Nástroj monitorovania RIP a RIPng

Sieťové aplikácie a správa sietí

2015/2016

22. novembra 2015

Autor: Peter Gazdík (xgazdi03@stud.fit.vutbr.cz)

Fakulta Informačních Technologií
Vysoké Učení Technické v Brně

Obsah

1 Popis implementácie

1.1 Sniffer RIPv1, RIPv2 a RIPng správ

Implementácia využíva knižnice ‘libpcap‘, ktorá umožňuje odchytávanie paketov v promiskuitnom móde sieťovej karty.

Aby klientská aplikácia nemusela spracovávať všetku komunikácia prichádzajúcu na sieťovú kartu, je využité filtrovanie, ktoré poskytuje táto knižica a ktoré obsluhuje jadro operačného systému. Nedochádza tak k častému prepínaniu kontextu. Takýmto spôsobom je zabezpečené, že aplikácia spracováva len komunikáciu, ktorá prichádza na UDP port číslo 520 a 521, viď popis jednotlivých protokolov.

Po prijatí paketu dochádza k jeho postupnému „vybaľovaniu“. Ako prvá sa na začiatku správy nachádza ethernetová hlavička, Nakoľko nás ale jej obsah nezaujíma a zároveň má fixnú dĺžku, môžeme sa posunúť priamo na IP hlavičku.

V prvom kroku musíme naskôr určiť verziu IP protokolu, t.j. či sa jedná o protokol IPv4 alebo IPv6. Po určení správnej verzie môžeme určiť odosieľateľa správy, ktorého uvedieme neskôr vo výpise. Následne sa môžeme v prípade IPv6 posunúť o fixnú dĺžku a v prípade IPv4 o veľkosť hlavičky, ktorá sa uvádza hneď za verziou protokolu.

Posledným protokolom obaľujúci RIP správu je UDP protokol, z ktorého môžeme pohodlne určiť veľkosť samotnej RIP správy a započať tak jej spracovávanie.

Spracovávanie správy vykonávame s prihliadnutím na verziu smerovacieho protokolu. Medzi protokolom RIPv1 a RIPv2 nie sú až také veľké rozdiely, avšak protokol RIPng je značne odlišný. Napriek tomu, že protokol RIPng nesie záznamy o IPv6 adresách, položky s týmito záznammi majú rovnakú dĺžku ako u RIP protokolu.

Výstup z aplikácie je možné vidieť v kapitole 2.

1.2 Podvrhovač falošných RIPv2 Response správ

Po spracovaní všetkých parametrov, ktorých je v prípade tejto aplikácie neúrekom, dochádza k zostaveniu RIPv2 paketu.

Po jeho zostavení, ktoré nie je nijak záludné, je odoslaný využitím BSD soketov. Nakoľko potrebujeme odosielať z UDP portu číslo 520, je potrebné aplikáciu spúšťať s oprávnením roota.

Ak nie je špecifikované rozhranie, na ktoré má byť paket odoslaný, je odoslaný na všetky dostupné rozhrania systému.

2 Popis útoku

Využitím aplikácie `myripsniffer` získame detailnejšie informácie o prebiehajúcej komunikácii na rozhraní, na ktorom chceme vykonať útok. V tomto prípade budeme zachytávať komunikáciu na rozhraní `eth0`. Aplikáciu je nutné spustíť s právami roota z dôvodu, že využíva 'libpcap' knižnicu.

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

Aplikácia je schopná zachytiť tri druhy protokolov: RIPv1, RIPv2 a RIPng. Pri všetkých prípadoch sa môže jednať o správy typu `Request` alebo `Response`. Vo verzii 2 protokolu RIP je možné vidieť okrem záznamov aj zabezpečenie správy spolu s heslom.

Zachytená komunikácia vyzerá napr. následovne:

```
[23:04:03] RIPv2 from 10.0.0.1
Command: Request (1)
========== ENTRY ===========
Route Tag: 0
Address Family Identifier: unknown (0)
Metric: 16

[23:04:04] RIPv2 from 10.0.0.1
Command: Response (2)
====== AUTHENTICATION ======
Authentication type: Simple password
Password: ISA>28114bb8715
========== ENTRY ===========
Route Tag: 0
Address Family Identifier: IP (2)
IP Address: 10.48.51.0
Netmask: 255.255.255.0
Next Hop: 0.0.0.0
Metric: 1
========== ENTRY ===========
    ...

[23:04:04] RIPng from fe80::a00:27ff:fe1b:716d
Command: Response (2)
========== ENTRY ===========
Route Tag: 0
IPv6 Prefix: fd00::
Prefix Length: 64
Metric: 1
========== ENTRY ===========
...
```

Najdôležitejšia časť pre úspešné vykonanie útoku je záznam s heslom, ktorým musíme náš záznam podpísať.

K podvrhnutiu falošného záznamu využijeme aplikáciu `myripresponse`. Útok môže vyzerať napr. následovne:

```
sudo ./myripresponse -i eth0 -r 10.10.10.0/24 -p "ISA>28114bb8715"
```

Aj v tomto prípade je nutné spustenie s oprávneniami roota, nakoľko aplikácia využíva port číslo 520. Ak všetko prebehlo úspešne, v smerovacej tabuľke routera sa bude nachádzať nový záznam obshujúci cestu k sieti `10.10.10.0/24`.

Literatúra

[1] Hedric, C.: Routing Information Protocol. RFC 1058.
URL http://tools.ietf.org/html/rfc1058

[2] Malkin, G.: RIP Version 2. RFC 2453.
URL http://tools.ietf.org/html/rfc2453

[3] Malkin, G.: RIPng for IPv6. RFC 2080.
URL http://tools.ietf.org/html/rfc2080