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

1. Cele zadania laboratoryjnego:

Celem zadania laboratoryjnego jest obserwacja transmisji danych wykorzystującej protokół TCP.

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>).

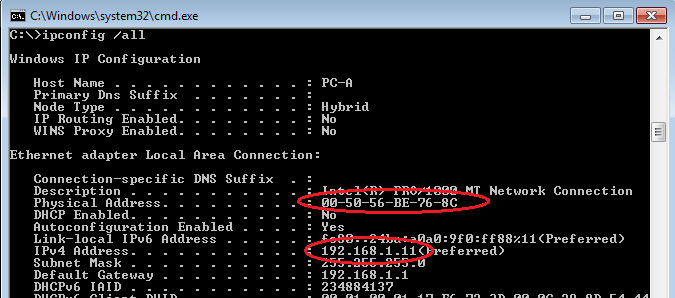
Zadania do realizacji

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***

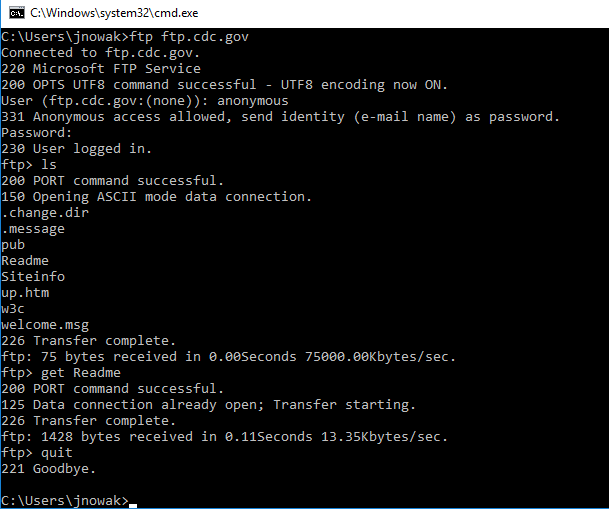
Adres MAC hosta: ***08-D4-0C-1B-AE-9F***

Krok 2:

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   
**ftp ftp.cdc.gov** i nacisnąć **Enter**

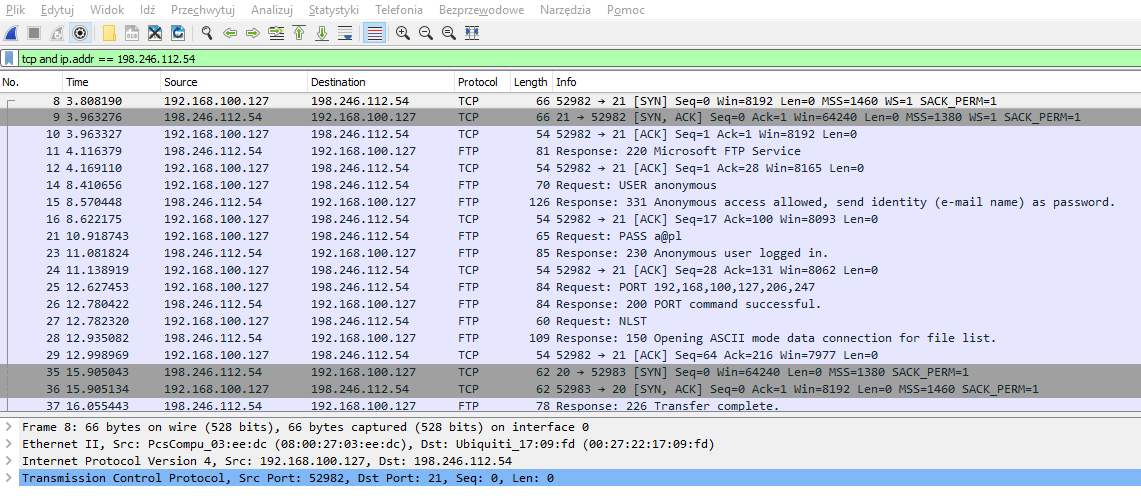
Zalogować się używając konta ***anonymous*** oraz dowolnego hasła

Wylistować zawartość zasobu FTP wykorzystując polecenia ***ls***, i następnie pobrać plik Readme wykorzystując polecenie ***get Readme***:  


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).

Krok 2:

1. Wireshark przechwycił wiele pakietów w trakcie sesji FTP do strony ftp.cdc.gov. Aby ograniczyć ilość danych do analizy, w polu filtru należy wpisać ***tcp and ip.addr == 198.246.112.54*** i zatwierdzić naciskając ***Enter*** (adres IP 198.246.112.54 jest adresem zasobu ftp.cdc.gov).  
   **Uwaga:** jeżeli powyższy filtr nie działa, to należy wykonać w wierszu poleceń polecenie ***ping ftp.cdc.gov***, odczytać adres IP na jaki aktualnie nakierowana jest w/w nazwa DNS, i w filtrze wskazać tenże odczytany aktualny prawidłowy adres IP.



