Monitorování DHCP komunikace

ISA - Síťové aplikace a správa sítí 2023/2024

19.11.2023

Jozef Bilko (xbilko03)

Vedoucí: Ing. Matěj Grégr, Ph.D.

Obsah

Základní informace o programu

Program po spuštění začne monitorovat DHCP provoz na zvoleném rozhraní nebo projde pcap soubor, uživatelovi na výstup statistiku zvoleném rozsahu sítě.

- Prefixů může být více a mohou se překrývat
- Maximální počet prefixů co program dokáže od uživatele zpracovat je 512
- Nevhodný vstup vrací chybu
- Je možné jenom číst nebo jenom monitorovat provoz na právě jednom zvoleném rozhraní (je možné taky využít rozhrání any)
- Když nějaký z prefixů překročí 50% aktuálně alokovaných adres, informace se zašle do logu
- Podpora výhradně masek podsítí 1 až 30

Návod na použití

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

- -r <filename> - statistika bude vytvořena z pcap souborů
- -i <interface> - rozhraní, na kterém může program naslouchat
- <ip-prefix> - rozsah sítě pro které se bude generovat statistika

Příklad:

./dhcp-stats -i any 192.168.1.0/24 192.168.0.0/22 171.16.32.0/24
IP-Prefix Max-hosts Allocated addresses Utilization
192.168.1.0/24 254 24 9.45%
192.168.0.0/22 1022 50 4.89%
171.16.32.0/24 254 0

Uvedení do problematiky

Při DHCP komunikaci v případě alokování adres nás zajímá především DHCP ACK, je to reakce na DHCP request, kdy DHCP server přijímá požadavek klienta a potvrdí jeho alokaci na IP adresu pak uvedenou v DHCP části paketu.

Počet těchto adres má DHCP server omezen, v tomto spočívá počítání počet alokovaných adres, maximálné množstív a využití.

Je standardní, že komunikace DHCP probíhá výhradně na portech 67-68, toto pak pomůže filtrovat komunikaci mimo a rychleji reagovat na ty správne pakety.

Když port sedí, můžeme se podívat, je-li konstanta tzv. Magic cookie uvedena v paketu, to nám potvrzuje, že to skutečně je DHCP paket.

Uvedení do návrhu aplikace

Aplikace spočátku vezme vstup uživatele, roztřídit žádané IP prefixy, rozhodnout jestli číst soubor nebo monitorovat rozhrání.

při analýze paketu zahazuje nepotřebné pakety, v případě, že zachycený paket má udp port 67, obsahuje magic cookie, adresu a je to typ DHCP ACK, podívá se program, jestli táto adresa není již v binárním vyhledávacím stromu, když ne, zapíše ji tam. Jinak paket považuje za duplicitní. (Je tady vhodné neukládat adresy jenom do seznamu, po dlhší analýze může být těchto adres mnoho)

Po zapsaní adresy do stromu sa aktualizují hodnoty statistik v strukturě podle toho, jestli patří adresa pod danou podsíť.

Když se jedná o monitorování rozhrání, pak hodnoty rovnou pošli do konzole pro uživatele, jinak se počká až se soubor přečte celý, až pak se statistika vypíše.

V případě nesprávneho vstupu, či jiných chyb (např. nemožnost otevřít soubor) ukonči program s návratovou hodnotou EXIT_FAILURE (teda 1).

Popis implementace

Program je implementovaný od počátku až po konec tak zhruba nasledovně:

Kontrola a počítání statistik pomocí funkce getopt(3), program dovoluje vykonávat jednom jednu akci, proto příkladem -i any -i eth0 vyvolá chybu

Kontrola a počítání statistik
struct ip_range rangeList[maxPrefixes]
Jde jenom o jednoduché pole jehož každá položka je jiná podsíť definovaná na vstupu programu. Maximální počet podsítí maxPrefixes je 512, je možné změnit v deklaraci makra.

void AnalyzeFileAndPrint a void AnalyzeInterfaceAndPrint
V obou případech se načte paket pomocí pcap knihovny, pak se identifikuje, jestli je to validní DHCP ACK paket.

Validace paketu se hlídá pomocí pohybu v ukazovateli od začátku paketu: např. zde je x počet bytů, které musí přeskočit v paketu ukazovatel, aby se dostal dál (konkrétně na UDP hlavičku)

x = (*(uint8_t*)(packet + ETHERNET_HDR_SIZE) & 0x0F) * 4;

V IPV4 hlavičce je definovaná jeho délka pomocí 4 dolních bytů, proto po skoku je potřeba po typecastu ještě aplikovat masku. Pak získame hodnotu kterou je potřeba násobit ještě krát 4, pak se do x uloží hodnota pro skok.

Nález unikátní adresy (když není uložena v BT), pak do stromu vložíme tuto adresu aby si to program pamatoval a nepočítal stejnú adresu do statistiky vícekrát.

```
if (TreeContains(root, yiaddr) == false)
    root = TreeInsert(root, yiaddr);
```

Bitový posun pro adresy v binárním tvaru za účelem zjistění, jestli daná adresa patří pod danou podsíť:

```
/* ip-prefix */ newAddr = newAddr >> subnet; /* int subnet = 32 – suffix*/
/* yiaddr */ newIp = newIp >> subnet;
```

Počas analýzy interfacu pravidelně po aktualizaci statistik jí posíláme pomocí knihovni ncurses na obrazovku pro uživatele.

```
PrintToWindow(struct ip_range rangeList[maxPrefixes], u_int32_t prefixCount)
{ …
printw(…); /* vypsat statistiku */
refresh();
clear();
… }
```

V případě, že jedna z podsítí přesáhne 50% utilizace, je záznam zaslán do logu (nejvíc 1x pro každou podsíť)

```
syslog(LOG_NOTICE, "prefix %s/%s exceeded 50%% of allocations", …);
```

Literatura

[1] DHCP protocol RFC 2131. https://datatracker.ietf.org/doc/html/rfc2131
[2] Lars Wirzenius, Manpages. http://liw.fi/manpages/
[3] Pradeep Padala, NCURSES Programming HOWTO. https://tldp.org/HOWTO/NCURSES-Programming-HOWTO/
[4] Tim Carstens, Guy Harris, PROGRAMMING WITH PCAP. https://www.tcpdump.org/pcap.html