VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

ISA-TOP

Aplikace pro zobrazení statistik o probíhajících síťových komunikacích na daném rozhraní

AUTOR PRÁCE Jindřich Halva (xhalva05)

ZAŘAZENÍ Předmět ISA, 3. ročník

BRNO 18.11.2024

Obsah

1. Zadání

„Vytvořte nástroj isa-top, který zobrazí aktuální přenosové rychlosti pro jednotlivé komunikující IP adresy. Program po spuštění začne zachytávat provoz na síťovém rozhraní pomocí knihovny libpcap a počítat přenosovou rychlost pro jednotlivá zachycená spojení. Program funguje jako konzolová aplikace, tj. statistiky jsou zobrazeny v rámci terminálu a aktualizují se pouze statistiky/pořadí.“

2. Teorie

2.1. Síťový paket

Paket je základní jednotka datové komunikace v počítačových sítích. Každý paket obsahuje hlavičku a datovou část. Hlavička nese například data o zdrojové a cílové adrese, užitém protokolu, velikosti…

2.2. Zachytávání provozu na síťovém rozhraní

Zachytávání provozu na síťovém rozhraní je proces, při kterém jsou odposlouchávány datové pakety přenášené v rámci počítačové sítě. Proces zachytávání umožňuje monitorovat a analyzovat komunikaci mezi různými zařízením a tvořit statistiky o síťovém provozu. Informace o daných uzlech komunikace jsme schopni získat z hlaviček síťových paketů.

2.3. Přenosová rychlost

Důležitou informací při přenosu dat po síti je přenosová rychlost. Určuje množství dat, přenesených za jednotku času. Údaj o přenosové rychlosti může být užitečný pro analýzu dané sítě nebo například pro optimalizaci.

2.4. Podobné nástroje

V dnešní době existuje více nástrojů, které zahrnují podobnou funkčnost jako nástroj isa-top. Patří mezi ně následující:

- **tcpdump** – nástroj pro zachytávání síťového provozu
- **iftop** – pokročilejší nástroj velmi podobného principu jako isa-top, slouží k sledování přenosových rychlostí.
- **Wireshark** – pokročilý analyzátor síťového provozu.

3. Návrh

Aplikace je z nemalé části podobná principu síťového snifferu. Od toho se odvíjel výchozí přístup k návrhu a vývoji. Základem je schopnost zachytávat a analyzovat síťový provoz.

4. Implementace

4.1. Popis implementace

Program byl implementován v jazyce C++. Základem pro práci s pakety byla knihovna libpcap. Pro práci s výstupem na terminál bylo užito knihovny ncurses. Program má nastavený filtr na zachytávání pouze IPv4, IPv6, udp, tcp, icmp paketů.

Samotný program začíná ve funkci *main*, kde se po parsování argumentů z terminálu a ověření existence zadaného zařízení, otevře dané rozhraní a umožní se zachytávání packetů. To umožňuje funkce *pcap_open_live()*. Důležitým parametrem této funkce je parametr udávající informaci o tom, že budeme hledat v promiskuitním režimu.

Poté se nastaví filtr na zachytáváni paketů a inicializuje se terminálové okno.

Následuje vytvoření dvou vláken programu. Jedno vlákno se stará o zachytávání paketů, pro něj je důležitá funkce *pcap_loop()*, ve které se ve smyčce volá funkce *PacketHandler* ze třídy *Handler,* V této funkci se pakety zpracují a informace o nich se uloží do globálního vektoru. Druhé vlákno se zajímá o výpis dat do terminálového okna. Vlákna společně pracují s již zmíněným globálním vektorem: *vector <Unit> units*, který obsahuje veškeré informace o zachycených komunikacích během daného časového intervalu (jedna komunikace, ať už ve směru A->B nebo B->A, je v programu popsána strukturou Unit). K tomuto vektoru se přistupuje přes mutex[1].

Struktura *Unit* má tuto podobu:

```
struct Unit {
  string src_ip;
  string dst_ip;
  string protocol;
  int Rx = 0;
  int Tx = 0;
  int rx_packets = 0;
  int tx_packets = 0;
};
```

4.2. Rozšíření zadání

Zadání projektu bylo rozšířeno o nepovinný přepínač *-t*, umožňující zvolit libovolný časový interval pro obnovu statistik. Hodnota přepínače se zadává v sekundách.

5. Návod na použití

5.1. Překlad

Pro překlad projektu je třeba užití příkazu *make*. Po přeložení je program připraven ke spuštění.