1. Po zastosowaniu filtru, pierwsze trzy ramki w okienku listy przechwyconych ramek (górna sekcja) stanowią sekwencję segmentów z ustawionymi flagami [SYN], [SYN, ACK], [ACK], która to sekwencja ilustruje tzw. 3-etapowe uzgodnienie sesji:



* + 1. W powyższym przykładzie ramka 8 jest początkiem procesu uzgadniania trójetapowego pomiędzy komputerem PC i serwerem ftp. W panelu listy ramek (górna część okna głównego), zaznacz pierwszą ramkę z ustawioną flagą SYN. Po zaznaczeniu linii pokażą się dodatkowe zdekodowane informacje o zawartości pakietu w dwóch dolnych panelach. Sprawdź informacje dotyczące protokołu TCP w okienku szczegółów pakietu (środkowa część okna głównego).

Tj. w panelu dotyczącym szczegółów ramki kliknąć ikonę **>** znajdującą się po lewej stronie pozycji ***Transmission Control Protocol***, aby rozwinąć informacje szczegółowe odnośnie nagłówków protokołu TCP.

Następnie kliknij ikonę **>** znajdującą się po lewej stronie wyrażenia ***Flags***.

Odczytaj w nagłówkach protokołu TCP numery portów źródłowych i docelowych oraz flagi, które są ustawione.

Wskaż jaki jest numer portu źródłowego TCP? ***52982***

Wskaż, jak można sklasyfikować w/w port źródłowy? (tj. jakiego typu jest to port źródłowy) - ***Ten port źródłowy można sklasyfikować jako port dynamiczny.***

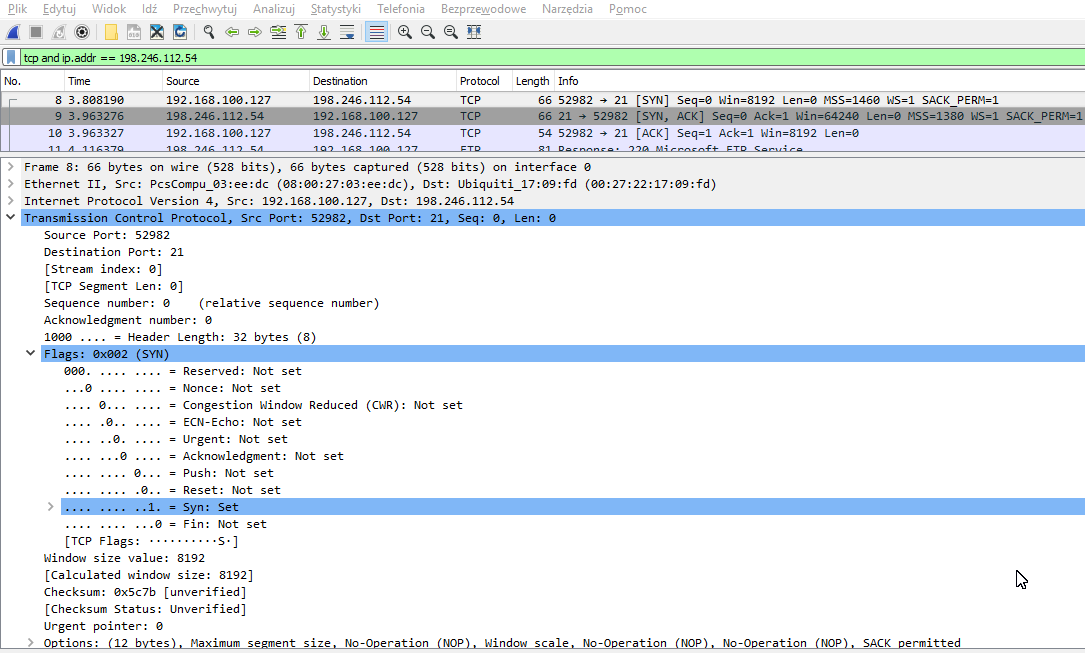
Wskaż jaki jest numer portu docelowego TCP? ***21***

Wskaż, jak można sklasyfikować w/w port docelowy? (jakiego typu jest to port docelowy) - ***Jest to port typu dobrze znanego, czyli ogólnie przyjętego do wykonywania określonych czynności.***

Wskaż, która flaga (lub flagi) w nagłówkach TCP są ustawione (1)? ***Jedynie flaga Syn ustawiona jest na 1. Odpowiada ona za nawiązywanie połączenia.***

Wskaż jaka jest wartość numeru sekwencyjnego w nagłówkach protokołu TCP?

***Wartość numeru sekwencyjnego wynosi 0***.  
  
Wskaż jaka jest wielkość (w bajtach) nagłówków protokołu TCP (co należy odczytać z informacji w nagłówkach TCP): ***32 bajty***



1. Wybrać kolejną drugą ramkę z trójetapowego procesu uzgadniania sesji i rozwinąć nagłówki protokołu TCP.   
     
   Wskaż jakie są wartości portów źródłowych i docelowych: ***Źródłowy: 21, Docelowy: 52982***  
   Wskaż, która flaga (lub flagi) są ustawione (1)?

