Instrukcja laboratoryjna dla „Sieci komputerowe i Internet” – Moduł 2, Zadanie 3 *– Radosław Terelak*

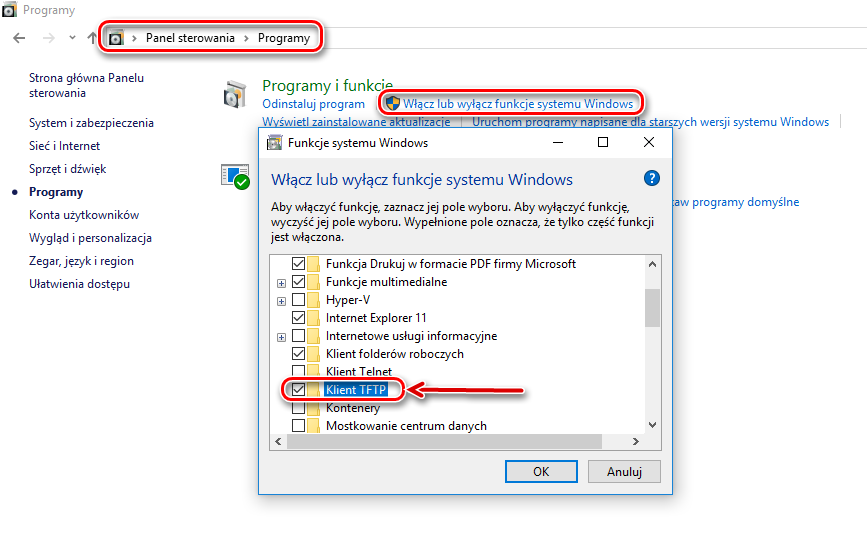
1. Cele zadania laboratoryjnego:

Celem zadania laboratoryjnego jest obserwacja transmisji danych wykorzystującej protokół UDP.

1. Przygotowanie środowiska do zajęć:

W ramach przygotowania środowiska do wykonania zadania laboratoryjnego, należy:

* 1. Zainstalować w systemie operacyjnym Windows aplikację serwera TFTP z witryny: <http://tftpd32.jounin.net/tftpd32_download.html>
  2. Zainstalować w systemie operacyjnym Windows aplikację klienta TFTP, w tym celu należy przejść do ***Panel sterowania/Programy*** a następnie kliknąć pozycję ***Włącz lub wyłącz funkcje system Windows***, a następnie w oknie, które się pojawiło zaznaczyć pozycję ***Klient TFTP*** i nacisnąć przycisk ***OK***:



* 1. Dodać odpowiednie wyjątki do wbudowanej w system operacyjny Windows zapory ogniowej, które umożliwią połączenie zarówno z klientem jak z serwerem TFTP. 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 ***Program***, a następnie jako ***Ta ścieżka programu:*** podać ***%SystemRoot%\System32\TFTP.EXE***  
Następnie w lewym panelu, kliknąć opcję ***Nazwa*** i w polu ***Nazwa*** wpisać jako nazwę ***Zezwól na połączenia do klienta TFTP***. Kliknąć ***Zakończ***.

Następnie dodać jeszcze jedną regułę przychodzącą, i w ramach kreatora tej nowej reguły należy wybrać jako typ reguły ***Program***, a następnie jako ***Ta ścieżka programu:*** podać ***C:\Program Files\Tftpd64\tftpd64.exe*** (o ile w trakcie instalacji aplikacji serwera TFTP została wybrana domyślna ścieżka instalacji, jeżeli została wybrana inna, należy odpowiednio wskazać prawidłową ścieżkę do pliku tftpd46.exe)  
Następnie w lewym panelu, kliknąć opcję ***Nazwa*** i w polu ***Nazwa*** wpisać jako nazwę ***Zezwól na połączenia do serwera TFTP***. Kliknąć ***Zakończ***:

* 1. Utworzyć na dysku C katalog o nazwie ***Dane***, i następnie pobrać do niego plik ***disk2vhd.exe*** z witryny: <https://docs.microsoft.com/en-us/sysinternals/downloads/disk2vhd>   
     Utworzyć na dysku C również katalog o nazwie ***Dane2***.
  2. Uruchomić aplikację Wireshark (jeżeli nie jest zainstalowana, to najpierw należy ją zainstalować z witryny <https://www.wireshark.org/download.html>).

