VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta informačních technologií

Dokumentácia k projektu z predmetu PDS

DHCP útoky

Brno
26. 04. 2018

Michal Gabonay
xgabon00@stud.fit.vutbr.cz

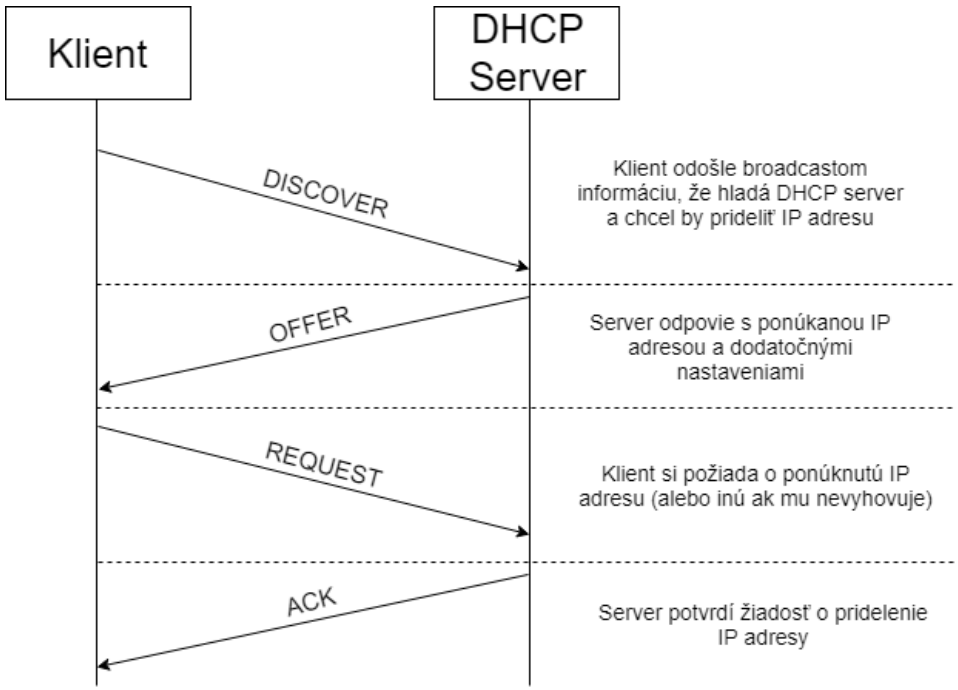
Obsah

1. Úvod

Tento dokument slúži ako dokumentácia k projektu do predmetu PDS, ktorého úlohou je naprogramovať aplikácie realizujúce dva DHCP útoky, a to DHCP Starvation a Rogue DHCP server. V tomto dokumente je ďalej vysvetlená problematika DHCP protokolu a princíp samotnýh DHCP útokov, popis implementácie týchto útokov, popis demonštrácie útokov na vytvorenej (virtuálnej) sieti a nakoniec návod na použitie výslednej aplikácie.

