# Netstat i Wireshark: Analiza TCP, UDP oraz FTP/TFTP

Eksploatacja Lokalnych Sieci Komputerowych

---

## Cele zajęć

1. Zaznajomienie się z narzędziem Netstat oraz jego zastosowaniem do monitorowania połączeń TCP i UDP
2. Analiza nagłówków TCP i UDP przy użyciu Wiresharka.
3. Śledzenie sesji FTP oraz analiza nagłówka UDP w połączeniu TFTP.

---

## Wprowadzenie

**Netstat** to polecenie służące do wyświetlania aktywnych połączeń sieciowych oraz informacji o używanych portach i protokołach. Daje ono wgląd w ruch TCP oraz UDP i pokazuje, które usługi są aktywne na danym komputerze.
**Wireshark** natomiast umożliwia bardziej szczegółową analizę ruchu sieciowego, pozwalając na śledzenie nagłówków protokołów TCP i UDP, a także sesji FTP oraz połączeń realizowanych za pomocą protokołu TFTP.

## Monitorowanie połączeń TCP i UDP

1. Uruchom terminal (cmd/powershell) na swoim komputerze.
2. Wpisz polecenie **netstat -a**, aby wyświetlić wszystkie aktywne połączenia sieciowe oraz porty nasłuchujące.
3. Zidentyfikuj połączenia TCP – zwróć uwagę na kolumny „Local Address" (adres lokalny) i „Foreign Address" (adres zdalny), a także stan połączeń (np. ESTABLISHED, LISTENING).
4. Zidentyfikuj połączenia UDP – zaznacz połączenia, które są oznaczone jako UDP, zidentyfikuj ich porty i adresy.
5. Wykonaj zrzut ekranu wyników dla połączeń TCP oraz UDP i zaznacz przykładowe aktywne sesje.

## Nagłówek TCP

1. Uruchom Wireshark i rozpocznij przechwytywanie ruchu sieciowego.
2. Otwórz stronę internetową lub aplikację, która używa połączeń TCP (np. przeglądarka WWW).
3. Zatrzymaj przechwytywanie po kilku sekundach.
4. Filtruj pakiety TCP: użyj filtra **tcp** w Wiresharku, aby wyświetlić tylko ruch TCP.
5. Kliknij na dowolny pakiet TCP, aby wyświetlić jego szczegóły.

6. Przeanalizuj nagłówek TCP – zwróć uwagę na numer portu, numer sekwencyjny, numer potwierdzenia oraz flagi kontrolne (SYN, ACK, FIN).
7. Zrób zrzut ekranu szczegółów nagłówka TCP i opisz kluczowe elementy (numery portów, sekwencyjne, flagi).

## Sesja FTP

1. Rozpocznij przechwytywanie w Wiresharku.
2. W terminalu/wierszu poleceń nawiąż połączenie FTP z serwerem, używając polecenia ftp (możesz użyć publicznego serwera FTP, np. **ftp.dlptest.com**).
3. Prześlij plik lub odbierz plik z serwera, aby zainicjować pełną sesję FTP.
4. Zatrzymaj przechwytywanie w Wiresharku po zakończeniu transmisji.
5. Filtruj pakiety FTP: użyj filtra ftp w Wiresharku, aby znaleźć ruch FTP.
6. Zrób zrzut ekranu z fragmentu sesji FTP, przedstawiając zarówno komendy (np. USER, PASS, RETR, STOR), jak i transfer danych.
7. Opisz przebieg sesji FTP i przeanalizuj kluczowe pakiety.

## Nagłówek UDP za pomocą TFTP

1. Opisz, jak wygląda nagłówek UDP oraz w jaki sposób różni się od nagłówka TCP.
2. Wyjaśnij, jak działa protokół TFTP (Trivial File Transfer Protocol) i jakie ma zastosowania.
3. Jakie są zalety i wady korzystania z TFTP w porównaniu do FTP?

## Zadanie dodatkowe

Przeanalizuj połączenie szyfrowane, takie jak FTPS lub SFTP. Jaka jest różnica w przesyłaniu danych w porównaniu do niezaszyfrowanego FTP?

---

**Przygotuj krótki raport z przeprowadzonych działań. Umieść w nim wykonane zrzuty ekranu oraz opisy. Pracę zapisz jako plik .pdf i prześlij na adres szkola@davidkasperek.com**