Fakulta informačních technologií

Vysoké Učení Technické v Brně

Projekt do předmětu ISA

Nástroje monitorující a generující zprávy jednoduchých distance-vector protokolů

Autor:
Hynek Bernard
xberna16

Datum: 14.11. 2018

Obsah

1 Zadání

1) nastudovat si směrovací protokoly RIP a RIPng;

2) naprogramovat sniffer RIPv1, RIPv2 a RIPng zpráv; DHCP serveru.

3) naprogramovat podvrhávač falešných RIPng Response zpráv;

4) za použití obou nástrojů, které jste si předpřipravili v předchozím bodě pak provést úspěšný útok;

2 Problematika

Je zapotřebí podvrhnout zprávu RIPng protokolu, která sdělí routerům falešnou trasu do jiné síťe (konkrétně 2001:db8:0:abcd::/64).

2.1 RIP Protokol

2.1.1 Popis

RIP odesílá v pravidelných intervalech (okolo 30 sekund), nebo při změně topologie sítě, zprávy o směrovacích tabulkách. Když router přijme zprávu od sousedního routeru ve které je popsána kratší cesta než dosavadní uložená, nebo ještě neuložená, aktualizuje svoji tabulku a přičte metric hodnotu o 1 (počet routerů přes které bude komunikace probíhat). Router udržuje vždy jen nejkratší cestu (tzn. nejnižší metric hodnota). Maximální metric hodnota je 15, pokud by se dostala na 16, tak se označí jako nekonečná a záznam se zahazuje.

3 Implementace

3.1 Sniffer

3.1.1 Popis

Program skenuje zadaný interface na portech 520 a 521 a vypisuje důležité údaje o packetech které souhlasí s formátem zprávy RIP protokolu.

3.1.2 Výstup

Formát vypsané zprávy :

```
---------------------------------
src: sourceMAC  sourceIP dst:  destinationMAC destinationIP
Version:verzeRIP Command:čísloCommandu
/*Zde se vypíšou všechny záznamy zprávy v následujícím formátu pro RIPng*/
IPv6 Prefix:ipv6Adresa Route Tag: hexRouteTag hopCount:čísloMetric
/*Pokud je ve zprávě ověřování v protokolu RIPv2*/
AuthType:AuthType(dvě čísla oddělena mezerou) Pass: heslo
/*Zde se vypíšou všechny záznamy zprávy v následujícím formátu pro RIPv1,RIPv2*/
IP addr:ipv4Adresa NetMask:síťováMaska NextHop:ipv4AdresaRouteru HopCount:čísloMetric
```

Výstup RIPv1 by mohl být osekaný o NetMask a NextHop, ale zachoval jsem tyto pole pro zachování formátu výstupu pro IPv4, vždy se do polí vypíše 0.0.0.0.

3.1.3 Použití

Program se spouští s parametrem interface který chceme scanovat, jiné spuštění není možné

```
./myripsniffer -i <interface>
```

3.1.4 Zajímavosti

Jakmile je packet odchycen, vytvoří se pro něj objekt, ihned poté se vypíše a zahodí se. Provádím scanování pouze portů 521 a 520 využitím pcap.

3.1.4.1 Testování Pro testování jsem použil packety ze stránky http://packetlife.net/captures/protocol/rip/ a ze zadání projektu. Přehrával jsem soubory .pcap na rozhraní a kontroloval správnost výstupu a také jsem měl zaplý image pro uskutečnění útoku, který v pravidelných intervalech odesílal packety. Porovnával jsem výstup svého programu s výstupem programu Wireshark.

3.2 Podvrhávač

3.2.1 Popis

Program slouží pro kraftování packetů RIPng zpráv. Podle zadaných parametrů vyplní packet a odešle ho na interface s názvem zadaným v parametru. Povinné parametry jsou -i (interface) a -r (adresa podvrhávané sítě), volitelné parametry jsou -n (adresa next hopu), -m (metrika), -n (next hop) a -t (hodnota router tagu).

3.2.2 Použití

V parametru -r musí být IPv6 adresa s maskou označenou za lomítkem, -n označuje adresu next hopu, zde se již maska neuvádí. Parametry -t a -m očekávají číslo v decimální podobě. -r a -i jsou arumenty povinné. Při zadání špatných parametrů (včetně parametru -h) se vypíše nápověda s popisem.

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

3.2.3 Zajímavosti

Packet tvořím celý už od ethernetové hlavičky v kódu. Poté odešlu svůj buffer na zadané rozhraní bez jakéhokoliv systémového zásahu do packetu. Neimplementoval jsem podporu výpisu MD5, jelikož jsem se o rozšíření standardu dozvěděl těsně před deadlinem a už nebyl čas na implementaci.

3.2.3.1 Testování Správnost vytvořených packetů byla testována programem wireshark, nejvíce jsem testoval checksum, protože při výpočtu IPv6 checksumu je jiný postup než u IPv4, proto se nedal použít celý kód z projektu předmětu IPK. Funkčnost byla otestována provedením úspěšného útoku.

4 Demonstrace

Vytvořil jsem síťový most (virtuální rozhraní) br1 na který jsem připojil virtualizovaný referenční obraz počítače, kde jsem aplikoval vygenerovanou konfiguraci pro můj login (xberna16).