2. DHCP

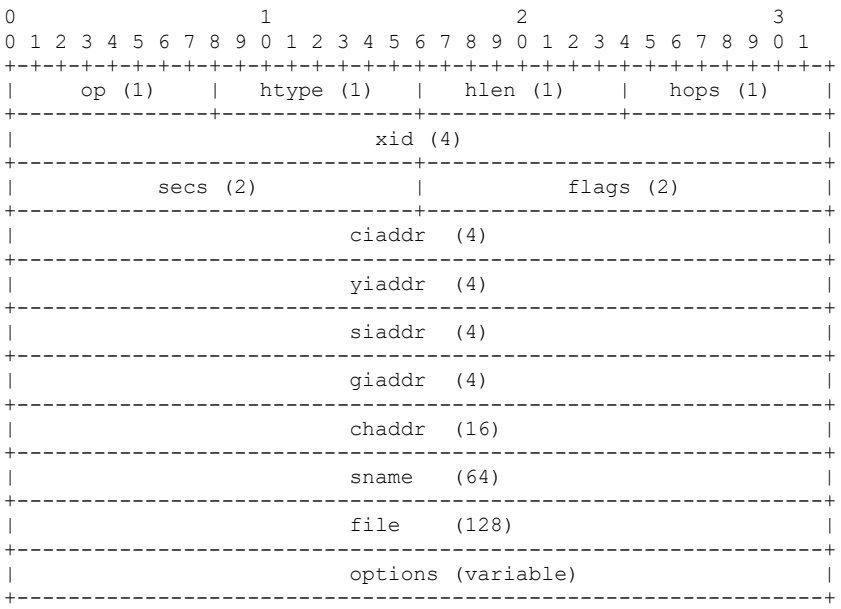
Protokol DHCP (**D**ynamic **H**ost **C**onfiguration **P**rotocol) je aplikačným protokolom, ktorý slúži na automatickú konfiguráciu počítača (klienta) pripojeného do počítačovej siete. DHCP server prostredníctvom protokolu DHCP dynamicky prideľuje IP adresy klientom, ktorých platnosť je obmedzená na určitú dobu. Funguje na princípe klient-server modelu [1]. Klient ako prvý naväzuje spojenie so serverom, zaslaním DHCP správy typu *DISCOVER*, odoslanú cez broadcast. Typická komunikácia medi klientom a DHCP serverom je znázornená na Obrázku 1. Server v sebe uchováva informácie o klientoch a to najmä ich MAC adresu, IP adresu a čas kedy končí „prenájom“ (lease) adresy. Okrem toho server udržiava zoznam s voľnými adresami, ktoré môže prenajať klientom.



Obrázok 1: Komunikácia s DHCP serverom

2.1. DHCP hlavička

Komunikácia medzi serverom a klientom má dopredu známy formát. DHCP hlavička je špecifikácia hlavičky protokolu BOOTP. Hlavička obsahuje mnoho informácií [2]. Ako je vidieť na Obrázku 2, všetky parametre správy (okrem parametra *options*) majú dopredu známu dĺžku. Informácie o jednotlivých parametroch definuje RFC 2131 (Droms, 1997). Parameter *options* je v skutočnosti zoznam ďalších parametrov. Parameter vždy začina tzv. *Magic Cookie*, ktorá obsahuje štyri oktety s hodnotami 99, 130, 83 a 99. Koniec zoznamu je označený jedným oktetom s hodnotou 255 tzv. *end option.*



Obrázok 2: Hlavička DHCP správy

2.2. Typy DHCP správ

Protokol DHCP definuje 8 rôznych druhov správ. Tieto správy môžeme rozdeliť podľa toho kto ich odosiela.

Správy odosielané klientom:

- DHCPDISCOVER – klient broadcastom zasiela správu, že má záujem o pridelenie IP adresy
- DHCPREQUEST – klient žiada o pridelenie ponúknutej IP adresy
- DHCPDECLINE – klient zamieta pridelenú IP
- DHCPRELEASE – klient uvoľňuje svoju IP adresu a ruší svoju dobu prenájmu
- DHCPINFORM – klient iba zisťuje lokálne konfiguračné parametre

Správy odosielané serverom:

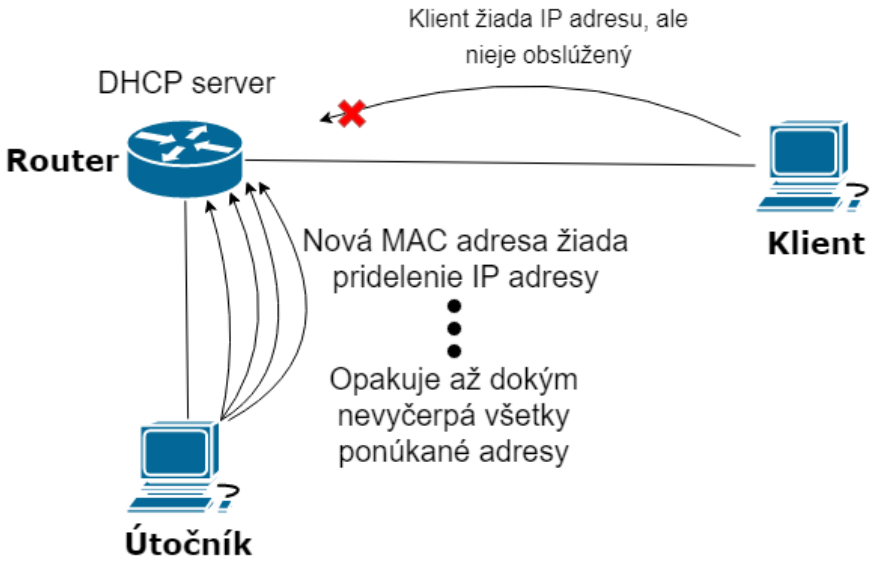
- DHCPOFFER – server odpovedá na DHCPDISCOVER s ponukou IP adresy a ďalšími konfiguráciami
- DHCPACK – server odpovedá na DHCPREQUEST a potvrdzuje priradenú IP adresu
- DHCPNAK – server odpovedá na DHCPREQUEST zamietnutím žiadosti na IP adresu

