VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

Dokumentácia k projektu do predmetu IPK

DHCP Starvation útok

9. apríla 2018

Vladimír Marcin xmarci10

Obsah

1 Cieľ projektu **2**

2 DHCP starvation **2**

3 Implementácia **3**

4 Demonštrácia funkčnosti **3**

1 Cieľ projektu

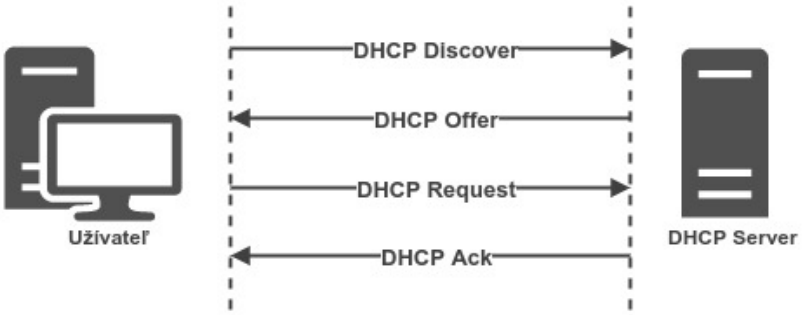
Cieľom projektu bolo naštudovanie problematiky DHCP útokov a následne naprogramovať aplikáciu realizujúcu DHCP Starvation útok, ktorý pomocou DHCP Discover správ vyčerpá adresný pool legitímneho DHCP serveru.

2 DHCP starvation

DHCP (Dynamic Host Configuration Protocol) je protokol aplikačnej vrstvy TCP/IP modelu, ktorý slúži na dynamické prideľovanie sieťových parametrov. Sú to IP adresa, maska, implicitná brána apod. DHCP funguje na báze klient–server. K svojej funkcii využíva transportný protokol UDP. DHCP definuje štyri základné typy správ:

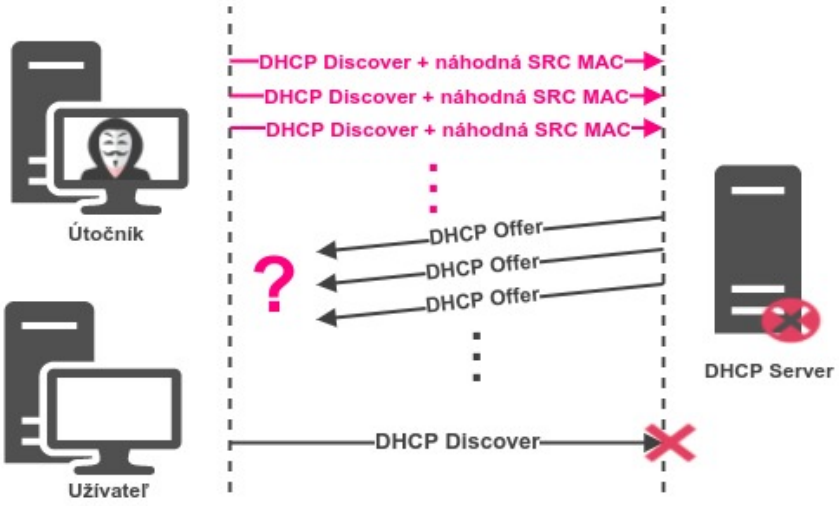
- DHCP Discover
- DHCP Offer
- DHCP Request
- DHCP Ack

Po pripojení do siete klient pošle správu DHCP discover ako broadcast. Touto správou nájde dostupné DHCP servery a informuje ich o jeho prítomnosti. Pokiaľ sa v tejto sieti nachádza DHCP server, odpovedá na túto správu paketom DHCP offer, čo predstavuje ponuku sieťových parametrov. Klient pokračuje v komunikácii odoslaním správy DHCP request, čím si vyžiada ponúkané parametre. Pokiaľ klient obdrží správu DHCP offer od viacerých klientov (v sieti je viac DHCP serverov), DHCP request odošle tomu, ktorý odpovedal ako prvý. Server následne potvrdzuje pridelenie správou DHCP ack [2].



Obr. 1: Základná DHCP komunikácia

DHCP starvation útok spočíva v snahe útočníka o vyčerpanie všetkých prideliteľných IP adries, ktoré ponúka DHCP server. Útočník to dosiahne intenzívnym tokom správ DHCP discover, ktoré obsahujú náhodne generované MAC adresy. DHCP server pri bežnom nastavení nie je schopný rozlíšiť, či sa jedná o legitímne alebo fiktívne žiadosti a preto sa snaží na každú vyhovieť odoslaním správy DHCP offer. Na vyčerpanie prideliteľných IP adries nemusí prebehnúť celý proces DHCP komunikácie (Obr. 1). DHCP server už po odoslaní správy DHCP offer danú IP adresu vypustí zo zoznamu prideliteľných adries po dobu ukončenia procesu DHCP komunikácie alebo po predom stanovený čas (timeout). Pokiaľ útočník pošle dostatočný počet DHCP discover správ, priestor prideliteľných adries DHCP servera bude v krátokom čase vyčerpaný. Tým, že DHCP server musí každú žiadosť jednotlivo spracovať s následným odpovedaním na ňu, znamená ďalší dôsledok útoku – vyčerpanie jeho systémových zdrojov ako CPU, vyrovnávacie pamäte apod. Na základe vyššie uvedených úkonov nastáva požadované odoprenie služby



