# Nástroje monitorující a generující zprávy jednoduchých distance-vector protokolů

Síťové aplikace a správa sítí

2018/2019

Autor: Miroslav Válka (xvalka05)

# Obsah

| Obsan                                     | 2 |
|---|---|
| Základní informace                        | 3 |
| Struktura RIPv1                           | 3 |
| Struktura RIPv2                           | 3 |
| Struktura RIPng                           | 4 |
| Popis implementace                        | 5 |
| Sniffer RIPv1, RIPv2 a RIPng zpráv        | 5 |
| Podvrhávač falešných RIPng Response zpráv | 5 |
| Použití programů                          | 6 |
| myripsniffer                              | 6 |
| Omezení                                   | 6 |
| Formát volání                             | 6 |
| myripresponse                             | 6 |
| Omezení                                   | 6 |
| Formát volání                             | 6 |
| Testování                                 | 7 |
| myripsniffer                              | 7 |
| myripresponse                             | 8 |
| Literatura                                | 9 |

## Základní informace

Protokoly RIPv1, RIPv2 a RIPng jsou směrovací protokoly distance-vector. Protokoly využívají UDP komunikaci z toho RIPv1 a RIPv2 komunikují skrze port 520 a RIPng využívá port 521. Pro práci s pakety těchto protokolů je nutné znát jejich strukturu interpretující obsažená data paketu.

#### Struktura RIPv1

- Celá struktura RIPv1 paketu.
- Paket je složen z hlavičky a jednoho záznamu o routě.

## Struktura RIPv2

 Paket RIPv2 se skládá z hlavičky, která je shodná jako pro RIPv1 a z 1 až 25 záznamů o routách.

Struktura záznamu o routě.

Jako první záznam může být následující struktura s informacemi o autentizaci.

#### Struktura RIPng

 Paket RIPng se skládá z hlavičky, která je shodná jako u předchozích RIP protokolů a ze záznamů o routách.

Struktura záznamu o routě.

 Next hop je samostatný záznam, který určuje next hop pro všechny následující záznamy o routách.

# Popis implementace

#### Sniffer RIPv1, RIPv2 a RIPng zpráv

Využívá se knihovna "libpcap", která poskytuje možnost odchytávat pakety v promiskuitním režimu síťové karty nebo načítání paketů přímo ze souboru. Pro odchytávání paketů je nastaven filtr, aby docházelo k odchytávání jen UDP komunikace na portech 520 a 521. Ostatní pakety nás nezajímají.

U zachycených paketů dochází k postupnému zpracování Ethernet hlaviček, IP hlaviček, UDP hlaviček a taktéž hlaviček rodiny protokolů RIP. Následně je zpracováno tělo paketu obsahující jednotlivé RIP záznamy. Pro zpracování každého typu hlavičky je vyčleněna jedna funkce. U každé z těchto funkcí lze ovlivnit zda bude tisknout na standardní výstup informace o dané hlavičce.

## Podvrhávač falešných RIPng Response zpráv

RIPng je protokol pracující nad UDP a IPv6. Je tedy možné otevřít klasický socket pro vytvoření a odeslání podvrhávaného paketu a není potřeba speciální knihovna jako "libpcap". Zde byla tato knihovna použita pouze k otestování dostupnosti zvoleného rozhraní.

U podvrhávaného paketu je nutné nastavit údaje jako port pro odeslání (521), hodnotu hop limit (255), přiřadit socket k zadanému rozhraní síťové karty. Paket je odeslán do multicastové skupiny s adresou "ff02::9" na port 521.

Podvrhávaný paket obsahuje jednu routu a pokud byl zadán next hop, tak je do paketu vložen také záznam o next hopu.

# Použití programů

## myripsniffer

#### Omezení

- Aplikaci je nutné spouštět jako root uživatel.
- Aplikace si neporadí s IPv6 rozšiřujícími hlavičkami (IPv6 Extension Headers).
- Aplikace nevypisuje informace o autentizaci pro RIPv2 pakety s MD5 autentizaci (Keyed Message Digest).