3. DHCP útoky

Existuje viacero typov útok zameraných na DHCP, pre účely projektu si popíšeme fungovanie útoku DHCP Starvation (vyhladovanie) a DHCP spoofing (Rogue DHCP server).

3.1. DHCP Starvation

Útok DHCP starvation je v podstate DoS útok na daný DHCP server [3]. To znamená, že útočník odosiela veľké množstvo fiktívnych žiadostí o pridelenie IP adresy pre falošné MAC adresy (resp. Client hardware adresy) tak, že bude odosielať DHCPDISCOVER a DHCPREQUEST správy pomocou UDP broadcastu. Týmto vyčerpá všetky možné adresy, ktoré daný DHCP server ponúka, jeho pool IP adries bude plne obsadený. V prípade, že do siete vstúpi skutočný klient, ktorý má záujem o pridelenie IP adresy, nebude obslúžený DHCP serverom, pretože ten je plne vyťažený a nemá žiadnu adresu na prenájom. Prípad takého útoku, je znázornený na Obrázku 3. Podrobnosti implementácie útoku sú popísané v nasledujúcej kapitole (4.1) tohto dokumentu.

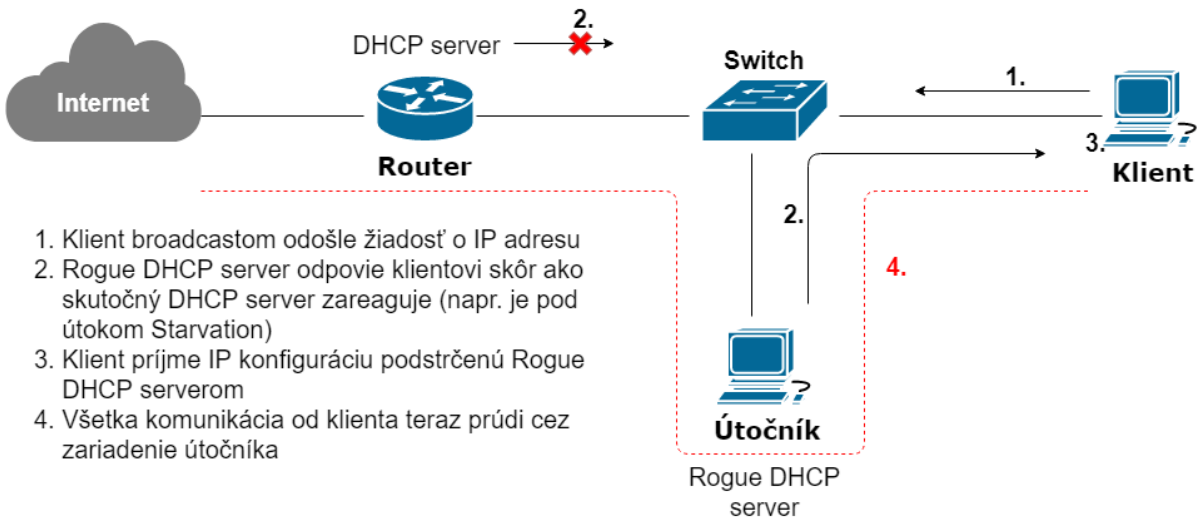


Obrázok 3: Model DHCP Starvation útoku

3.2. Rogue DHCP server

Rogue DHCP server síce je DHCP server a klientovi dá IP konfiguráciu, ale tento server nie je autorizovaný administrátorom siete, a tým pádom predstavuje bezpečnostné riziko [4].

