

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA INFORMAČNÍCH TECHNOLOGIÍ



Počítačové komunikace a sítě – 2.projekt
DHCP Starvation útok

Varianta *II*

Obsah

1	Úvod	2
2	DHCP Protokol	2
2.1	DHCP Proces	2
3	DHCP Starvation útok	3
3.1	Princíp	3
3.2	Nadväzujúce útoky	3
4	Implementácia	4
4.1	DHCP Discover Message	4
4.2	Zaujímave časti implementácie	5
5	Demonštrácia DHCP útoku	6
6	Referencie	8

1 Úvod

Schopnosť a funkcionálnosť DHCP serveru je jednou z mála vecí, ktorú považujeme za samozrejmosť každý deň. V každom routeri sa skrýva pre mnohých neznáma, funkcia DHCP, ktorá zaisťuje funkčnosť vašej domácej či firemnej siete. Dokumentácia k projektu popisuje DHCP protokol v skratke, princíp a implementáciu DHCP Starvation útoku v jazyku C a následnú demonštráciu funkčnosti v sieti.

2 DHCP Protokol

DHCP (Dynamic Host Configuration Protocol) je sieťový protokol, ktorý automaticky prideliť IP adresu, masku podsiete (Subnet Mask), predvolenú bránu (Default Gateway, primárny a sekundárny DNS server a ďalšie konfiguračné parametre siete každému zariadeniu v sieti, tak aby mohli komunikovať s ostatnými zariadeniami v sieti. DHCP server udržiava zdieľaný rozsah IP adries, tzv. adresný pool a prepožičiava IP adresu každému DHCP klientovi ktorý je v sieti, po jeho zapnutí.

2.1 DHCP Proces

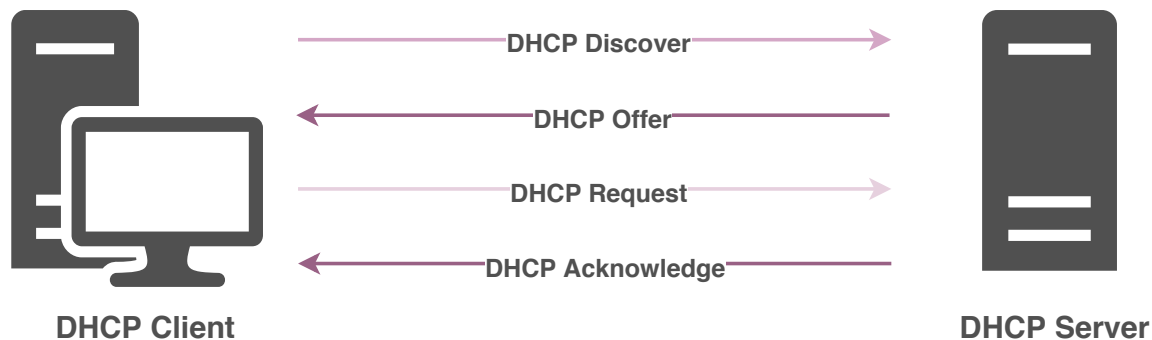
Komunikácia medzi klientom a serverom prebieha na porte 68 - klient (zariadenie, ktoré žiada o pridelenie konfiguračných parametrov) a na porte 67 - server (port na ktorom načúva DHCP server).

Užívateľ spustí počítač, ktorý reprezentuje DHCP klienta. Klientský počítač požiada server o pridelenie IP adresy, tým že pošle broadcast request správu, nazývanú **DHCP Discover Message**, všetkým serverom v sieti, a počká na odpoveď od DHCP servera.

DHCP server obdrží Discover paket a na základe dostupnosti a podmienok pridelenia IP adresy na serveri, server určí vhodnú adresu pre klienta. Server následne dočasne rezervuje IP adresu pre klienta a pošle unicast packet na MAC adresu klienta vo forme **DHCP Offer Message** správy, ktorá obsahuje ponúkanú IP adresu, masku podsiete a ďalšie konfiguračné parametre.

DHCP klient následne pošle broadcast paket vo forme **DHCP Request Message** správy, čím si vyžiada IP adresu, ktorú vybral server na používanie.

Server pošle unicast paket vo forme **DHCP Acknowledge Message** správy, čím potvrdí, že daná IP adresa bola vypožičaná pre klienta na dobu špecifikovanú serverom.