5.2. Argumenty

Argumenty programu:

- „-i“ ... povinný, vyžaduje hodnotu, a to název rozhraní
- „-s“ ... nepovinný, vyžaduje hodnotu, a to buď písmeno „b“ nebo „p“, udává, zda se výstup řadí podle počtu přenesených bytů nebo packetů (pokud není uveden, řadí se podle bytů)
- „-t“ ... nepovinný, vyžaduje hodnotu, která udává interval v sekundách pro obnovu statistik (pokud není uveden, interval je roven jedné sekundě)

5.3. Příklad použití

```
./isa-top -i interface_name -s p -t 2
```

Podle ukázky by se pakety zachytávali na rozhraní „interface_name“, výstup by se řadil podle počtu přenesených paketů za sekundu a obnova statistik by proběhla každé dvě sekundy.

[1] Mutex uděluje výhradní přístup ke sdílenému prostředku pouze jednomu vláknu. Pokud vlákno získá mutex, druhé vlákno, které chce tento mutex získat, je pozastaveno, dokud první vlákno mutex neuvolní.

6. Testování

Testování bylo uskutečněno pomocí programu Wireshark a probíhalo následovně:

Doba obnovy statistik u isa-top byla nastavena na tři sekundy, aby bylo snadnější pracovat s oběma nástroji zároveň. Ve stejný moment (s drobnou odchylkou vzniklou při přepínání mezi programy) bylo spuštěno monitorování v programu Wireshark (s příslušným filtrem) i v programu isa-top. Výstup zachycený oběma programy je prezentován následujícími snímky.

6.1. Test č.1

SrcIP:Port	DstIP:Port	Proto	Rx		Tx	
			b/s	p/s	b/s	p/s
[2a00:ca8:a1f:9efb:b1b9:ce52:885:270]:55122	[2600:1901:1:4be::]:443	tcp	28.7	0.3	28.7	0.3

Obrázek 1: Výstup z isa-top

No.	Time	Source	Destination	Protocol	Length	Info
2	0.006928236	2600:1901:1:4be::	2a00:ca8:a1f:9efb:b1b9…	TCP	86	[TCP ACKed unseen segment] 443 → 55122 [ACK] Seq=1 Ack=2 Win=826 Len=0 TSval…
1	0.000000000	2a00:ca8:a1f:9efb:b1b9…	2600:1901:1:4be::	TCP	86	55122 → 443 [ACK] Seq=1 Ack=1 Win=417 Len=0 TSval=3811891584 TSecr=2220680706

Obrázek 2: Výstup z Wireshark

6.2. Test č.2

SrcIP:Port	DstIP:Port	Proto	Rx		Tx	
			b/s	p/s	b/s	p/s
192.168.100.3:38874	85.135.32.100:53	udp	37.3	0.3	132.7	0.3
192.168.100.3:50487	85.135.32.100:53	udp	37.3	0.3	132.7	0.3
192.168.100.3:33676	85.135.32.100:53	udp	37.3	0.3	132.7	0.3
192.168.100.3:34755	85.135.32.100:53	udp	37.3	0.3	109.3	0.3
192.168.100.3:34772	85.135.32.100:53	udp	37.3	0.3	109.3	0.3
192.168.100.3:35566	85.135.32.100:53	udp	37.3	0.3	109.3	0.3
[2a00:ca8:a1f:9efb:b1b9:ce52:885:270]:49404	[2600:1901:1:566::]:443	tcp	71.7	0.7	70.7	0.7
192.168.100.3:55009	85.135.32.100:53	udp	41.7	0.3	65.0	0.3
192.168.100.3:57527	85.135.32.100:53	udp	41.7	0.3	65.0	0.3
192.168.100.3:57942	85.135.32.100:53	udp	41.7	0.3	65.0	0.3