#### Formát volání

```
./myripsniffer -i <rozhrani> {-E} {-I} {-U}
./myripsniffer -f <soubor.pcap> {-E} {-I} {-U}
./myripsniffer -h
```

- -i <rozhraní>
  - o Rozhrani sitove karty na kterem se bude naslouchat.
  - o Nelze kombinovat s -f.
- -f <soubor.pcap>
  - o Nazev soboru obsahujici zachycenou sitovou komunikaci.
  - Nelze kombinovat s -i.
- -E
- o Budou se vypisovat i nektere informace z eternetove hlavicky.
- -|
- Budou se vypisovat i nektere informace z ip hlavicky.
- -U
- o Budou se vypisovat i nektere informace z udp hlavicky.
- -h
- Vypíše nápovědu.

#### myripresponse

#### Omezení

Aplikaci je nutné spouštět jako root uživatel.

#### Formát volání

./myripresponse -i <rozhrani> -r <IPv6>/[16-128] {-n <IPv6>} {-m [0-16]} {-t [0-65535]} ./myripresponse -h

- -i <rozhrani>
  - o Rozhrani sitove karty, ze ktereho je odesilan paket.
- -r <IPv6>/[16-128]
  - Nastaveni podvrhavane routy.

- o Format hodnoty je IPv6 adresa site lomeno prefix site.
- o př. fd00:9f0:1415::/64
- -n <IPv6>
  - o Zadání adresy pro next-hop.
- -m [0-16]
  - o Zadání metriky.
- -h
- Vypsání nápovědy.

## Testování

Na virtuálním serveru pro generování RIP komunikace byl zapnut generátor komunikace pro můj login xvalka05.

Z důvodu méně výkonného počítače byl virtuální server spuštěn na počítači č.1 a byla mu přidělena síťová karta přes kterou byl server propojen s počítačem č.2 na kterém byly programy vyvíjeny. (Zmiňuji zde převážně, jako odůvodnění, proč mi sniffer nefungoval správně při testování v laboratoři. Domácí síť jsem upravil a opravil chyby vzniklé špatným nastavením.)

#### myripsniffer

Snímky výpisu zachycených paketu RIPv2

```
>====> START PACKET <====<
                                                     === RIPv2 Response ====
>===> START PACKET <====<
                                                      [Authentication (Type - Plain-text password)]
=== RIPv2 Response ====
                                                          Password: ISA>28b13e584d1
 [Authentication (Type - Plain-text password)]
                                                      [Route (Family/Tag - 2/0)]
      Password: ISA>28b13e584d1
                                                         IP Addres: 10.0.0.0
 [Route (Family/Tag - 2/0)]
                                                        Subnet Mask: 255.255.255.0
      IP Addres: 10.48.53.0
                                                          Next Hop: 0.0.0.0
    Subnet Mask: 255.255.255.0
                                                            Metric: 1
                                                      [Route (Family/Tag - 2/0)]
       Next Hop: 0.0.0.0
                                                         IP Addres: 10.48.53.0
         Metric: 1
                                                        Subnet Mask: 255.255.255.0
 [Route (Family/Tag - 2/0)]
                                                          Next Hop: 0.0.0.0
      IP Addres: 10.97.107.0
                                                            Metric: 1
    Subnet Mask: 255.255.255.0
                                                      [Route (Family/Tag - 2/0)]
       Next Hop: 0.0.0.0
                                                         IP Addres: 10.97.107.0
         Metric: 1
                                                        Subnet Mask: 255.255.255.0
                                                          Next Hop: 0.0.0.0
 [Route (Family/Tag - 2/0)]
                                                            Metric: 1
      IP Addres: 10.108.226.0
                                                      [Route (Family/Tag - 2/0)]
    Subnet Mask: 255.255.255.0
                                                         IP Addres: 10.108.226.0
       Next Hop: 0.0.0.0
                                                        Subnet Mask: 255.255.255.0
         Metric: 1
                                                          Next Hop: 0.0.0.0
 [Route (Family/Tag - 2/0)]
                                                            Metric: 1
                                                      [Route (Family/Tag - 2/0)]
      IP Addres: 10.204.97.0
                                                         IP Addres: 10.204.97.0
    Subnet Mask: 255.255.255.0
                                                        Subnet Mask: 255.255.255.0
       Next Hop: 0.0.0.0
                                                          Next Hop: 0.0.0.0
         Metric: 1
                                                            Metric: 1
====> END PACKET <====<
                                                     >====> END PACKET <====<
```