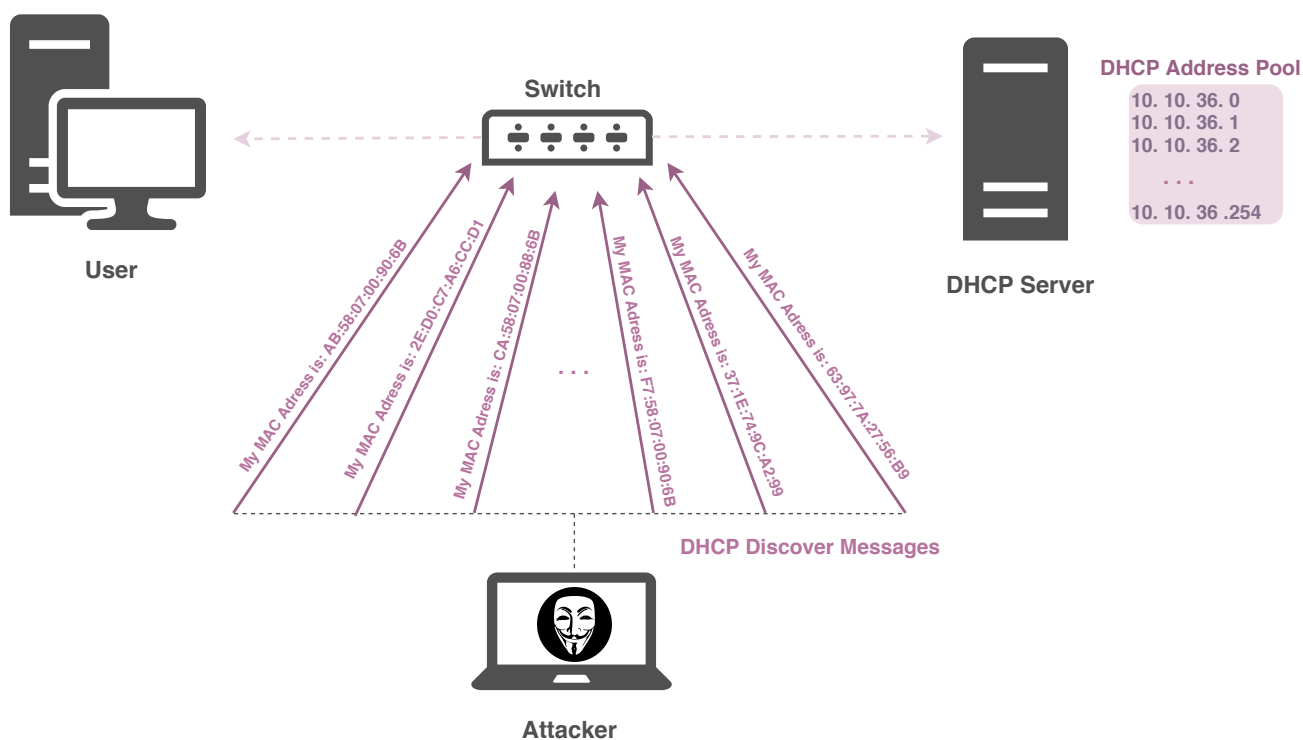


3 DHCP Starvation útok

3.1 Princíp

DHCP Starvation útok je útok v sieti, kedy útočník posiela nadmerný počet broadcast správ tzv. **DHCP Discover Message** správ s falošnými MAC adresami. Ak začne legitímny server v sieti odpovedať na všetky tieto Discover Messages, všetky dostupné IP adresy v adresovom poole tohto DHCP servera budú vyčerpané vo veľmi krátkom čase. Pri tomto útoku môžu byť oprávneným používateľom siete odopreté serverové služby.