Obr. 2: DHCP starvation útok

3 Implementácia

Aplikácia bola napísaná v jazyku C. Implementácia je rozdelená do týchto modulov:

- `libs.h` - hlavičkové súbory, zdieľané naprieč všetkými modulmi
- `dhcp.h` - štruktúra dhcp správy zo štandardu RFC2131 a jej inicializácia (DHCP Discover)
- `msg.h` - vytvorenie udp packetu a následne odoslanie packetu
- `packet_headers.h` - vytvorenie a inicializácia hlavičiek paketu

Implementácia spočíva vo vytvorení a inicializácii DHCP Discover správy pomocou Ethernet raw packetov[1]. Formát DHCP Discover správy je popísaný tu [2]. Následne je táto správa posielaná v nekonečnom cykle až do ukončenia aplikácie pomocou signálu SIGINT (Ctrl+C).

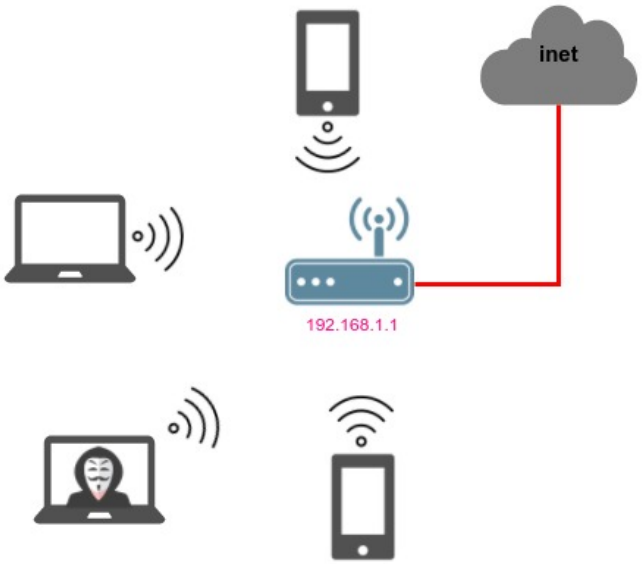
V každej DHCP Discover správe sa generuje nová MAC adresa pomocou funkcie `generate_mac` z modulu `msg.c`, ktorá má predstavovať MAC adresu užívateľa žiadajúceho o pridelenie IP adresy.

4 Demonštrácia funkčnosti

Spustenie aplikácie: **`./ipk-dhcpstarve -i wlan0`**

Obr. 3: Nastavenie DHCP

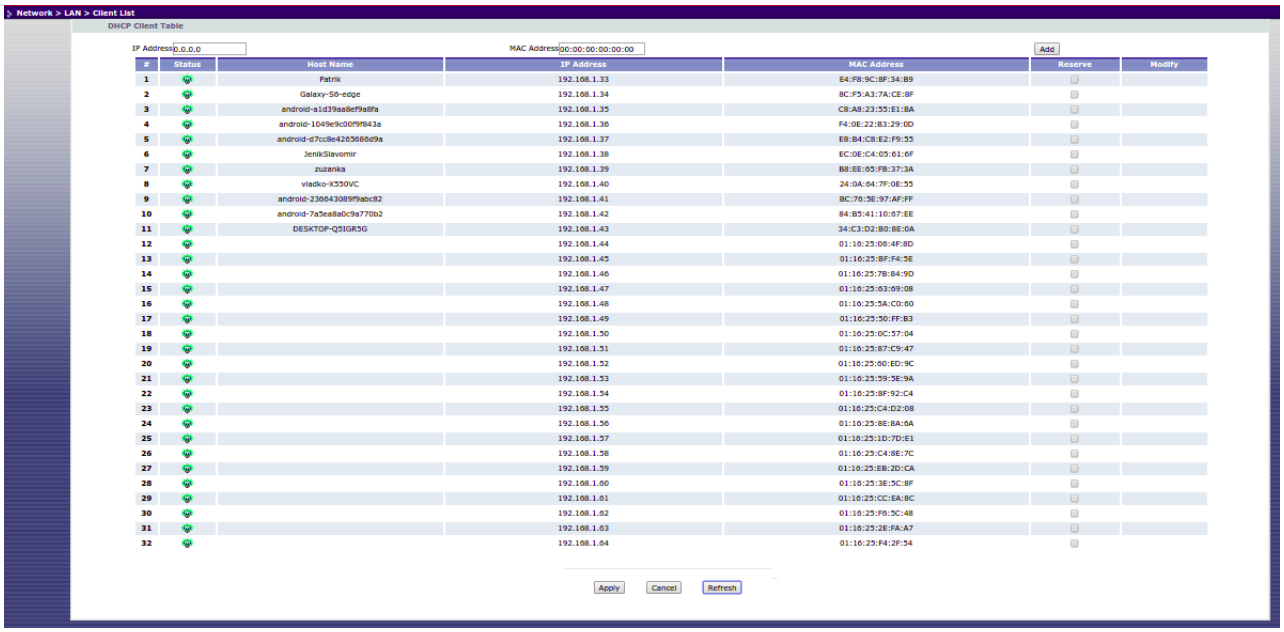
Testovaná topológia pozostáva z wifi zariadení (notebooky, smartphony). Ide o domácu LAN sieť. Konfiguráciu DHCP je možné vidieť na obrázku Obr. 3. V danej sieti môže byť adresa pridelená 32 zariadeniam.