Útočník takýto rogue DHCP server podsunie do siete. Keď klient odošle pomocou broadcastu DHCP DISCOVER paket, rogue DHCP server odpovie skôr ako pravý DHCP server. Buď je proste rýchlejší ale obvykle útočník tento pravý DHCP server predtým zamestnal, napríklad DHCP Starvation útokom. Rogue DHCP server klientovi odošle DHCP OFFER správu s IP adresou, ale taktiež s ďalšími nastaveniami ako hlavne „default gateway“. Vďaka tomu bude všetka komunikácia zo zariadenia klienta prúdiť cez zariadenie útočníka. Všetky takéto odosielané a prijímané pakety od klienta môžu byť útočníkom odchytené, otvárané a spracovávané. Základný princíp je tiež znázornený na Obrázku 4. Podrobnosti implementácie útoku sú popísané v nasledujúcej kapitole (4.2) tohto dokumentu.



Obrázok 4: Model Rogue DHCP server útoku

4. Popis implementácie

Táto kapitola popisuje postup, postrehy a zaujímavosti z implementácie aplikácie vykonávajúcej útoky DHCP Starvation a DHCP rogue server.

4.1. Implementácia Starvation útoku

Vstupom aplikácie je len názov rozhrania, na ktorom sa má nachádzať DHCP server, na ktorý má byť vykonaný útok. Aplikácia si vytvorí 2 *sockety,* jeden na odosielanie a jeden na prijímanie. Socket na odosielanie je v móde *RAW*, hlavne kvôli prispôsobeniu L2 a L3 vrstvy. Podstatnou časťou implementácie bolo vytváranie samotných správ, ktoré sa majú odosielať. Keďže zdrojová IP adresa má byť 0.0.0.0, je treba v odosielaný správach vytvárať jednotlivé hlavičky - Ethernotevú, IPv4, UDP a DHCP.

V ethernetovej hlavičke sa ako zdrojová MAC adresa nastavuje adresa cieľového rozhrania, a ciľová adresa je broadcastová (ff:ff:ff:ff:ff:ff). IP hlavička nieje ničim zaujímavá, zdrojovú adresu nastavuje na 0.0.0.0 a cieľovú nastavuje na 255.255.255.255, čo odpovedá broadcastovej komunikácii. V UDP hlavičke sa nastavuje zdrojový port je nastavený na 68 čo reprezentuje DHCP klienta a cieľový port je 67, čo je DHCP server. Najdôležitejšou úlohou bolo vytvorenie DHCP hlavičky, kde sa hlavne nastavovala hodnota xid, chaddr a options. Xid je identifikátor transakcie medzi klientom a serverom, ktorý sa náhodne generuje, chaddr je náhodne generovaná MAC adresa, ktorá reprezentuje fiktívne zariadenie žiadajúce o priradenie IP. Parameter options sa nastavuje v závislosti od typu posielanej správy. Priebeh útoku je nasledovný:

