

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ



Dokumentácia k projektu do predmetu IPK

DHCP Starvation útok

9. apríla 2018

Obsah

1	Cieľ projektu	2
2	DHCP starvation	2
3	Implementácia	3
4	Demonštrácia funkčnosti	3

1 Cieľ projektu

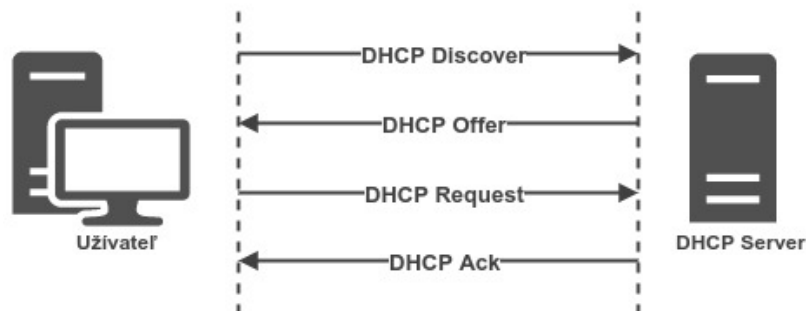
Cieľom projektu bolo naštudovanie problematiky DHCP útokov a následne naprogramovať aplikáciu realizujúcu DHCP Starvation útok, ktorý pomocou DHCP Discover správ vyčerpá adresný pool legitímneho DHCP serveru.

2 DHCP starvation

DHCP (Dynamic Host Configuration Protocol) je protokol aplikačnej vrstvy TCP/IP modelu, ktorý slúži na dynamické pridelenie 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:

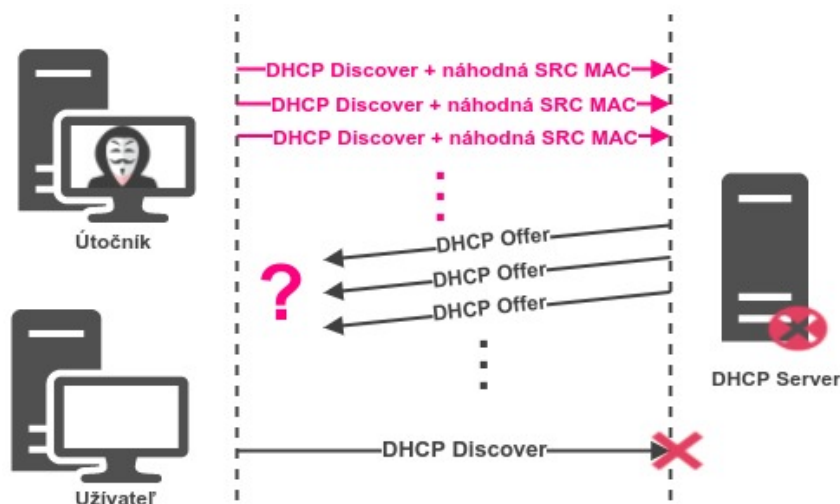
- DHCP Discover
- DHCP Offer
- DHCP Request
- DHCP Ack

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 krátkom čase vyčerpaný. Tým, že DHCP server musí každú žiadosť jednotlivito 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 packetu

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.

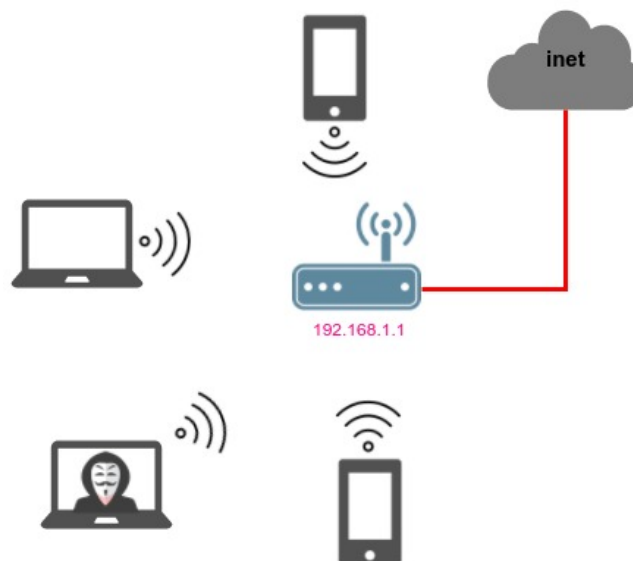
4 Demonštrácia funkčnosti

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

DHCP Setup	
DHCP	Server ▼
IP Pool Starting Address	192.168.1.33
Pool Size	32
Remote DHCP Server	0.0.0.0

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 môžeme 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.