- Zachycené heslo je "ISA>28b13e584d1" a zachycené routy RIPv2 paketů:
  - 0 10.48.53.0/24
  - o 10.97.107.0/24
  - o 10.108.226.0/24
  - 0 10.204.97.0/24
  - 0 10.0.0.0/24

Snímek výpisu zachyceného paketu RIPng

```
>====> START PACKET <====<
==== RIPng Response ====
  [Route (Tag - 0)]
    IP Address: fd00::/64
        Metric: 1
  [Route (Tag - 0)]
    IP Address: fd00:cd:2d78::/64
        Metric: 1
  [Route (Tag - 0)]
    IP Address: fd00:d8:76::/64
        Metric: 1
  [Route (Tag - 0)]
    IP Address: fd00:fc:3152::/64
        Metric: 1
  [Route (Tag - 0)]
IP Address: fd00:9f0:1415::/64
        Metric: 1
>====> END PACKET <====<
```

Zachycené routy RIPng paketu:

o fd00::/64

fd00:cd:2d78::/64
 fd00:d8:76::/64
 fd00:fc:3152::/64
 fd00:9f0:1415::/64

#### myripresponse

Snímek výpisu o routách před útokem.

- Snímek Výpisu o routách po 1. útoku.
  - ./myripresponse -r 2001:db8:0:abcd::/64

- Snímek výpisu o routách po 2. útoku.
  - ./myripresponse -r 2001:a:b:c::/64 -n fe80::4444:3333:2222:1111

```
Routing> show ipv6 route
Codes: K - kernel route, C - connected, S - static, R - RIPng, O - OSPFv3,
         I - ISIS, B - BGP, \star - FIB route.
K>* ::/0 via fe80::a00:27ff:fe22:8a6e, em0
K>* ::/96 via ::1, lo0, rej
C>* ::1/128 is directly connected, lo0
K>* ::ffff:0.0.0.0/96 via ::1, lo0, rej
R>* 2001:a:b:c::/64 [120/2] via fe80::4444:3333:2222:1111, em0, 00:00:04
R>* 2001:db8:0:abcd::/64 [120/2] via fe80::2bce:ebea:6b0f:e89a, em0, 00:00:21
C>* Za00:1028:9199:2d0a::/64 is directly connected, em0
C>* fd00::/64 is directly connected, em0
C>* fd00:cd:2d78::/64 is directly connected, lo0
C>* fd00:d8:76::/64 is directly connected, lo0
C>* fd00:fc:3152::/64 is directly connected, lo0
C>* fd00:9f0:1415::/64 is directly connected, lo0
K>* fe80::/10 via ::1, lo0, rej
C * fe80::/64 is directly connected, lo0
C>* fe80::/64 is directly connected, em0
K>* ff02::/16 via ::1, lo0, rej
Routing>
```

#### Literatura

- [1] [RFC1058] Hedrick, C., "Routing Information Protocol", RFC 1058, June 1988. https://tools.ietf.org/html/rfc1058
- [2] [RFC2453] Malkin, G., "RIP Version 2", STD 56, RFC 2453, November 1998. https://tools.ietf.org/html/rfc2453
- [3] [RFC2080] Malkin, G. and R. Minnear, "RIPng for IPv6", RFC 2080, January 1997. https://tools.ietf.org/html/rfc2080
- [4] [RFC2082] Fred Baker and Randall Atkinson and Gary Scott Malkin, "RIP-2 MD5 Authentication", RFC 2082, January 1997, https://tools.ietf.org/html/rfc2082