# IPK Projekt 2

Varianta 2: DHCP Starvation útok

Daniel Dolejška (xdolej08)

Duben 2018

# Obsah



# Seznam obrázků

# 1 Teorie útoku

V této sekci je popsána teorie a princip DHCP starvation útoku a k čemu jej lze využít.

## 1.1 Princip útoku

Cílem útoku je simulovat v síti zařízení žádající o přiřazení IP adresy (popř. dalšího síťového nastavení) a vyčerpat tak množinu adres, kterou má místní DHCP server/servery k dispozici.

Útočník poté může spustit svůj vlastní DHCP server a uživatelům přidělovat legitimní síťové adresy, které získal. Následně může, díky plné kontrole nad přiděleným nastavením, směrovat síťový provoz dle libosti a dospět tak k dalšímu typu útoku - **MITM, man-in-the-middle attack**.

## 1.2 Zprostředkování útoku

Útočící aplikace provede za pomoci **MAC spoofing** odeslání DHCPDISCOVER packetu s podvrženou MAC adresou. Vyčká na odpověď DHCP serveru ve formě DHCPOFFER packetu, který následně potvrdí pomocí DHCPREQUEST packetu. Celý proces je dokončen ve chvíli, kdy útočící aplikace obdrží DHCPACK.

Celý tento proces může aplikace opakovat, dokud množinu přiřaditelných adres legitimního DHCP serveru nevprázdní.

Útočící aplikace následně může začít odpovídat na DHCP broadcasty zařízení namísto legitimního DHCP serveru a nabízet získané IP adresy s podvrženým síťovým nastavením.

# 2 Implementace

Tato sekce obsahuje informace o mé implementaci útočící aplikace.

## 2.1 Soubory aplikace

Aplikace je rozdělena do několika souborů v několika kategoriích, kde se každá kategorie stará pouze o svou oblast:

**Hlavní program** Obsahuje hlavní řídící program, využívající funkce z ostatních souborů projektu, implementující funkcionalitu DHCP starvation útoku.

- main.c

**DHCP** Obsahuje funkce zajišťující práci s daty protokolu DHCP v přijatém packetu, dále zajišťují možnost vytváření těchto packetů, validaci dat a jejich jednoduchou modifikaci.

Část obsahu tohoto souboru (definice datové struktury protokolu a definice konstantních hodnot) byla převzata od Internet Systems Consortium, Inc.

- dhcp.h
- dhcp.c

**Síť** Obsahuje funkce zajišťující práci s daty ethernetové hlavičky, hlavičky protokolu IP a UDP, dále zajišťují možnost vytváření těchto dat v packetech, validaci dat a jejich jednoduchou modifikaci.

- network.h
- network.c

**Obecné funkce** Obsahuje několik jednoduchých funkcí pro náhodné generování čísel a MAC adres.

- general.h
- general.c

## 2.2 Posloupnost akcí

1. Příprava před prvotním odesíláním

   V této chvíli aplikace generuje náhodnou MAC adresu a vytváří hlavičky datagramu pro broadcast.

2. Odesílání DHCPDISCOVER

   Aplikace přidá za vytvořené hlavičky do datagramu potřebná data DHCP protokolu a ten následně odešle.

3. Příjem DHCPOFFER

   Při příjmu datagramů probíhá kontrola *IP adresy zdroje*, *atributu chaddr, xid a op DHCP protokolu* a v neposlední řadě *option 0x35 (message type) DHCP protokolu.*

   Na základě výsledků kontrol bud probíhá krok číslo 3 znovu (příjem dalšího datagramu), nebo se pokračuje ve zpracování dalším krokem.

   V případě nepřijetí žádného datagramu protokolu DHCP se aplikace po několika sekundách vrací na krok číslo 2 a opakuje odeslání DHCPDISCOVER datagramu. Při opakovaném neúspěchu stejného typu je aplikace ukončena.

4. Odesílání DHCPREQUEST

   Probíhá vytvoření a odeslání odpovědi na přijatý DHCPOFFER datagram.

5. Příjem DHCPACK

   Při příjmu datagramů probíhají stejné kontroly jako při kroku 3. Pokud se jedná o datagram požadovaného typu je IP adresa vypsána na stdout a označena za získanou.

   *Aplikace dále pokračuje znovu bodem 1.*

# 3 Demonstrace činnosti

## 3.1 Spuštění aplikace

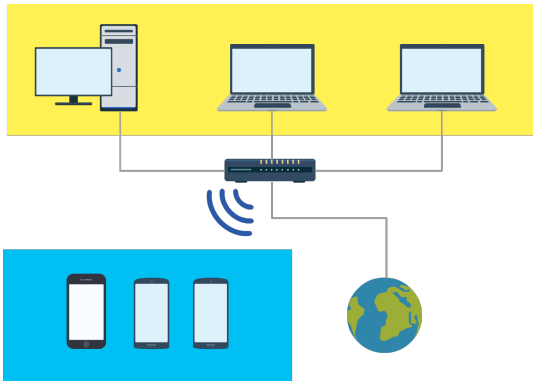
Aplikace má povinný přepínač -i s názvem síťového rozhraní, ze kterého bude aplikace odesílat kompromitující data do sítě.

```
isa2015@isa2015:/media/sf_ipk$ sudo ./ipk-dhcpstarve -i <interface>
```

*Podrobnější informace k spuštění aplikace či překladu zdrojových souborů jsou k dispozici v README.md souboru.*

## 3.2 Útok na malou domácí síť

V této sekci jsou uvedeny příklady použití aplikace v domácím prostředí malé sítě (diagram sítě viz Obrázek 1). Součástí jsou i příklady časové náročnosti implementovaného řešení za různé velikosti množiny přiřaditelných adres DHCP serveru (DHCP pool).



Obrázek 1: Diagram použité sítě

V příkladu číslo 1 je ukázka jednoduchého použití aplikace. *Podrobnější informace k spuštění aplikace či překladu zdrojových souborů jsou k dispozici v README.md souboru.*

```
isa2015@isa2015:/media/sf_ipk$ sudo ./ipk-dhcpstarve -i eth0
192.168.0.100
192.168.0.101
...
192.168.0.108
192.168.0.109
isa2015@isa2015:/media/sf_ipk$
```

Příklad 1: Výstup aplikace při použití v malé síti

Zmocnění se desíti adres v malé domácí síti trvala zhruba 28 vteřin. Z toho 16 vteřin je konečný timeout. Příklad použití a výstupů viz Příklad 2.

```
isa2015@isa2015:/media/sf_ipk$ time sudo ./ipk-dhcpstarve -i eth0
192.168.0.100
...
192.168.0.109

real        0m27.878s
user        0m0.000s
sys         0m0.008s
isa2015@isa2015:/media/sf_ipk$
```

Příklad 2: Výstup aplikace při měření času a získávání 10 adres v malé síti

Příklad časové náročnosti se zmocněním se 150 adres ve stejné síti viz Příklad 3.

```
isa2015@isa2015:/media/sf_ipk$ time sudo ./ipk-dhcpstarve -i eth0
192.168.0.100
...
192.168.0.249

real        2m46.688s
user        0m0.000s
sys         0m0.040s
isa2015@isa2015:/media/sf_ipk$
```

Příklad 3: Výstup aplikace při měření času a získávání 150 adres v malé síti

Všechny příklady uvedené v této sekci provedeny za použití výchozího nastavení (více o možnostech a výchozím nastavení viz soubor README.md).