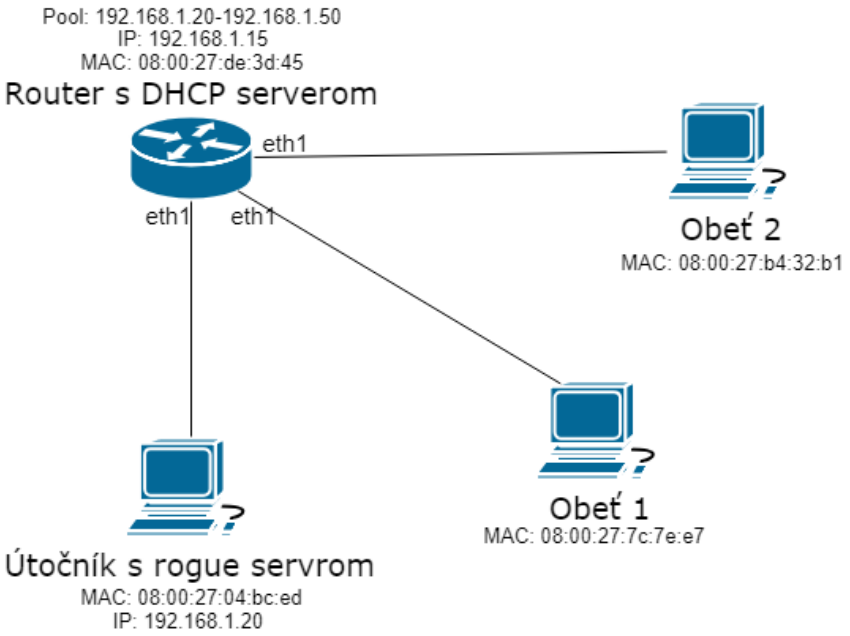
1. Vytvorí sa a odošle sa správa typu *DHCPDISCOVERY*. A čaká sa 1 sekundu, čím sa dá čas DHCP serveru na spracovanie požiadavku.
2. Čaká sa na príchod správy typu *DHCPOFFER*, ak správa nepríde do 4 sekúnd, aplikácia predpokladá, že cieľový DHCP server je vyťažený a nemá čo viac ponúknuť a aplikácia končí, ak správa *DHCPOFFER* príde, spracuje sa.
3. Vytvorí sa a odošle sa správa typu *DHCPREQUEST*, s nastavenými parametrami, ktoré sa získali v kroku (2).
4. Predpokladá sa príchod správy typu *DHCPACK* a pokračuje sa na krok (1).

4.2. Implementácia DHCP Rogue servera

Server po spustení spracuje vstupné parametre. Následne v nekonečnom cykle čaká na príchod DHCP správy na broadcaste, na ktorú by mohol odpovedať. Po príchode správy, server vytvorí DHCP správu, ktorú naplní potrebnými údajmi, hlavne zo vstupných parametrov aplikácie. Žiaľ tento rogue server sa mi nepodarilo stihnúť dokončiť.

5. Demonštrácia činnosti

Testovanie scenára útokov prebehlo na virtuálne sieti, ktorej virtualizácia bola vytvorená za pomoci nástroja *VirtualBox*. Topológia siete je znázornená na Obrázku 5.



Obrázok 5: Topológia testovanej siete

DHCP server ktorý je na routery má pool vyhradený od 192.168.1.20-192.168.1.50. Útočníkovi bola priradená adresa 192.168.1.20.

Priebeh testovanie:

1. Útočník spustí program príkazom *sudo ./pds-dhcpstarve –i eth1*. Vo výpise aplikácie z Obrázku 6 vidno IP adresy, ktoré útočník postupne zaberal.

```
isa2015@isa2015:~/Documents/project2$ sudo ./pds-dhcpstarve -i eth1
taking ip: 192.168.1.40
taking ip: 192.168.1.41
taking ip: 192.168.1.42
taking ip: 192.168.1.43
taking ip: 192.168.1.44
taking ip: 192.168.1.45
taking ip: 192.168.1.46
taking ip: 192.168.1.48
taking ip: 192.168.1.49
taking ip: 192.168.1.47
taking ip: 192.168.1.21
taking ip: 192.168.1.23
taking ip: 192.168.1.24
taking ip: 192.168.1.50
taking ip: 192.168.1.25
taking ip: 192.168.1.26
taking ip: 192.168.1.27
taking ip: 192.168.1.28
taking ip: 192.168.1.29
taking ip: 192.168.1.30
taking ip: 192.168.1.31
taking ip: 192.168.1.34
taking ip: 192.168.1.35
taking ip: 192.168.1.32
taking ip: 192.168.1.33
taking ip: 192.168.1.36
taking ip: 192.168.1.37
taking ip: 192.168.1.38
taking ip: 192.168.1.39
taking ip: 192.168.1.22
isa2015@isa2015:~/Documents/project2$
```