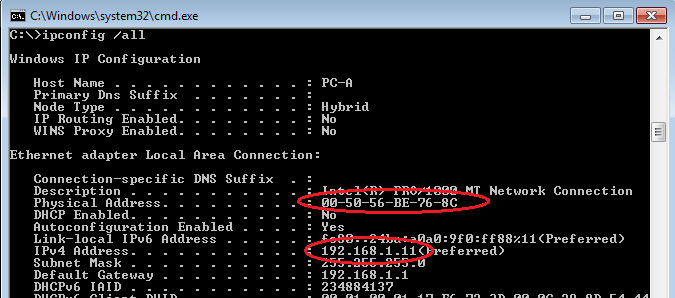
Zadania do realizacji

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, oraz adres MAC):

Adres IP hosta: ***192.168.1.101***

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

Krok 2:

W tym kroku zostanie przechwycony ruch aplikacji ping skierowanej do urządzenia wskazanego z użyciem nazwy DNS. Analiza poniższa ma udowodnić, że zanim nastąpi połączenie właściwej aplikacji z urządzeniem przez sieć komputerową, to najpierw zostaje wysłane zapytanie do serwera DNS w celu rozwiązania wskazanej nazwy DNS na adres IP, i następnie serwer DNS zwraca odpowiedź. Zapytanie i odpowiedź DNS przesyłane są z wykorzystaniem protokołu UDP, co pozwoli również na analizę działania tegoż protokołu.

Uruchomić aplikację Wireshark i włączyć przechwytywanie ruchu sieciowego na interfejsie, który system operacyjny wykorzystuje do transmisji z siecią Internet.

Otworzyć okno wiersza poleceń w systemie operacyjnym, następnie wpisać polecenie i***pconfig /flushdns*** (polecenie to powoduje wyczyszczenie pamięci podręcznej klienta DNS) i nacisnąć **Enter,** a następnie polecenie **ping sekurak.pl** i nacisnąć **Enter***.*

Po zakończeniu działania aplikacji ping, zakończyć przechwytywanie ruchu sieciowego w aplikacji Wireshark.

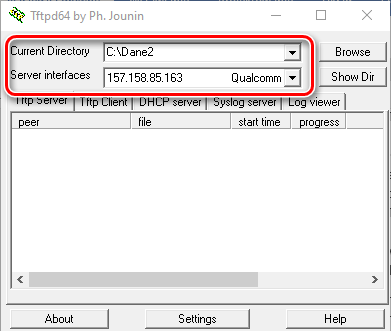
Przejrzyj przechwycone dane w programie Wireshark, i znajdź pierwszą ramkę w ramach której zawarte jest żądanie ***Echo (ping) request*** skierowane na adres IP urządzenia pod adresem sekurak.pl (tenże adres IP można odczytać w wierszu poleceń gdzie wykonane zostało polecenie ping, aplikacja ta wskazuje 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***.  
  
Zaznaczyć pierwszą z tychże dwóch ramek protokołu DNS, które zawiera zapytanie do serwera DNS o rozwiązanie wskazanej nazwy na adres IP i następnie w środkowej sekcji aplikacji Wireshark rozwinąć nagłówki protokołu UDP oraz zawartość wiadomości protokołu DNS.   
  
Odczytaj z informacji w nagłówkach dla w/w ramki, i wskaż, jaki był adres serwera DNS, który został wykorzystany przez klienta DNS do procesu rozwiązania nazwy sekurak.pl na adres IP:   
***185.124.116.186***  
  
Odczytaj z informacji w komunikacie protokołu DNS, i wskaż, o jaki typ rekordu DNS zostało przekazane zapytanie:   
***sekurak.pl: type A, class IN***  
  
Odczytaj z informacji w nagłówkach protokołu UDP, i wskaż, jaki był wykorzystany port źródłowy oraz port docelowy:   
***Źródłowy: 59163 Docelowy: 53***   
  
Przejrzyj wymianę ramek pomiędzy swoim komputerem a serwerem DNS, i wskaż czy widać w ramach tej komunikacji mechanizm potwierdzeń, jak również mechanizm trójetapowego zestawienia połączenia, oraz mechanizm zakończenia połączenia?   
***Nie ma takich mechanizmów, w tej komunikacji liczy się szybkość, dlatego nie są używane.***

W wierszu poleceń systemu Windows wpisać polecenie ***ipconfig /displaydns*** i odnaleźć w wyświetlonej pamięci podręcznej rekord dla nazwy sekurak.pl, a następnie odczytaj i wskaż następne informacje/wartości:  
Adres IP: ***51.77.40.125***  
Time To Live: ***246***

W wierszu poleceń systemu Windows ponownie wpisać polecenie ***ipconfig /displaydns*** i odnaleźć w wyświetlonej pamięci podręcznej rekord dla nazwy sekurak.pl, a następnie odczytaj i wskaż następne informacje/wartości:  
Time To Live: ***191***  
  
