VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta informačních technologií

Počítačová komunikácia a siete 2020

Dokumentácia

Zadanie ZETA – Sniffer paketov

Juraj Lahvička (xlahvi00)

Brno, 3.5.2020

Zadanie

Navrhnite a implementujte sieťový analyzítor v C/C++/C#, ktorý bude schopný na určitom sieťovom rozhraní zachatávať a filtrovať pakety. Vytvorte relevantný manuál/dokumentáciu k projektu.

Problematika

Zachytávanie paketov je proces zbierania dát paketov, ktoré prejdú cez dané sieťové rozhranie. Zachytávanie sieťových paketov nám ponúka možnosť monitorovať a analyzovať dáta prechádzajúce cez toto rozhranie. Knižnice libcap (pre UNIX systémy) a WinPcap (pre Windows) sú najpoužívanejšie systémové ovládače, ktoré umožňujú zachytávanie paketov. Populárne nástroje Wireshark a tcpdump používajú tieto knižnice.

Implementácia

Projekt bol implementovaný v programovacom jazyku C#. Knižnica, ktorá bola použitá je SharpPcap. Program pozostáva zo súborov:

- Program.cs
- Sniffer.cs
- PacketPrinter.cs

V súbore Program.cs sa nachádza trieda Program, ktorá má triedu Options, ktorá definuje vstupné parametre programu.
V súbore Sniffer.cs je statická trieda Sniffer, ktorá má na starosti manipuláciu a filtrovanie paketov podľa zadaných argumentov programu.
Súbor PacketPrinter.cs obsahuje statickú triedu PacketPrinter, ktorá sa stará o výpis dát paketu (informácie o pakete, hlavičky a „nálože“ paketu) podľa zadania.
Pre parsovanie zadaných argumentov bol použitý Nuget balíček/knižnica CommandLineParser.

Testovanie

Projekt bol testovaný pomocou nástroja wireshark a curl, kde cez nástroj curl bol poslaný dotaz, program wireshark zachytil paket a jeho dáta boli následne manuálne porovnané s výstupom z implementovaného programu.

Bibliografia

SharpPcap - A Packet Capture Framework for .NET [online]. In: . 5.5.2014 [cit. 2020-05-03]. Dostupné z: https://www.codeproject.com/Articles/12458/SharpPcap-A-Packet-Capture-Framework-for-NET

Tcpdump. *Tcpdump & libpcap* [online]. [cit. 2020-05-03]. Dostupné z: http://www.tcpdump.org/