Obr. 4: Topológia testovanej siete

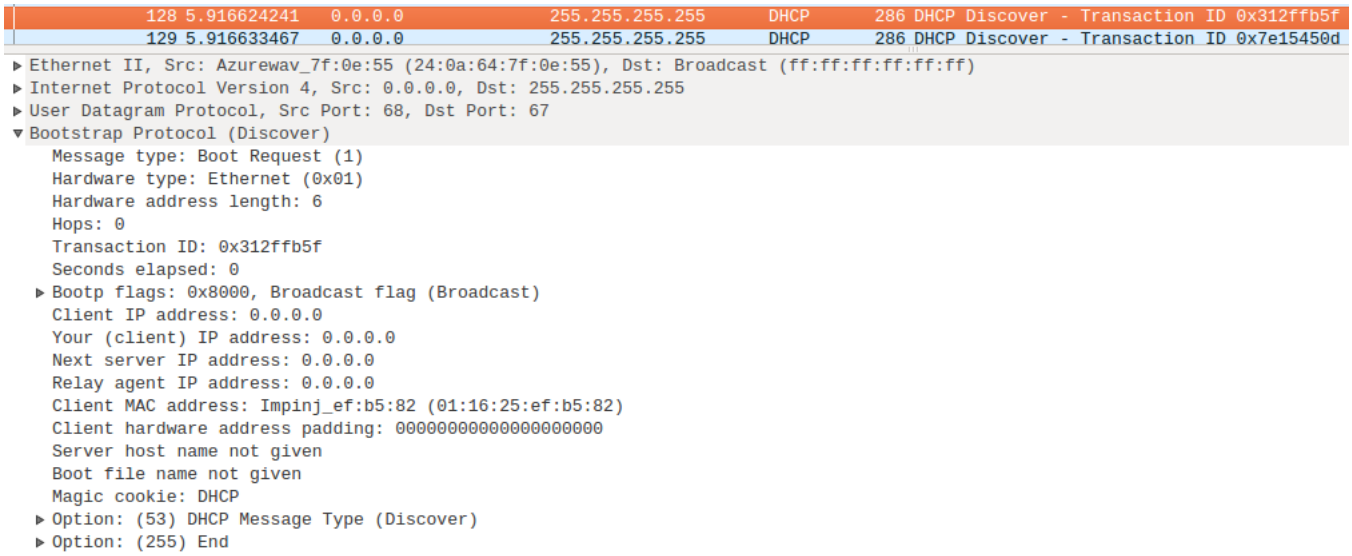
Po spustení aplikácie si môžme v zozname vypožičaných adries (Obr. 6) všimnúť adresy, ktoré sú vyčerpané našou aplikáciou (ide o adresy kde sa MAC adresa zariadenia kvôli demonštrácii začína prefixom "01:16:25").

Z nastavenia DHCP (Obr. 3) si taktiež vieme spočítať že bol vyčerpaný celý adresný pool.



Obr. 5: Zoznam vypožičaných IP adries na testovanom AP

Na obrázku nižšie ešte naviac demonštrujeme výstup z programu Wiresharku po spustení aplikácie. Z výstupu môžme vidieť, že packet, ktorý poslala aplikácia je správne vyplnený keďže ho Wireshark identifikoval ako DHCP Discover správu.



Obr. 6: Výstup wireshark

Literatúra

[1] blog, A.: Sending raw Ethernet packets from a specific interface in C on Linux. online, 2014.
URL https://austinmarton.wordpress.com/2011/09/14/sending-raw-ethernet-packets-from-a-specific-interface-in-c-on-linux/

[2] Netmanias: Understaning the Basic Operations of DHCP. online, 2013.
URL https://www.netmanias.com/en/?m=view&id=techdocs&no=5998&xtag=dhcp-network-protocol&xref=understanding-the-basic-operations-of-dhcp&vm=pdf