Obrázok 6: výpis aplikácie pds-dhcpstarve

2. Obeť číslo 1 sa snaží získať IP adresu. Zadáva príkaz *sudo ifup eth1*. Na Obrázku 7 je vidno výpis tejto neúspešnej snahy.

```
isa2015@isa2015:~/Documents/project$ sudo ifup eth1
Internet Systems Consortium DHCP Client 4.2.4
Copyright 2004-2012 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/eth1/08:00:27:7c:7e:e7
Sending on   LPF/eth1/08:00:27:7c:7e:e7
Sending on   Socket/fallback
DHCPDISCOVER on eth1 to 255.255.255.255 port 67 interval 3 (xid=0x41cb6872)
DHCPDISCOVER on eth1 to 255.255.255.255 port 67 interval 6 (xid=0x41cb6872)
DHCPDISCOVER on eth1 to 255.255.255.255 port 67 interval 12 (xid=0x41cb6872)
DHCPDISCOVER on eth1 to 255.255.255.255 port 67 interval 16 (xid=0x41cb6872)
DHCPDISCOVER on eth1 to 255.255.255.255 port 67 interval 18 (xid=0x41cb6872)
DHCPDISCOVER on eth1 to 255.255.255.255 port 67 interval 19 (xid=0x41cb6872)
DHCPDISCOVER on eth1 to 255.255.255.255 port 67 interval 14 (xid=0x41cb6872)
DHCPDISCOVER on eth1 to 255.255.255.255 port 67 interval 17 (xid=0x41cb6872)
DHCPDISCOVER on eth1 to 255.255.255.255 port 67 interval 21 (xid=0x41cb6872)
DHCPDISCOVER on eth1 to 255.255.255.255 port 67 interval 7 (xid=0x41cb6872)
DHCPDISCOVER on eth1 to 255.255.255.255 port 67 interval 21 (xid=0x41cb6872)
DHCPDISCOVER on eth1 to 255.255.255.255 port 67 interval 17 (xid=0x41cb6872)
DHCPDISCOVER on eth1 to 255.255.255.255 port 67 interval 14 (xid=0x41cb6872)
DHCPDISCOVER on eth1 to 255.255.255.255 port 67 interval 18 (xid=0x41cb6872)
DHCPDISCOVER on eth1 to 255.255.255.255 port 67 interval 7 (xid=0x41cb6872)
DHCPDISCOVER on eth1 to 255.255.255.255 port 67 interval 12 (xid=0x41cb6872)
DHCPDISCOVER on eth1 to 255.255.255.255 port 67 interval 15 (xid=0x41cb6872)
DHCPDISCOVER on eth1 to 255.255.255.255 port 67 interval 20 (xid=0x41cb6872)
DHCPDISCOVER on eth1 to 255.255.255.255 port 67 interval 15 (xid=0x41cb6872)
DHCPDISCOVER on eth1 to 255.255.255.255 port 67 interval 9 (xid=0x41cb6872)
DHCPDISCOVER on eth1 to 255.255.255.255 port 67 interval 14 (xid=0x41cb6872)
DHCPDISCOVER on eth1 to 255.255.255.255 port 67 interval 6 (xid=0x41cb6872)
No DHCPOFFERS received.
No working leases in persistent database - sleeping.
```

Obrázok 7: snaha o pridelenie IP adresy obeťou 1 (pred rogue servrom)

3. Útočník spustil rougue server príkazom *sudo ./pds-dhcprogue -i eth1 -p 192.168.1.100-192.168.1.199 -g 192.168.1.1 -n 8.8.8.8 -d fit.vutbr.cz -l 3600*
4. Obeť sa znova pokúša získať IP adresu zadaním príkazu sudo ifup eth1, avšak teraz už úspešne. Výpis tejto snahy je na Obrázku 8. Na Obrázku 9 je výpis ifconfig obete 1.

```
isa2015@isa2015:~/Documents/project$ sudo ifup eth1
Internet Systems Consortium DHCP Client 4.2.4
Copyright 2004-2012 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/eth1/08:00:27:7c:7e:e7
Sending on   LPF/eth1/08:00:27:7c:7e:e7
Sending on   Socket/fallback
DHCPDISCOVER on eth1 to 255.255.255.255 port 67 interval 3 (xid=0xfd45af1e)
DHCPREQUEST of 192.168.1.100 on eth1 to 255.255.255.255 port 67 (xid=0x1eaf45fd)
DHCPOFFER of 192.168.1.100 from 192.168.1.1
DHCPACK of 192.168.1.100 from 192.168.1.1
suspect value in domain_name option - discarded
bound to 192.168.1.100 -- renewal in 115228141 seconds.
```