Network > LAN > Client List

DHCP Client Table

IP Address: 0.0.0.0 MAC Address: 00:00:00:00:00:00

#	Status	Host Name	IP Address	MAC Address	Reserve	Modify
1	✓	Patrik	192.168.1.33	E4:F8:9C:8F:34:B9	<input type="checkbox"/>	
2	✓	Galaxy-S0-edge	192.168.1.34	BC:F3:A3:7A:CE:BF	<input type="checkbox"/>	
3	✓	android-a1d39a8e998f8a	192.168.1.35	C8:A8:23:25:E1:BA	<input type="checkbox"/>	
4	✓	android-1049e9c009843a	192.168.1.36	F4:0E:22:83:29:00	<input type="checkbox"/>	
5	✓	android-d7c28e420508d9e	192.168.1.37	E8:84:C8:E2:F9:35	<input type="checkbox"/>	
6	✓	JenikSlavomir	192.168.1.38	EC:0E:C4:05:01:0F	<input type="checkbox"/>	
7	✓	zuzanka	192.168.1.39	88:EE:65:78:37:3A	<input type="checkbox"/>	
8	✓	viadko-K550VC	192.168.1.40	24:0A:04:7F:06:35	<input type="checkbox"/>	
9	✓	android-239643089f9ebc82	192.168.1.41	BC:79:5E:97:AF:FF	<input type="checkbox"/>	
10	✓	android-7a5ea8dc9a770b2	192.168.1.42	84:85:41:10:07:EE	<input type="checkbox"/>	
11	✓	DESKTOP-Q3IGK5G	192.168.1.43	34:C3:D2:80:8E:0A	<input type="checkbox"/>	
12	✓		192.168.1.44	01:16:25:08:4F:8D	<input type="checkbox"/>	
13	✓		192.168.1.45	01:16:25:8F:F4:5E	<input type="checkbox"/>	
14	✓		192.168.1.46	01:16:25:78:84:90	<input type="checkbox"/>	
15	✓		192.168.1.47	01:16:25:03:09:08	<input type="checkbox"/>	
16	✓		192.168.1.48	01:16:25:5A:C0:00	<input type="checkbox"/>	
17	✓		192.168.1.49	01:16:25:30:FF:B3	<input type="checkbox"/>	
18	✓		192.168.1.50	01:16:25:0C:37:04	<input type="checkbox"/>	
19	✓		192.168.1.51	01:16:25:87:C9:47	<input type="checkbox"/>	
20	✓		192.168.1.52	01:16:25:00:ED:9C	<input type="checkbox"/>	
21	✓		192.168.1.53	01:16:25:39:36:9A	<input type="checkbox"/>	
22	✓		192.168.1.54	01:16:25:8F:52:C4	<input type="checkbox"/>	
23	✓		192.168.1.55	01:16:25:C4:02:08	<input type="checkbox"/>	
24	✓		192.168.1.56	01:16:25:8E:8A:0A	<input type="checkbox"/>	
25	✓		192.168.1.57	01:16:25:1D:7D:E1	<input type="checkbox"/>	
26	✓		192.168.1.58	01:16:25:C4:8E:7C	<input type="checkbox"/>	
27	✓		192.168.1.59	01:16:25:E8:2D:CA	<input type="checkbox"/>	
28	✓		192.168.1.60	01:16:25:3E:3C:BF	<input type="checkbox"/>	
29	✓		192.168.1.61	01:16:25:CC:EA:BC	<input type="checkbox"/>	
30	✓		192.168.1.62	01:16:25:F6:3C:48	<input type="checkbox"/>	
31	✓		192.168.1.63	01:16:25:2E:FA:A7	<input type="checkbox"/>	
32	✓		192.168.1.64	01:16:25:F4:2F:54	<input type="checkbox"/>	

Apply Cancel Refresh

Obr. 5: Zoznam vypožičaných IP adries na testovanom AP

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

128	5.916624241	0.0.0.0	255.255.255.255	DHCP	286 DHCP Discover - Transaction ID 0x312ffb5f
129	5.916633467	0.0.0.0	255.255.255.255	DHCP	286 DHCP Discover - Transaction ID 0x7e15450d

▶ Ethernet II, Src: Azurewv_7f:0e:55 (24:0a:64:7f:0e:55), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 ▶ Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
 ▶ User Datagram Protocol, Src Port: 68, Dst Port: 67
 ▼ Bootstrap Protocol (Discover)
 Message type: Boot Request (1)
 Hardware type: Ethernet (0x01)
 Hardware address length: 6
 Hops: 0
 Transaction ID: 0x312ffb5f
 Seconds elapsed: 0
 ▶ Bootp flags: 0x8000, Broadcast flag (Broadcast)
 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: Impinj_ef:b5:82 (01:16:25:ef:b5:82)
 Client hardware address padding: 00000000000000000000
 Server host name not given
 Boot file name not given
 Magic cookie: DHCP
 ▶ Option: (53) DHCP Message Type (Discover)
 ▶ Option: (255) End

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`