Obrázek 3: Výstup z isa-top

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.100.3	85.135.32.100	DNS	112	Standard query 0x0545 A westus-0.in.applicationinsights.azure.com OPT
2	0.000266340	192.168.100.3	85.135.32.100	DNS	112	Standard query 0x9868 AAAA westus-0.in.applicationinsights.azure.com O…
3	0.013762572	192.168.100.3	85.135.32.100	DNS	125	Standard query 0x01af AAAA gig-ai-prod-wus-0-app-v4-tag.westus.cloudap…
4	0.022730320	85.135.32.100	192.168.100.3	DNS	328	Standard query response 0x0545 A westus-0.in.applicationinsights.azure…
5	0.023055672	85.135.32.100	192.168.100.3	DNS	398	Standard query response 0x9868 AAAA westus-0.in.applicationinsights.az…
6	0.027347598	85.135.32.100	192.168.100.3	DNS	195	Standard query response 0x01af AAAA gig-ai-prod-wus-0-app-v4-tag.westu…
7	0.048599762	2a00:ca8:a1f:9efb:b1b9…	2600:1901:1:566::	TLSv1.2	129	Application Data
8	0.059490453	2600:1901:1:566::	2a00:ca8:a1f:9efb:b1b9…	TCP	86	443 → 49404 [ACK] Seq=1 Ack=44 Win=1044 Len=0 TSval=3419210254 TSecr=1…
9	0.069644111	2600:1901:1:566::	2a00:ca8:a1f:9efb:b1b9…	TLSv1.2	126	Application Data
10	0.069664294	2a00:ca8:a1f:9efb:b1b9…	2600:1901:1:566::	TCP	86	49404 → 443 [ACK] Seq=44 Ack=41 Win=489 Len=0 TSval=1038614459 TSecr=3…
11	0.569847795	192.168.100.3	85.135.32.100	DNS	112	Standard query 0xc7f9 A westus-0.in.applicationinsights.azure.com OPT
12	0.570236140	192.168.100.3	85.135.32.100	DNS	125	Standard query 0x7066 A gig-ai-prod-wus-0-app-v4-tag.westus.cloudapp.a…
13	0.570589312	192.168.100.3	85.135.32.100	DNS	112	Standard query 0x4e15 AAAA westus-0.in.applicationinsights.azure.com O…
14	0.570876359	192.168.100.3	85.135.32.100	DNS	125	Standard query 0xbf7c AAAA gig-ai-prod-wus-0-app-v4-tag.westus.cloudap…
15	0.583090105	192.168.100.3	85.135.32.100	DNS	112	Standard query 0xd0f9 A westus-0.in.applicationinsights.azure.com OPT
16	0.583391801	192.168.100.3	85.135.32.100	DNS	125	Standard query 0x717a A gig-ai-prod-wus-0-app-v4-tag.westus.cloudapp.a…
17	0.583717414	192.168.100.3	85.135.32.100	DNS	112	Standard query 0x0de8 AAAA westus-0.in.applicationinsights.azure.com O…
18	0.583984089	192.168.100.3	85.135.32.100	DNS	125	Standard query 0xf3d7 AAAA gig-ai-prod-wus-0-app-v4-tag.westus.cloudap…
19	0.638449489	85.135.32.100	192.168.100.3	DNS	328	Standard query response 0xc7f9 A westus-0.in.applicationinsights.azure…
20	0.640329668	85.135.32.100	192.168.100.3	DNS	141	Standard query response 0x7066 A gig-ai-prod-wus-0-app-v4-tag.westus.c…
21	0.643329835	85.135.32.100	192.168.100.3	DNS	195	Standard query response 0xbf7c AAAA gig-ai-prod-wus-0-app-v4-tag.westu…
22	0.643330050	85.135.32.100	192.168.100.3	DNS	398	Standard query response 0x4e15 AAAA westus-0.in.applicationinsights.az…

Obrázek 4: Výstup z Wireshark

Z obou snímků je možné vyčíst, že v daném intervalu bylo zachyceno 22 paketů s danými adresami.

Lze si povšimnout, že za tuto výměnu byly zachyceny celkem 4 TCP pakety. To u obou snímků také sedí.

Zdroje

https://www.networkacademy.io/ccna/ipv6/ipv4-vs-ipv6

https://www.ibm.com/docs/en/zos/3.1.0?topic=functions-getprotobynumber-get-protocol-entry-by-number

https://www.tcpdump.org/manpages/pcap_loop.3pcap.html

https://www.tcpdump.org/pcap.html

https://www.root.cz/clanky/psani-aplikaci-pro-terminal-jak-funguje-knihovna-ncurses/

https://pubs.opengroup.org/onlinepubs/7908799/xcurses/curses.h.html

https://www.tcpdump.org/manpages/pcap.3pcap.html

https://www.liveaction.com/resources/blog-post/what-is-a-network-packet/

https://networklessons.com/cisco/ccna-routing-switching-icnd1-100-105/ipv4-packet-header

https://www.devdungeon.com/content/using-libpcap-c

https://homes.di.unimi.it/~gfp/SiRe/2002-03/progetti/libpcap-tutorial.html

http://yuba.stanford.edu/~casado/pcap/section4.html