Sieťový analyzátor C++

2020

Andrej Ježík
xjezik03

Popis programu

Používanie (upresnenie výnimiek)

-i <rozhranie>

Sieťový analyzátor, zachytáva pakety z rozhrania ktoré bolo špecifikované užívateľom pomocou parametra -i, avšak ak parameter -i nebol zadaný tak analyzátor zobrazí aktívne rozhrania, konkrétne ich názov, ip adresu a broadcast.

-n <počet paketov>

Analyzátor zachytí jeden paket a potom ukončí svoju činnosť pokiaľ chce užívateľ zachytiť viac paketov tak môže použiť argument -n, pri zápornom argumente n program bude bežať v nekonečnej smyčke.

-p <port>

Bude filtrovať iba pakety ktoré budú mať rovnaký port v destinačnej alebo počiatočnej adrese.

--tcp/-t, --udp/-u, --icmp/-c

Argumenty --tcp/-t, --udp/-u, --icmp/-c fungujú na tlačenie iba paketov s určitým protokolom, ak ich užívateľ bude kombinovať tak program bude tlačiť všetky ktorých argument použil

-h

Zobrazí nápovedu a ukážky použitia argumentov a spustenia programu.

Zaujímavé časti implementácie

Pre odchytávanie paketov používam knižnicu pcap, slučku pre zachytenie viacerých paketov zabezpečujem pomocou vstavanej funkcie pcap_loop.

Po použití pcap_loop získaný paket spracováva vo funkcií my_packet_handler, program zistí pomocou switchu aký má daný paket protokol a zavolá nasledovnú funkciu. V danom swichy taktiež prebieha rozhodovanie aké pakety filtrujeme (e.g. pomocou argumentu --tcp). Každý protokol má vlastnú funkciu čo umožňuje jednoduché a prehľadné odstránenie alebo pridanie podporovaného protokolu alebo tlačenie informácii špecifických pre daný protokol.

Funkcie pre jednotlivé protokoly:

Čas získava program z hlavičky paketu pomocou štruktúry pcap_pkthdr, v ktorej sa nachádza štruktúra timeval z ktorej dostaneme čas.
Čas potom sformátujeme do stringu pomocou funkcií strftime a snprintf.

Ip adresy dostaneme s ip hlavičky a potom pomocou funkcie gethostbyaddr vyskúšame získať doménové meno, ak sa nepodarí tak vytlačíme ip adresu.

Obsah paketu program tlačí vo funkcii print_data kde ich už podľa požiadavky naformátuje.

Bonusové rozšírenia

ICMP pakety

Ako bonusové úlohy program spracováva aj ICMP pakety a teda program akceptuje nové dva argumenty -c a --icmp, ktoré budú filtrovať iba ICMP pakety

Testovanie

Môj program

Testovanie prebehlo úspešne a to pomocou porovnávania výstupom s programu Wireshark testoval som správny obsah paketu ale taktiež funkčnosť prevodu ip adresy na DN. Pre testovanie argumentu -n som používal kontrolný výpis s počtom paketov pre jednotlivé protokoly ako TCP, UDP, ICMP, IGMP, Others pre ostatné protokoly. Nenarazil som pri koncovom testovaní na iné chyby

Wireshark

Veľmi užívateľsky priateľský program, ktorý má mnoho funkcii, i keď som mnoho z nich nevyužil tak pokročilé filtrovanie paketov mi veľmi pomohlo pri testovaní môjho programu. Farebné značenie rôznych typov paketov je tiež veľkou výhodou ktorú môj program nemá. Wireshark mi umožnil si bližšie pozrieť podrobnú štruktúru paketu ktorý som chcel s výpisom všetkých pre mňa dôležitých informácii.