Obrázok 8: snaha o pridelenie IP adresy obeťou 1 (po rogue serveri)

```
eth1      Link encap:Ethernet  HWaddr 08:00:27:7c:7e:e7
          inet addr:192.168.1.100  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe7c:7ee7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1469 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1164 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:259552 (259.5 KB)  TX bytes:244985 (244.9 KB)
```

Obrázok 9: výpis ifconfig obete 1

Zhrnutie demonštrácie činnosti:

Útok sa dá predpokladať za úspešný, keďže je zjavne vidno, že klientovi (obeti č. 1) bolo zamedzené získanie IP adresy od autorizovaného DHCP servera na sieti a následne mu boli podsunuté informácieo konfigurácii sieti, ktoré si útoční zadal. Je pravda, že DHCP rogue server nie je úplne správne funkčný, z toho dôvodu, že niektoré podsunuté informácie sú natvrdo dané v kóde, avšak podstatu a princím DHCP rogue serveru spĺňa.

6. Návod na použitie

DHCP starve obsahuje súbory na DHCP starvation útok. Po preložení sa program sa spúšťa pomocou príkazu:

- `./pds-dhcpstarve -h`
- `./pds-dhcpstarve -i interface`

Kde argument `-i interface` znamená meno rozhrania podľa OS, na ktoré útočník vygeneruje príslušnú prevádzku s kompromitujúcimi účinkami na DHCP server.
Príklad: `./pds-dhcpstarve -i eth1`

DHCP rogue obsahuje súbory na vytvorenie rogue DHCP serveru. Po preložení sa program sa spúšťa pomocou príkazu:

- `./pds-dhcprogue -h`
- `./pds-dhcprogue -i interface -p pool -g gateway -n dns-server -d domain -l lease-time`
- Kde argument
- `-i interface` znamená meno rozhrania podľa OS, na ktoré útočník vygeneruje príslušnú prevádzku s kompromitujúcimi účinkami na DHCP server;
- `-p pool` znamená pool adries reprezentovaný vo formáte <prvá_IPv4_adresa>-<posledná_IPv4_adresa> (napr. 192.168.1.100-192.168.1.199);
- `-g gateway` znamená IPv4 adresa sieťovej brány pre segment, v ktorom sa nachádza obeť;
- `-n dns-server` znamená IPv4 adresa DNS serveru;
- `-d domain` znamená meno domény, v ktorej sa zariadenie nachádza;
- `-l lease-time` znamená počet sekúnd reprezentujúci dobu DHCP pôžičky;

Príklad: `./pds-dhcprogue -i eth1 -p 192.168.1.100-192.168.1.199 -g 192.168.1.1 -n 8.8.8.8 -d fit.vutbr.cz -l 3600`

Súbor `Makefile` slúži na preloženie oboch častí, teda stačí príkaz `make`.

7. Záver

V tomto projekte sa mi úspešne podarilo implementovať a odskúšať DHCP Starvation útok. DHCP rogue server som bohužiaľ nestihol úplne dokončiť, preto je jeho funkcionalita obmedzená.

8. Literatúra

[1] R. Droms. *Dynamic Host Configuration Protocol.* URL: http://www.rfc-editor.org/info/rfc2131

[2] *DHCP Message Format.* URL: http://www.tcpipguide.com/free/t_DHCPMessageFormat.htm

[3] Lucideus Research. *DHCP Starvation Attack with DHCP Rogue Server.* URL: https://lucideustech.blogspot.cz/2018/01/dhcp-starvation-attack-with-dhcp-rogue.html

[4] Ezra Undag. *Attack a network by using a rogue DHCP server*. URL: https://medium.com/tech-jobs-academy/attack-a-network-by-using-a-rogue-dhcp-server-8c8acea315ab