Porównując powyższą wartość z wartością podaną we wcześniejszym punkcie wskaż jaka może być logika działania tegoż mechanizmu TTL:  
***Wartość TTL określa jak długo dany adres IP oraz powiązane z nim dane będą znajdować się w naszej pamięci podręcznej. Po upływie tego czasu, aby nawiązać połączenie, należy ponowić zapytanie do serwera DNS.***

Krok 3:

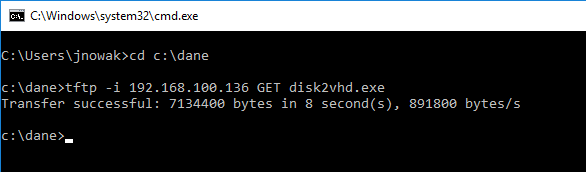
W tym kroku zostanie przechwycony ruch aplikacji TFTP, służącej do przesyłania plików pomiędzy urządzeniami znajdującymi się z założenia w tej samej lokalnej sieci komputerowej i wykorzystującej do tego celu protokół UDP. Analiza poniższa ma udowodnić, że mimo zastosowania protokołu UDP pozbawionego mechanizmu potwierdzeń i retransmisji, możliwe jest przy pewnych założeniach wykorzystanie go do przesyłania danych, gdzie zależy nam mimo wszystko na przesłaniu ich w stanie pełnym.

Uruchomić aplikację serwera TFP, a następnie jako katalog wskazać ***C:\Dane2*** (w którym znajduje się wcześniej pobrany plik disk2vhd.exe), oraz z listy interfejsów wybrać ten, który aktualnie jest wykorzystywany przez system operacyjny do komunikacji z lokalną siecią komputerową (po dokonanej konfiguracji, aplikacja ma zostać cały czas uruchomiona w tle):  


Dobierz się w parę z kolegą/koleżanką obok i poproś go/ją o podanie adresu IPv4 jej/jego komputera, oraz przekaż swój.   
Zanotuj adres IPv4 komputera kolegi/koleżanki: ***nie dotyczy***

Uruchomić aplikację Wireshark i włączyć przechwytywanie ruchu sieciowego na interfejsie, który system operacyjny wykorzystuje do transmisji z lokalną siecią komputerową.

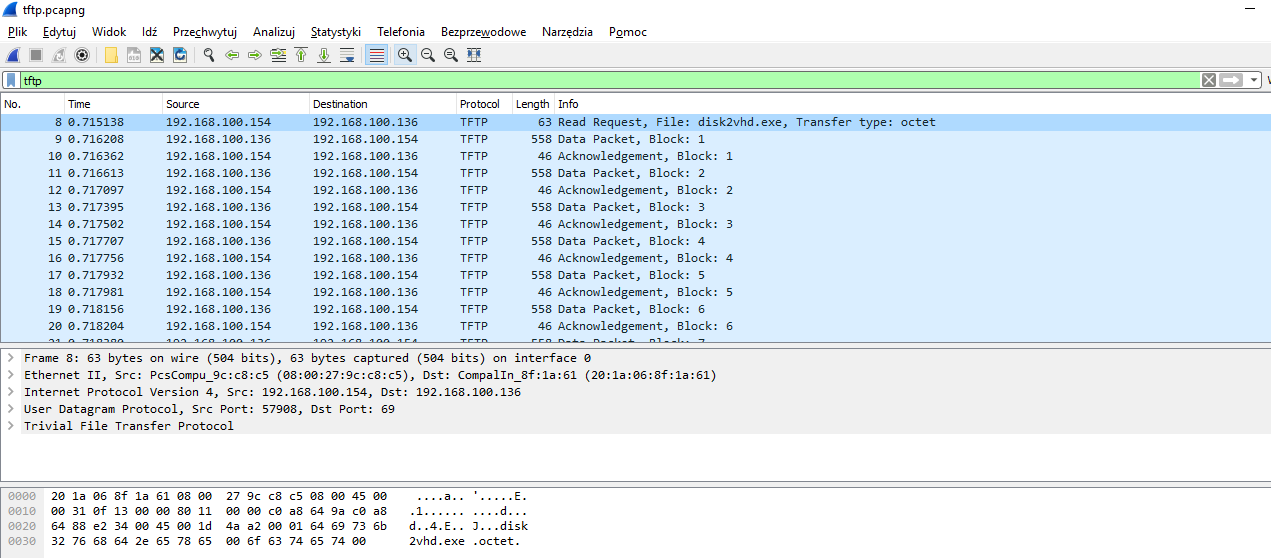
Otworzyć okno wiersza poleceń w systemie operacyjnym, następnie wpisać polecenie cd ***C:\Dane*** (polecenie to spowoduje przejście do katalogu C:\Dane), a następnie polecenie   
***tftp -i 192.168.100.136 GET disk2vhd.exe*** (przy czym w poleceniu tymże adres IP należy wymienić na właściwy adres IP wskazany we wcześniejszym punkcie „b” przez kolegę/koleżankę) i nacisnąć **Enter** (nastąpi pobranie pobranie pliku disk2vhd.exe z komputera koleżanki/kolegi do katalogu C:\Dane):

