Vysoké učení technické v Brně
Fakulta informačních technologií

Síťové aplikace a správa sítí
Projektová domunetace

Monitorování DHCP komunikace

15. listopadu 2023 Michal Novák (xnovak3g)

Obsah

1 Problematika monitorování DHCP **2**
1.1 Ethernetový rámec [3] . . . 2
1.2 IPv4 datagramy [2] . . . 2
1.3 UDP pakety [1] . . . 2
1.4 DHCP zprávy [4] . . . 2

2 Popis implementace **2**
2.1 Třída Options . . . 2
2.2 Třída EventLogger . . . 2
2.3 Třída Stats . . . 3
2.4 Třída PcapHandler . . . 3

3 Informace o programu **3**

4 Návod k použití **3**
4.1 Odposlouchávání probíhající komunikace . . . 4
4.2 Čtení z PCAP souborů . . . 4

1 Problematika monitorování DHCP

Monitorování DHCP je možno provádět odposlouchánváím síťového provozu, při kterém se zkoumají jednotlivé pakety zachycené síťovým rozhraním.

DHCP zprávy pro verzi IPv4 jsou při síťovém přenosu zapouzdřeny. Jednotlivé ethernetové rámce obalují IPv4 datagramy, které obsahují UDP pakety nesoucí DHCP zprávy. Pro získání dat z DHCP zprávy je tedy nutné nejříve získat samoutnou DHCP zprávu z tohoto „pouzdra“.

1.1 Ethernetový rámec [3]

Ethernetová hlavička má pevnou velikost 14 B pro přenos, který neprobíhá bezdrátově. V paketu je tedy možné se posunout o pevnou velikost a tím se zpřístupní data, která nese ethernetový rámec.

1.2 IPv4 datagramy [2]

IPv4 hlačicka nemá pevnou délku a je nutné ji tedy zjistit přímo z hlavičky samotné. Údaj o velikosti hlavičky se nachází na 4-8 bitu od začátku hlavičky. Tento údaj je poté nutné vynásobit číslem 4 a výsledkem této operace je skutečná velikost. Posunem o tuto hodnotu od začátku IP hlavičky v paketu se zpřístupní data uložená v IPv4 datagramu.

1.3 UDP pakety [1]

Velikost UDP hlavičky je pevné velikosti 8 B a je tedy opět možný posun za hlavičku pro zpřístupnění dat.

1.4 DHCP zprávy [4]

Pro monitorování DHCP komunikace přidělování klientských adres je nutné extrahovat ze zprávy její typ a přidělenou adresu. Adresa přidělená klientovi (položka `yiaddr`) o velikosti 4 B je odsazená o 16 B od počátku DHCP zprávy. Typ zprávy („Message Type“) je údaj, který je zapouzdřen v sekci možnosti („Options“) DHCP. Pro účely tohoto projektu je zkoumají jen DHCP balíčky typu ACK. Možnosti jsou odsazeny o 240 B také od začátku DHCP zprávy. Jednotlivé možnosti se poté drží normy, a je tedy jednoduché jimi procházet a hleda možnost označenou hodnotou 53, která značí možnost typu zprávy. V těle této možnosti je následovně možno ověřit, zda-li je zpráva typu ACK.

2 Popis implementace

Aplikace je implementována v jazyce C++. Návrh uplatňuje objektový přístup.

2.1 Třída Options

Třída pro zpracování argumentů příkazové řádky. Při nalezení chyby je vyhozena výjimka a program je ukončen. Zpracované argumenty se ukládají pro použití v dalších částech programu.

2.2 Třída EventLogger

EventLogger slouží k výpisu informací týkajících se změn ve statistikách. Průběžný výpis statistik je realizován pomocí knihovny `ncurses`. Při překročení 50 % vytížení podsítě je na konec standardního výstupu a do syslogu vypsáno upozornění o této události.

2.3 Třída Stats

Pro každý zadaný prefix získaný pomocí třídy Options se vytvoří struktura StatsItem_t, která v obsahuje: adresu sítě, broadcast adresu, masku sítě, délku prefixu a množinu, v níž budou uloženy zaznamenané IP adresy patřící do dané podsítě.

Při získávání IP adres z DHCP zpráv se zkoumá, zda patří do dané podsítě. Pokud IP patří do podsítě, uloží se do množiny a aktualizuje se statistika na výstupu.

2.4 Třída PcapHandler

Nejdůležitější část programu, která se stará o zpracování síťového provozu. Podle vstupních argumentů se provádí sběr paketů z definovaného zdoje. Pakety jsou fltrovány filtrem `"( ip and udp and ( src port 67 ) )"`, který by měl zaručit přítomnost pouze paketů protokolu DHCP přicházejících od DHCP serveru. Každý přijatý paket je poté zpracován. Jen pakety typu DHCP ACK se začlení do statistik.

Inspirací k Implementace této třídy byly ve velké míře ukázkové kódy ke 3. přednášce předmětu ISA.

3 Informace o programu

Aplikace bude zkoumat jednotlivé DHCP ACK balíčky a shromažďovat přidělené IP adresy. Z přidělených adres se bude průběžně tvořit statistika, která bude vypisována na výstup konzole.

Program je možné spustit na libovolném zařízení s operačním systémem linux. Podmínkou správného chodu aplikace je přítomnost dynamických knihoven `libpcap`[1] a `ncurses`[2], které jsou využívány v implementaci.

4 Návod k použití

Program lze spustit na libovolném zařízení, které splňuje výše zmíněné požadavky. Přeložení zdrojových souborů na na spustitelný program je možno provést příkazem `make`. Po přeložení se program spouští příkazem:

```
./dhcp-stats [-r] [-r <filename>] [-i <interface-name>] <ip-prefix> [ <ip-prefix> [ ... ] ]
```

, kde

- `-h` vypíše pomocné informace a ukončí program,
- `-r` je název PCAP souboru,
- `-i` je název internetového rozhraní,
- `<ip-prefix>` je prefix podsítě.

[1] Odkaz na oficiální stránky libpcap: https://www.tcpdump.org
[2] Odkaz na oficiální stránky ncurses: https://invisible-island.net/ncurses

Program umožňuje vypracování statistik 2 způsoby:

4.1 Odposlouchávání probíhající komunikace

Statistiky jsou postupně zpracovávány ze síťové komunikace, která je zachytávána na síťovém rozhraní. Běh programu musí být přerušen uživatelem.

4.2 Čtení z PCAP souborů

Pro vypracování statistiky se použije zachycená komunikace uložená v PCAP souboru. Po zpracování celého PCAP souboru se běh programu přeruší.

Odkazy

[1] User Datagram Protocol. RFC 768, Srpen 1980, doi:10.17487/RFC0768. Dostupné z: https://www.rfc-editor.org/info/rfc768

[2] Internet Protocol. RFC 791, Září 1981, doi:10.17487/RFC0791. Dostupné z: https://www.rfc-editor.org/info/rfc791

[3] Standard for the transmission of IP datagrams over IEEE 802 networks. RFC 1042, Únor 1988, doi:10.17487/RFC1042. Dostupné z: https://www.rfc-editor.org/info/rfc1042

[4] Droms, R.: Dynamic Host Configuration Protocol. RFC 2131, Březen 1997, doi:10.17487/RFC2131. Dostupné z: https://www.rfc-editor.org/info/rfc2131