VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
Fakulta informačních technologií

Technická zpráva

ISA projekt - PCAP NetFlow v5 exportér

18. listopadu 2024 Michálek Kryštof (xmicha94)

Obsah

1 Úvod

Cílem mojí práce dle zadání bylo implementovat program p2nprobe, který extrahuje informace o síťových tocích ze souboru PCAP a odešle tyto informace pomocí protokolu UDP na kolektor ve formátu NetFlow v5.

Agregace paketů do toků je důležitý proces, zejména pro monitoring a analýzu síťového provozu. V tomto projektu jsem dle zadání využil protokol NetFlow verze 5, vyvinutý společností Cisco Systems, která je jednou z největších firem zabývajících se síťovými prvky. Díky NetFlow zprávám lze mít snadný real-time vhled do síťového provozu, což usnadňuje jeho zabezpečení a optimalizaci výkonu.

Pro implementaci jsem si zvolil jazyk C++.

2 Návrh aplikace

Celý proces od čtení jednotlivých paketů až po exportování NetFlow v5 zprávy na kolektor byl potřeba rozdělit na několik klíčových podčástí:

1. **Čtení paketů ze vstupního PCAP souboru**: Prvním krokem je načítání síťových paketů ze zadaného PCAP souboru. Tento krok využívá knihovnu libpcap pro efektivní zpracování souborů a získání paketových dat.

2. **Extrahování dat z jednotlivých paketů**: Jakmile jsou pakety načteny, je potřeba extrahovat relevantní informace z každého paketu, jako jsou IP adresy, porty, protokol, časové značky a velikost paketu.

3. **Přiřazení paketu do toku podle získaných informací**: Na základě extrahovaných informací je každý paket přiřazen k odpovídajícímu toku. Tok je definován 5-ticí (zdrojová IP, cílová IP, zdrojový port, cílový port, protokol).

4. **Kontrola timeoutů jednotlivých toků a jejich ukončení**: Během zpracování toku je důležité sledovat časové limity (timeouty) pro aktivní a neaktivní toky. Pokud dojde k překročení těchto limitů, tok je ukončen a připraven k exportu.

5. **Vytvoření NetFlow v5 zpráv a přidání záznamů**: Po ukončení toku je potřeba vytvořit záznam ve formátu NetFlow v5. Tento záznam obsahuje všechny relevantní informace o toku, které jsou nezbytné pro další analýzu na kolektoru.

6. **Příprava a následné odeslání NetFlow v5 zpráv**: Posledním krokem je příprava NetFlow zpráv a jejich odeslání na kolektor pomocí protokolu UDP.

3 Popis implementace

Tento projekt jsem implementoval v jazyce C++. Tento jazyk jsem zvolil z důvodu možnosti využití objektově orientovaného programování, jelikož pracuji s různými objekty - pakety, toky, zprávy, záznamy. Celý program je tedy rozdělen do několika souborů podle tříd.

3.1 main.cpp

- Základní nastavení, zpracování a ověření argumentů.
- Otevření a čtení vstupního PCAP souboru.
- Iterování přes všechny pakety.
- Pomocí dalších implementovaných tříd a jejich metod dále:

- Kontrola shody paketu s toky
- Kontrola expirace toku
- Převod toků na záznamy
- Připravení a odeslání zprávy

3.2 packet.cpp + packet.h

- Implementuje třídu pro ukládání dat o jednotlivých paketech přečtených ze vstupního PCAP souboru.
- Tyto informace lze pak číst pomocí get metod.

3.3 flow.cpp + flow.h

- Implementuje třídu pro ukládání jednotlivých toků. Je zde uloženo dynamické pole třídy Packet, první a poslední časová značka, počet paketů a součet velikosti všech paketů.
- Obsahuje get metody pro první a poslední časovou značku a velikost toku v bajtech.
- Dále metody pro přidání paketu do toku, kontrolu expirace toku, kontrolu shody paketu s tokem a převod toku na NetFlow v5 záznam.

3.4 netflowV5.cpp + netflowV5.h

- Implementuje třídu pro ukládání hlavičky NetFlow v5 a dynamické pole s NetFlow v5 záznamy.
- Dále metody pro přidání záznamu do zprávy, připravení dat hlavičky pro odeslání a samotné odeslání zprávy.

4 Návod na použití

Po stažení rozbalte soubor příkazem: `tar -xf xmicha94.tar`. Program přeložte příkazem `make`, poté lze program spustit následovně:

```
./p2nprobe <host>:<port> <pcap_file_path> [-a <active_timeout> -i <inactive_time
```

Pro výpis nápovědy použijte příkaz `./p2nprobe -h`.

5 Popis testování aplikace

Testování jsem prováděl kontrolou s programem `softflowd` a `wireshark`. K odchytávání TCP paketů jsem použil `tcpdump`. Odchytávání jsem provedl následujícím příkazem:

```
sudo tcpdump -i <port> -w <dest_pcap_file>
```

Pomocí kolektoru `nfcapd` jsem přijímal UDP komunikaci posílanou exportéry příkazem:

```
sudo nfcapd -w <dest_file> -p <port>
```

Následně jsem pomocí programu `softflowd` agregoval tento soubor s pakety do toků pomocí příkazu:

```
sudo softflowd -r ~/Desktop/ISA_tests/tcp.pcap -n 127.0.0.1:2055 -v 5
```

Poté jsem mým programem provedl to samé:

```
./p2nprobe <host>:<port> <pcap_file_path>
```

Poté jsem si vypsal data o tocích zachycené kolektorem pro můj program i `softflowd`:

```
nfdump -r <nfcapd_file>
```

5.1 Výsledky testů

Výsledky testů nejsou totožné se `softflowd`, jelikož program `softflowd` neexpiruje toky pouze podle časových značek, ale také podle příznaků jednotlivých paketů (FIN nebo RST), které jsem ve svém projektu neimplementoval. Porovnání mého výstupu a výstupu `softflowd`:

6 Zdroje

- `https://cs.wikipedia.org/wiki/NetFlow`
- `https://www.cisco.com/c/en/us/td/docs/net_mgmt/netflow_collection_engine/3-6/user/guideformat.html`

7 Závěr

Bohužel nemám mentální kapacitu tento projekt bez ublížení si na zdraví dokončit. Počet toků je víceméně stejný, jako mají moji kolegové, kteří se o výstup svého programu podělili. bohužel jsem nebyl schopen správně nastavit časové značky, stejně tak mi u větších souborů nesedí počet paketů a bajtů.