Vysoké učení technické v Brně

FIT

IPK - Počítačové komunikace a sítě
2018

Projekt - DHCP Starvation útok

Jiří Juřica / xjuric29

Obsah

Teorie

DHCP

DHCP (z anglického Dynamic Host Configuration Protocol) je klient-server služba sloužící k zaslání potřebných informací o síti nově se připojujícímu klientu. Po připojení klient zažádá o údaje pomocí zprávy Discover a pokud má server volné prostředky (má volnou ip adresu z nastaveného rozsahu), odpoví zprávou Offer. Tím výměna zpráv ale nekončí a klient ještě serveru musí potvrdit pomocí zprávy Request, že má o údaje zájem. Je to ošetření stavu, kdy na síti funguje více DHCP serverů a server vrátí zprávu Ack.

DHCP Starvation

Útok probíhá zahlcením serveru fiktivními požadavky, dokud nevyčerpá všechny jeho prostředky a je možné jej aplikovat dvěma způsoby [1]:

- Zasílat pouze Discover zprávy
    - Protože se komunikace korektně nedokončí, prostředky jsou uvolněny jen na velmi krátkou dobu. Takový útok má smysl v případě, že je třeba DHCP server bez zbytečných stop pouze krátkodobě vyřadit z provozu a snažit se např. podvrhnout konkrétnímu klientovi údaje.
- Korektně vést celou komunikaci
    - Při korektním dokončení útok vede k vyřazení DHCP serveru z provozu na platnou dobu poskytnutých prostředků (lease time, obvykle 24h). Nově se připojující klienti nedostanou údaje žádné.

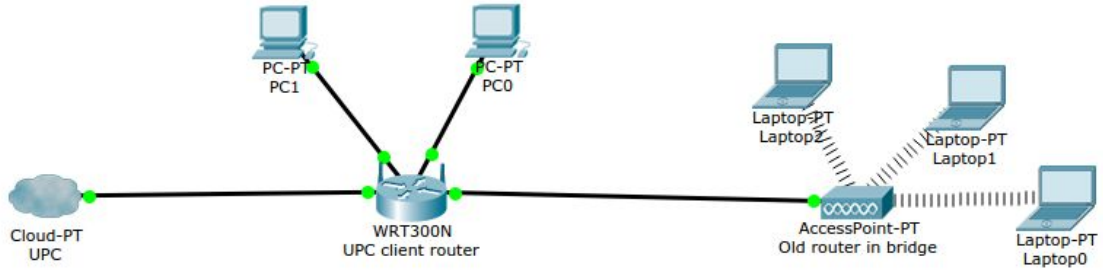
Implementace

Pro svou práci jsem si zvolil zjednodušený útok se zasíláním Discover zpráv, který mi umožnil použít běžný udp socket. I tak bylo ale zapotřebí nastudovat si standard rfc2131 [2], ve kterém je podrobně uveden obsah jednotlivých DHCP zpráv, které se klient a server vyměňují. Informace ze standardu jsem doplňoval obsahem reálných zpráv z mé sítě zjištěných pomocí programu Wireshark.

Pro generování zprávy jsem nakonec zvolil vytvoření vlastní struktury a k tomu přidal jednoduchou funkci na generování mac adres, která začíná vždy od 00:00:00:00:00:00. Program pak cyklicky zasílá zprávy s odlišnými mac adresami, dokud mu není zaslán signál SIGINT. Po dobu běhu programu není možné od DHCP serveru dostat ip adresu.

Demonstrace činnosti aplikace

Pro demonstraci jsem zvolil reálnou síť, kterou máme v domě.



Pro zatím, když útok neprobíhá, zahodím informace, co mi přidělilo DHCP a zažádám o nové.

```
jirkaj@Inspiron-7537:~/Git/ipk/projects/proj2$ sudo dhclient -r enp3s0f1
Killed old client process
jirkaj@Inspiron-7537:~/Git/ipk/projects/proj2$ sudo dhclient enp3s0f1
jirkaj@Inspiron-7537:~/Git/ipk/projects/proj2$
```

Oba dva příkazy se vykonaly, znamená to tedy, že DHCP služba normálně funguje a s mým počítačem se domluví. Teď spustím aplikaci pro útok.

```
jirkaj@Inspiron-7537:~/Git/ipk/projects/proj2$ sudo ./ipk-dhcpstarve -i enp3s0f1
00:00:00:00:00:00
00:00:00:00:00:01
00:00:00:00:00:02
00:00:00:00:00:03
00:00:00:00:00:04
00:00:00:00:00:05
00:00:00:00:00:06
00:00:00:00:00:07
00:00:00:00:00:08
00:00:00:00:00:09
00:00:00:00:00:0A
00:00:00:00:00:0B
00:00:00:00:00:0C
00:00:00:00:00:0D
00:00:00:00:00:0E
00:00:00:00:00:0F
00:00:00:00:00:10
00:00:00:00:00:11
```

K tomu přidávám snímek z Wiresharku.

```
1442… 1821.6873893… 192.168.0.136    255.255.255.255    DHCP    342 DHCP Discover - Transaction ID 0x0
1442… 1821.6873993… 192.168.0.136    255.255.255.255    DHCP    342 DHCP Discover - Transaction ID 0x0
1442… 1821.6874094… 192.168.0.136    255.255.255.255    DHCP    342 DHCP Discover - Transaction ID 0x0
1442… 1821.6874190… 192.168.0.136    255.255.255.255    DHCP    342 DHCP Discover - Transaction ID 0x0
1442… 1821.6874288… 192.168.0.136    255.255.255.255    DHCP    342 DHCP Discover - Transaction ID 0x0
1442… 1821.6874385… 192.168.0.136    255.255.255.255    DHCP    342 DHCP Discover - Transaction ID 0x0
1442… 1821.6874484… 192.168.0.136    255.255.255.255    DHCP    342 DHCP Discover - Transaction ID 0x0
1442… 1821.6874582… 192.168.0.136    255.255.255.255    DHCP    342 DHCP Discover - Transaction ID 0x0
```

```
Client IP address: 0.0.0.0
Your (client) IP address: 0.0.0.0
Next server IP address: 0.0.0.0
Relay agent IP address: 0.0.0.0
Client MAC address: 00:00:00_00:00:8b (00:00:00:00:00:8b)
Client hardware address padding: 00000000000000000000
```

A pokusím znovu zažádat o údaje z DHCP.

```
jirkaj@Inspiron-7537:~$ sudo dhclient -r enp3s0f1
jirkaj@Inspiron-7537:~$ sudo dhclient enp3s0f1
```

Tentokrát se druhý příkaz neprovedl a vykoná se, až se program vypne.

Literatura

[1] HALAŠKA, Peter. *Generátor kybernetických útoků* [online]. Vysoké učení technické v Brně. Fakulta elektrotechniky a komunikačních technologií, 2016 [cit. 2018-04-09]. Dostupné z: http://hdl.handle.net/11012/59938. Diplomová práce. Vysoké učení technické v Brně. Fakulta elektrotechniky a komunikačních technologií. Ústav telekomunikací. Vedoucí práce Jan Hajný.

[2] R. Droms, RFC 2131:Dynamic Host Configuration Protocol, https://tools.ietf.org/html/rfc2131