



Dokumentace k projektu pro předmět ISA

# **Nástroj monitorování RIP a RIPng**

22. listopadu 2015

Autor: Dávid Molnár, [xmolna02@stud.fit.vutbr.cz](mailto:xmolna02@stud.fit.vutbr.cz)

VUT FIT Brno

# Obsah

1	Úvod .....	1
2	Použití.....	1
2.1	myripsniffer .....	1
2.2	myripresponse .....	2
3	Výsledky.....	2

# 1 Úvod

Protokol RIP umožňuje výměnu rootovacích informací mezi směrovači. Směrovače pravidelně posílají informace o připojených sítích.

Nástroj myripsniffer slouží k zachycení těchto zpráv a druhý nástroj, myripresponse pak ke posílání falešných RIPv2 Response zpráv.

Protokol má verzi RIPv1 a RIPv2 pro IPv4 adresy a pro IPv6 existuje protokol RIPv6.

## 2 Použití

### 2.1 myripsniffer

Argumenty příkazového řádku:

`./myripsniffer -i interface:` povinný název rozhraní

Příklad:

```
sudo ./myripsniffer -i eth0
```

Výstup:

```
=====> RIPv2 Response (104 bytes) <=====
[MAC] 00-0C-29-76-BD-BE -> 01-00-5E-00-00-09
[IP:Port] 10.0.0.1:520 -> 224.0.0.9:520
[Authentication] Password: ISA>29012c28622
[Route (2/0)] 10.48.50.0/24 -> 0.0.0.0 [1]
```

Formát hlavičky: RIPv<verze> <command> (velikost RIP paketu)

Formát routy: [Route (<address family>/<route tag>)] <network ip>/<netmask> -> <next\_hop> [<metric>]

```
=====> RIPv6 Response (104 bytes) <=====
[MAC] 00-0C-29-76-BD-BE -> 33-33-00-00-00-09
[IPv6:Port] fe80::20c:29ff:fe76:bdb:521 -> ff02::9:521
[Route (0)] fd00::/64 [1]
[Route (0)] fd00:cd:2d78::/64 [1]
[Route (0)] fd00:10d:2ed6::/64 [1]
[Route (0)] fd00:4a4:6d::/64 [1]
[Route (0)] fd00:960:15ae::/64 [1]
```

Formát: [Route (<route tag>) <network ipv6>/<prefix> [<metric>]

## 2.2 myripresponse

Argumenty:

- i <interface\_name>: nepovinný název rozhraní, např. eth0
- r <IPv4>/[8-30]: povinná adresa sítě a prefix
- n <IPv4>: nepovinná adresa next hop
- m [0-16]: nepovinný atribut metric
- t [0-65535]: nepovinný atribut route tag
- p <password>: nepovinné autentizační heslo

Příklad:

```
sudo ./myripresponse -i 10.10.10.0/24 -p "ISA>123546789"
```

Výstup

```
creating socket... OK
binding socket... OK
setting socket parameters... OK
creating RIPv2 Response packet... OK
sending packet... OK
packet sent
```

## 3 Výsledky

Zachycené zprávy:

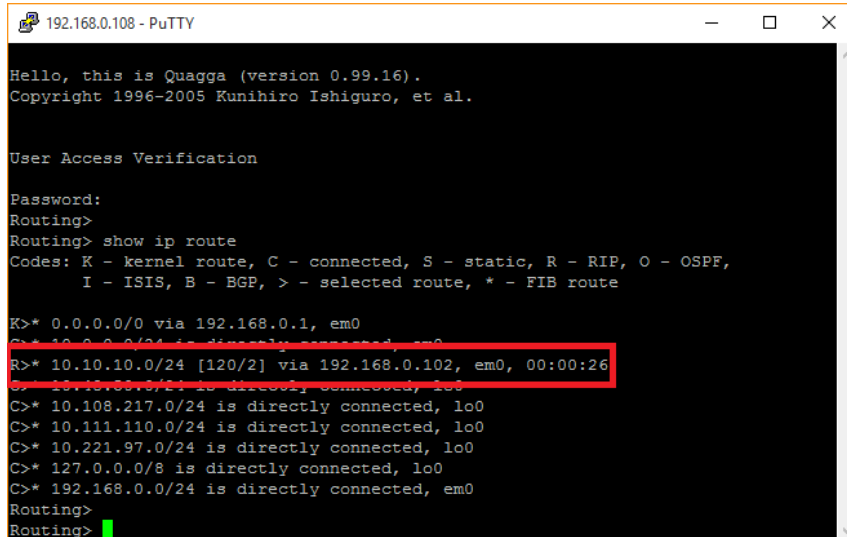
```
=====> RIPv2 Response (124 bytes) <=====
[MAC] 00-0C-29-76-BD-BE -> 01-00-5E-00-00-09
[IP:Port] 192.168.0.108:520 -> 224.0.0.9:520
[Authentication] Password: ISA>29012c28622
[Route (2/0)] 10.0.0.0/24 -> 0.0.0.0 [1]
[Route (2/0)] 10.48.50.0/24 -> 0.0.0.0 [1]
[Route (2/0)] 10.108.217.0/24 -> 0.0.0.0 [1]
[Route (2/0)] 10.111.110.0/24 -> 0.0.0.0 [1]
[Route (2/0)] 10.221.97.0/24 -> 0.0.0.0 [1]

=====> RIPv2 Response (104 bytes) <=====
[MAC] 00-0C-29-76-BD-BE -> 33-33-00-00-00-09
[IPv6:Port] fe80::20c:29ff:fe76:bdb:521 -> ff02::9:521
[Route (0)] fd00::/64 [1]
```

```
[Route (0)] fd00:cd:2d78::/64 [1]
[Route (0)] fd00:10d:2ed6::/64 [1]
[Route (0)] fd00:4a4:6d::/64 [1]
[Route (0)] fd00:960:15ae::/64 [1]
```

RIPv2 attack:

```
sudo ./myripresponse -r 10.10.10.0/24 -p "ISA>29012c28622"
```



```
192.168.0.108 - PuTTY
Hello, this is Quagga (version 0.99.16).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

User Access Verification

Password:
Routing>
Routing> show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - ISIS, B - BGP, > - selected route, * - FIB route

K>* 0.0.0.0/0 via 192.168.0.1, em0
C>* 10.0.0.0/24 is directly connected, em0
R>* 10.10.10.0/24 [120/2] via 192.168.0.102, em0, 00:00:26
C>* 10.108.217.0/24 is directly connected, lo0
C>* 10.111.110.0/24 is directly connected, lo0
C>* 10.221.97.0/24 is directly connected, lo0
C>* 127.0.0.0/8 is directly connected, lo0
C>* 192.168.0.0/24 is directly connected, em0
Routing>
Routing>
```

## Literatura

- [1] CARSTENS, T.: *Programming with pcap*, 2011, <http://www.tcpdump.org/pcap.html>
- [2] SCHIFFMAN, M.: *Building Open Source Network Security Tools: Components and Techniques*, Wiley, 2003, ISBN 0-47-1205443-3
- [3] RFC 1058: RIP version 1, <http://tools.ietf.org/html/rfc1058>
- [4] RFC 2453: RIP version 2, <http://tools.ietf.org/html/rfc2453>
- [5] RFC 2080: RIPv2 for IPv6, <http://tools.ietf.org/html/rfc2080>