Zadania

1. Uruchomić program Wireshark
2. Pole capture filter należy pozostawić puste
3. Wybrać interfejs wykorzystywany do połączenia z siecią poprzez dwukrotne kliknięcie
4. Wykonać następujące czynności:
    a) uruchomić przeglądarkę i wejść na stronę www: http://.....
    b) uruchomić linię poleceń (cmd.exe) i wykonać ping do adresu: .....
    c) wykonać połączenie z serwerem ftp: ftp://.....

5. Po wykonaniu wybranych połączeń należy zakończyć przechwytywanie pakietów
6. Wykorzystując stworzony zapis ruchu sieciowego należy wykonać następujące operacje:

    a) wykonać zrzut ekranu przedstawiający żądanie i odpowiedź DNS dla domeny ustalonej w punkcie 4a, (ważne, aby rozwinięte były wszystkie warstwy od 3 wzwyż, czyli od IP)
    b) na podstawie odpowiedzi z serwera DNS określić adresy IP powiązane z domeną ustaloną w punkcie 4a
    c) wykonać zrzut ekranu przedstawiający pakiety odpowiedzialne za nawiązanie połączenia TCP (tzw. Three-way handshake) z domeną ustaloną w punkcie 4a
    d) dla połączenia z punktu 4a wykonać zrzut ekranu przedstawiający żądanie HTTP GET oraz odpowiedź na to żądanie
    e) wykonać zrzut ekranu pakietów ICMP Echo Request i Echo Reply powiązanych z wykonanym poleceniem ping do adresu z punktu 4b
    f) wykonać zrzuty ekranu pakietów zawierających początkową fazę komunikacji z serwerem ftp: wysłanie loginu (+odpowiedź), wysłanie hasła (+odpowiedź), żądanie nazwy aktualnego katalogu po stronie serwera (+odpowiedź), żądanie o zawartości aktualnego katalogu po stronie serwera (+odpowiedź)
    g) dla połączenia z punktu 4a wykonać zrzut ekranu przedstawiający żądanie HTTP POST oraz odpowiedź na to żądanie

UWAGA! W przypadku braku pakietów DNS związanych z wykonanymi połączeniami należy uruchomić linię poleceń, następnie wpisać `ipconfig /flushdns`, a następnie powtórzyć przechwytywanie pakietów.

Wyniki pomiarów:

a) Przedstawić zrzuty ekranów dla podpunktów 6a-g
b) Przedstawić w formie tabelarycznej:

- zawartość pakietu zawierającego żądanie do serwera DNS (nagłówki warstwy 3, 4 i 5) (punkt 6a).
- zawartość pakietu zawierającego odpowiedź z serwera DNS (nagłówki warstwy 3, 4 i 5).
- zawartość pakietów (nagłówki IP i TCP) odpowiedzialnych za nawiązanie połączenia TCP (tzw. Three-way handshake) (punkt 6c)
- zawartość pakietu (nagłówki IP, TCP i HTTP) zawierającego żądanie HTTP GET oraz odpowiedź (punkt 6d)
- zawartość nagłówków ICMP Echo Request i Echo Reply (punkt 6e)

c) Na podstawie pakietów DNS napisać jakie adresy IP są przypisane do badanych domen
d) Opisać co zawierała odpowiedź na żądanie HTTP GET
e) Opisać co zawierała odpowiedź na żądanie HTTP POST
f) Na podstawie analizy pakietów FTP ocenić bezpieczeństwo korzystania z tego protokołu
g) Przedstawić wnioski z wykonanego ćwiczenia