4.1 Získání hesla a odchycení cest

Na svém počítači jsem spustil ripsniffer pro odchytávání packetů a čekal na příjem packetů z image.

```
./myripsniffer -i br1
```

Do 30 sekund jsem odchytil 4 packety, z čehož 2 byly duplikáty, na screenu můžeme vidět výstup.

```
--------------------------------
src: 33:33:00:00:00:9 fe80::a00:27ff:fe98:cff2 dst: 08:00:27:98:cf:f2 ff02::9
Version:1 Command:2
IPv6 Prefix:fd00::/64 Route Tag: 0x0000 hopCount:1
IPv6 Prefix:fd00:d3:2d78::/64 Route Tag: 0x0000 hopCount:1
IPv6 Prefix:fd00:104:2a1c::/64 Route Tag: 0x0000 hopCount:1
IPv6 Prefix:fd00:9cc:62::/64 Route Tag: 0x0000 hopCount:1
IPv6 Prefix:fd00:a56:154e::/64 Route Tag: 0x0000 hopCount:1
--------------------------------
src: 33:33:00:00:00:9 fe80::a00:27ff:fe98:cff2 dst: 08:00:27:98:cf:f2 ff02::9
Version:1 Command:2
IPv6 Prefix:fd00::/64 Route Tag: 0x0000 hopCount:1
IPv6 Prefix:fd00:d3:2d78::/64 Route Tag: 0x0000 hopCount:1
IPv6 Prefix:fd00:104:2a1c::/64 Route Tag: 0x0000 hopCount:1
IPv6 Prefix:fd00:9cc:62::/64 Route Tag: 0x0000 hopCount:1
IPv6 Prefix:fd00:a56:154e::/64 Route Tag: 0x0000 hopCount:1
--------------------------------
src: 01:00:5e:00:00:9 10.0.0.1 dst: 08:00:27:98:cf:f2 224.0.0.9
Version:2 Command:2
AuthType:0 2 Pass: ISA>2861445865a
IP addr:10.49.54.0 NetMask:255.255.255.0 NextHop:0.0.0.0 hopCount:1
IP addr:10.101.110.0 NetMask:255.255.255.0 NextHop:0.0.0.0 hopCount:1
IP addr:10.114.212.0 NetMask:255.255.255.0 NextHop:0.0.0.0 hopCount:1
IP addr:10.211.97.0 NetMask:255.255.255.0 NextHop:0.0.0.0 hopCount:1
--------------------------------
src: 01:00:5e:00:00:9 10.0.0.1 dst: 08:00:27:98:cf:f2 224.0.0.9
Version:2 Command:2
AuthType:0 2 Pass: ISA>2861445865a
IP addr:10.49.54.0 NetMask:255.255.255.0 NextHop:0.0.0.0 hopCount:1
IP addr:10.101.110.0 NetMask:255.255.255.0 NextHop:0.0.0.0 hopCount:1
IP addr:10.114.212.0 NetMask:255.255.255.0 NextHop:0.0.0.0 hopCount:1
IP addr:10.211.97.0 NetMask:255.255.255.0 NextHop:0.0.0.0 hopCount:1
```

Při analýze zjistíme, že heslo je **ISA>2861445865a** a odchycené routy pro protokol RIPv2 jsou:

```
10.49.54.0 | 255.255.255.0 | 0.0.0.0 | 1
10.101.110.0 | 255.255.255.0 | 0.0.0.0 | 1
10.114.212.0 | 255.255.255.0 | 0.0.0.0 | 1
10.211.97.0 | 255.255.255.0 | 0.0.0.0 | 1
```

Routy pro protokol RIPng jsou:

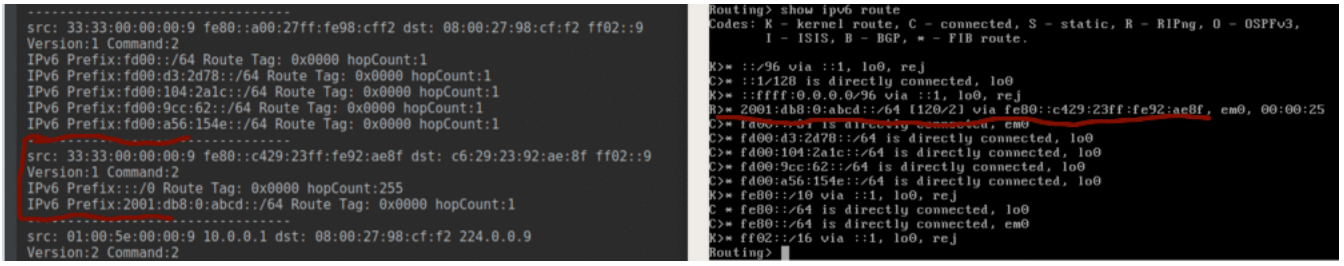
```
fd00::/64 | 0x0000 | 1
fd00:d3:2d78::/64 | 0x0000 | 1
fd00:104:2a1c::/64 | 0x0000 | 1
fd00:9cc:62::/64 | 0x0000 | 1
fd00:a56:154e::/64 | 0x0000 | 1
```

4.2 Simulace útoku

Na svém počítači jsem spustil ripsniffer pro odchytávání packetů a potom jsem spustil program ripresponse následovně

```
./myripsniffer -i br1
./myripresponse -i br1 -r 2001:db8:0:abcd::/64
```

Na screenu je na levé straně znázorněný odeslaný packet programem a na pravé straně výpis routovací tabulky referenčního obrazu s podtrženou podvrženou cestou, útok byl proveden úspěšně.



5 Literatura

RFC 1058 - SIP-RIP https://tools.ietf.org/html/rfc1058

RFC 2453 - RIP Version 2 https://tools.ietf.org/html/rfc2453

RFC 2080 - RIPng for IPv6 https://tools.ietf.org/html/rfc2080

Van Jacobson, Craig Leres and Steven McCanne
Manpage of PCAP
http://www.tcpdump.org/manpages/pcap.3pcap.html