: 00:90:fa:1a:87***

Wskaż jaki adres MAC został przekazany w odpowiedzi *Neighbor Advertisement*:

***MAC: dc:a6:32:b7:f6:1f***