***Flaga Syn oraz flaga Acknowledgment.***

Wskaż, jakie są względne numery sekwencyjne i potwierdzenia?

***Sekwencyjny 0, potwierdzenia 1.***

1. Wybrać ostatnią trzecią ramkę z trójetapowego procesu uzgadniania sesji i rozwinąć nagłówki protokołu TCP.   
     
   Wskaż, która flaga (lub flagi) są ustawione (1)?

***Jedynie flaga Acknowledgment.***

Względne numery sekwencyjne oraz potwierdzenie są ustawione na 1. Dopiero teraz jest ustanowione połączenie TCP i możliwa jest komunikacja pomiędzy komputerem a serwerem.

1. Znaleźć pierwszą ramkę normalnej już transmisji danych w ramach której przekazany jest komunikat ***Response***.

Wskaż jakie są wartości portów źródłowych i docelowych: ***Źródłowy: 21, Docelowy: 52982***  
Wskaż, jakie są względne numery sekwencyjne i potwierdzenia?

***Sekwencyjny 1, potwierdzenia 1.***  
Wskaż jaka jest wskazana wielkość danych zawartych w segmencie (w bajtach): ***27 bajtów***

1. Znaleźć ramkę stanowiącą odpowiedź hosta na przesłaną wcześniej przez serwer ramkę z komunikatem ***Response***.  
   Wskaż jakie są wartości portów źródłowych i docelowych: ***Źródłowy: 52982, Docelowy: 21***  
   Wskaż, która flaga (lub flagi) są ustawione (1)? ***Jedynie flaga Acknowledgment.***

Wskaż, jakie są względne numery sekwencyjne i potwierdzenia? ***Sekwencyjny 1, potwierdzenia 28.***

1. Znaleźć drugą ramkę, w ramach której przekazany jest komunikat ***Response*** (331 Anonymous access allowed …).

Wskaż jakie są wartości portów źródłowych i docelowych: ***Źródłowy: 21, Docelowy: 52982***  
Wskaż, jakie są względne numery sekwencyjne i potwierdzenia?

***Sekwencyjny 28, potwierdzenia 17.***  
Wskaż jaka jest wskazana wielkość danych zawartych w segmencie (w bajtach): ***72 bajty***

1. Znaleźć ramkę stanowiącą odpowiedź hosta na przesłaną wcześniej przez serwer ramkę z komunikatem ***Response***.  
     
   Wskaż jakie są wartości portów źródłowych i docelowych: ***Źródłowy: 52982, Docelowy: 21***  
   Wskaż, która flaga (lub flagi) są ustawione (1)? ***Jedynie flaga Acknowledgment.***  
   Wskaż, jakie są względne numery sekwencyjne i potwierdzenia?

***Sekwencyjny 17, potwierdzenia 100.***

Analizując informacje w punktach „f - h”, wskaż jak obliczana jest wartość numeru potwierdzenia:  
***Numer sekwencyjny początkowo jest równy 0. Każdy kolejny to wartość numeru potwierdzenia z poprzedniej ramki. Numer potwierdzenia to suma wielkości danych zawartych w segmencie poprzedniej ramki oraz numeru sekwencyjnego poprzedniej ramki.***

1. Znaleźć ramkę, w ramach której widać proces przesyłania podanego hasła w ramach procesu uwierzytelniania.  
     
   Czy podane hasło w ramach przechwyconej ramki zgadza się z hasłem podanym w procesie logowania do zasobu FTP? ***Zgadza się, jest to: a@pl***
2. Znaleźć ramkę w ramach której widać przekazane polecenie pobrania pliku Readme (***RETR Readme***).  
   Prześledzić następnie ramki odpowiadające za proces pobrania pliku.  
     
   Wskaż jakie są wartości portów źródłowych i docelowych użytych w procesie pobierania pliku: ***Źródłowy: 20, Docelowy: 52984***   
   Porównując z informacjami zebranymi wcześniej dla procesu trójetapowego uzgadniania, wskaż co ciekawego można wywnioskować przeglądając informacje o ramkach odpowiadających za proces pobrania pliku :  
   ***Zostaje nawiązane nowe połączenie na porcie 20, a nie jak dotychczas na 21. Po stronie hosta zostaje wykorzystany kolejny port dynamiczny o jeden wyższy od poprzednio używanego.***
3. Przejść na koniec listy ramek w ramach przechwyconej sesji FTP.

Wskaż jakie 4 segmenty z jakimi ustawionymi flagami kończą sesję FTP:  
***[FIN, ACK] – flagi: Acknowledgment, Fin***

***[FIN, ACK] – flagi: Acknowledgment, Fin***

***[ACK] – flagi: Acknowledgment***

***[ACK] – flagi: Acknowledgment***