Arkadiusz Kowalczyk
Nr indeksu: 276564

Projekt z przedmiotu Programowanie Sieciowe
„Analizator ruchu TCP z wykorzystaniem biblioteki libpcap”

1. Założenia projektu

Program ma za zadanie badać ruch TCP, za pomocą biblioteki pcap, na wybranym interfejsie sieciowym. Wyświetlane powinny zostać najważniejsze pola nagłówków warstw łącza danych, sieciowej oraz transportowej. Dodatkowo, powinno zostać sporządzone podsumowanie przechwyconego ruchu, pokazujące liczbę przechwyconych pakietów, ilość wysłanych i odebranych wiadomości, użycie portów oraz przybliżona prędkość przechwytywania.

2. Budowa i działanie programu.

Program *mytcpsniffer* należy skompilować z pomocą libpcap, oraz uruchomić z prawami administratora oraz podając jak argument nazwę interfejsu sieciowego, który chcemy podsłuchiwać, np.

gcc mytcpsniffer.c -o mytcpsniffer -lpcap
sudo ./mytcpsniffer enp2s0

Program przechwytuje zdefiniowaną w zmiennej *CAP_PACKETS* liczbę pakietów, lub jego działanie może zostać przerwane sygnałem (CTRL + C z klawiatury). Zgodnie z sugerowaną, przedstawioną w czasie wykładu instrukcją korzystania z biblioteki pcap, po wyborze interfejsu, sprawdzeniu, czy on istnieje, i otworzeniu go (*pcap_open_live*) następuje zdefiniowanie filtra przechwytywania za pomocą funkcji *pcap_compile* oraz *pcap_setfilter*. Za łapanie pakietów odpowiada funkcja *pcap_next*, zawarta w pętli for o długości odpowiadającej zdefiniowanej wcześniej ilości pakietów do przechwycenia, która zwraca wskaźnik na dane pakietu. Wyświetlane są odpowiednio: długość pakietu, EtherType, adresy warstwy drugiej i trzeciej (zależnie od protokołu: IPv4 lub IPv6), wersja protokołu warstwy 3, oraz dane z nagłówka TCP: numery portów, numery sekwencyjny, potwierdzenia, flagi, szerokość okna, suma kontrolna oraz wskaźnik priorytetu. Po zakończeniu, lub przerwaniu działania programu wyświetlane jest podsumowanie zgodne z założeniami projektu.