Fakulta informačních technologií
Vysoké učení technické v Brně

Počítačové sítě a komunikace
2019/2020

ZETA: Sniffer paketů

Jméno a příjmení: Daniel Štěpánek
Email: xstepa61@stud.fit.vutbr.cz

Datum: 3. 5. 2020

Obsah

Úvod do problematiky

Sniffer (Analyzátor) paketů je počítačový program nebo kus počítačového hardwaru, pomocí kterého je možné zachytávat a zaznamenávat komunikaci v počítačové síti nebo v její části. V okamžiku, kdy datové proudy tečou přes síť, tak analyzátor paketů zachycuje každý paket. Ten je poté v případě potřeby dekódován na surová data paketu, která ukazují hodnoty různých polí v paketu. Dále pak je analyzován jeho obsah podle na příslušné RFC nebo jiných specifikací.

Zachycení paketů je proces zachycování a protokolování provozu v síti.[1]

Návrh aplikace

Při návrhu aplikace bylo využito několik zdrojů zabývajících se touto tématikou.[2][3]. Program je rozdělen do hlavních tří částí: Zpracování parametrů příkazové řádky, zachytávání paketů a jejich filtrování, výpis výstupu programu.

Popis implementace

Zpracování parametrů příkazové řádky probíhá pomocí funkce *getlongopt()*. V případě parametru -h/--help, je vypsána nápověda k programu a program je ukončen s kódem 0.

Pro práci s pakety je využita knihovna *libpcap*. Po nastavení filtru, dle zadaných parametrů, je spuštěno zachytávání paketů. Program je omezen pouze na práci s pakety IPv4. Každý paket je postupně rozbalován až na transportní vrstvu dle ISO/OSI modelu. Z TCP/UDP hlavičky je získán zdrojový a cílový port, poté z IP hlavičky zdrojová a cílová IP adresa, která je přeložena (pokud je o ni záznam) na doménové jméno. Pokud záznam neexistuje, nebo nelze získat, vypisuje se IP adresa zařízení. Pro hlavičky na jednotlivých vrstvách jsou využity struktury z knihoven *netinet*. Vypisován je celý paket ve tvaru odpovídajícím zadání.

Časový údaj, kdy byl paket zachycen, je získán pomocí funkce *timespec_get()*. K získané hodnotě je přidáno 7200s, aby časový údaj odpovídal našemu časovému pásmu.

Parametry

-i *eth0* (rozhraní, na kterém se bude poslouchat. Nebude-li tento parametr uveden, vypíše se seznam aktivních rozhraní)

-p *23* (bude filtrování paketů na daném rozhraní podle portu; nebude-li tento parametr uveden, uvažují se všechny porty)

-t nebo --tcp (bude zobrazovat pouze tcp pakety)

-u nebo --udp (bude zobrazovat pouze udp pakety)

Pokud nebude -tcp ani -udp specifikováno, uvažují se TCP a UDP pakety zároveň

-n *10* (určuje počet paketů, které se mají zobrazit; pokud není uvedeno, uvažujte zobrazení pouze 1 paket)

Testování

Program byl ručně testován s různými kombinacemi parametrů. Výstup programu byl porovnáván s výstupy programu *Wireshark*.

Reference

[1]: https://cs.wikipedia.org/wiki/Analyzátor_paketů

[2]: http://yuba.stanford.edu/~casado/pcap/section1.html

[3]: https://www.tcpdump.org/pcap.html