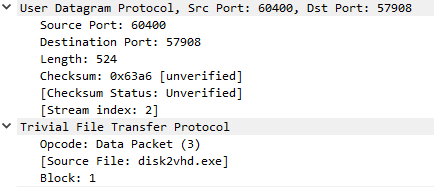


Po zakończonym pobieraniu pliku zakończyć przechwytywanie ruchu sieciowego w aplikacji Wireshark (w razie czego w platformie Moodle znajduje się gotowy plik do pobrania dla aplikacji Wireshark z już przechwyconym w/w ruchem transmisji FTP), i sprawdzić w katalogu ***C:\Dane*** czy plik został faktycznie pobrany.

**Uwaga:** Jeżeli plik nie został pobrany to problem może wynikać z nieprawidłowego dodania reguł do zapory ogniowej (muszą być dodane odpowiednie reguły zarówno dla klienta TFTP jak i serwera TFTP), podania nieprawidłowego adresu IP w poleceniu, bądź problemów z komunikacją między dwoma urządzeniami (co można zweryfikować poleceniem ping, pamiętając również o problemie dodania odpowiednich reguł zapory ogniowej na komputerze, do którego polecenie ping jest skierowane).

W aplikacji Wireshark polu ***Filter***, znajdującym się w górnej części programu Wireshark należy wpisać ***tftp*** i kliknąć przycisk ***Zastosuj filtr*** lub nacisnąć ***Enter***.

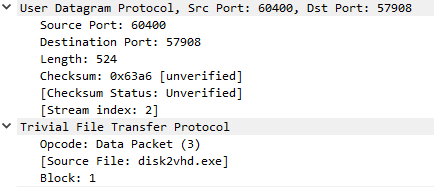


Zaznaczyć w górnej sekcji aplikacji Wireshark drugą ramkę transmisji protokołu TFTP, która de facto jest pierwszą ramką w ramach przesyłania pliku. Następnie należy w środkowej sekcji aplikacji Wireshark rozwinąć nagłówki wykorzystywanego protokołu warstwy transportowej, jak również komunikat protokołu TFTP.  


Odczytaj i wskaż jaki protokół warstwy transportowej został wykorzystany do procesu przesyłania pliku:

***UDP***  
  
Odczytaj i wskaż jaki był wykorzystany port źródłowy oraz port docelowy:   
***Źródłowy: 60400 Docelowy: 57908***

Odczytaj i wskaż z komunikatu protokołu TFTP jakie jest przeznaczenie/cel/zawartość tejże przesyłanej ramki:   
***Przesłanie pierwszego fragmentu/bloku pliku.***

Zaznaczyć w górnej sekcji aplikacji Wireshark trzecią ramkę transmisji protokołu TFTP, która de facto jest drugą ramką w ramach przesyłania pliku. Następnie należy w środkowej sekcji aplikacji Wireshark rozwinąć nagłówki wykorzystywanego protokołu warstwy transportowej, jak również komunikat protokołu TFTP.  
  
  
  
Odczytaj i wskaż jaki protokół warstwy transportowej został wykorzystany do procesu przesyłania pliku:

***UDP***  
  
Odczytaj i wskaż jaki był wykorzystany port źródłowy oraz port docelowy, oraz jaka zmiana nastąpiła porównując do wartości wskazanych dla poprzedniej ramki (rozpatrywanej w poprzednim punkcie):   
***Źródłowy: 57908 Docelowy: 60400, porty zamieniły się miejscami.***

Odczytaj i wskaż z komunikatu protokołu TFTP jakie jest przeznaczenie/cel/zawartość tejże przesyłanej ramki, oraz jaki wniosek z tego można wysnuć biorąc pod uwagę zawartość również komunikatu poprzedniej ramki (rozpatrywanej w poprzednim punkcie):

***Potwierdzenie odbioru pierwszego fragmentu/bloku pliku. Wynika z tego, że każdy etap przesyłania danych otrzymuje informację zwrotną o poprawnym pobraniu fragmentu pliku.***

Zamknąć aplikację serwera TFTP oraz aplikację Wireshark.