Po vyčerpaní všetkých možných adries z adresového poolu, sieťový útočník môže založiť tzv. **Rogue DHCP Server** a následne odpovedať na nové DHCP Request Messages od DHCP klientov v sieti. [2]



3.2 Nadväzujúce útoky

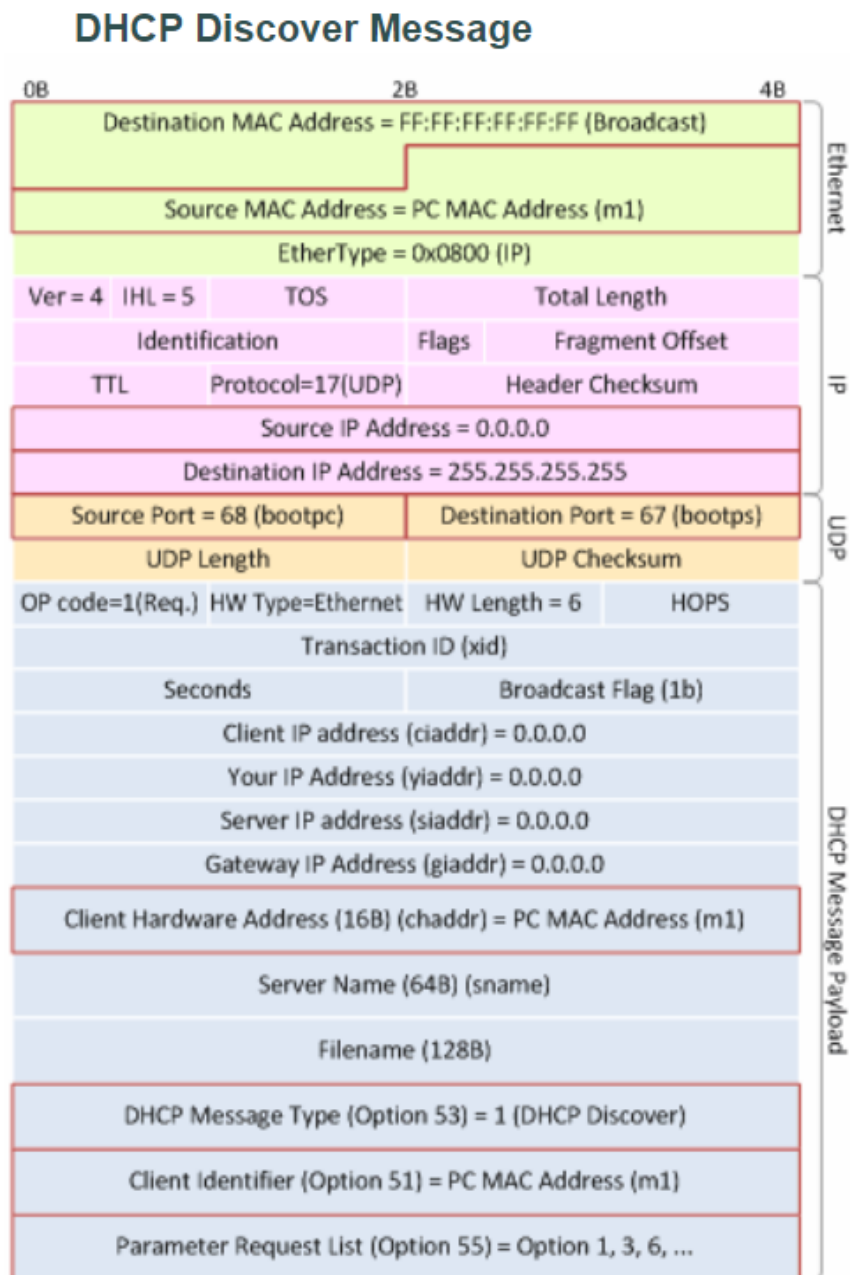
Uskutočnením DHCP Starvation útoku, vyčerpaním adresového poolu legitímneho servera a založením Rogue DHCP servera môže útočník následne uskutočniť **DHCP Spoofing útok**. Útočník môže začať distribuovať IP adresy a ďalšie konfiguračné parametre, DHCP klientom. Útočník v sieti teraz môže nahradiť originálnu legitímnu IP adresu predvolenej brány (Default Gateway) a IP adresu DNS servera na svoju vlastnú IP adresu. Klient začne posilať pakety po sieti a útočník dokáže odchytať osobné užívateľské dáta a spustiť útok *man-in-the-middle*. Útočník taktiež môže založiť Rogue DHCP Server a presmerovať koncového užívateľa na falošné webové stránky a prípadne spustiť útoky typu *phishing*. [3]

4 Implementácia

Posielanie DHCP Discover správ je realizované cez RAW socket. Bolo nutné naplniť štruktúru DHCP Discover Message. Všeobecne známe informácie ako čísla komunikačných portov pre DHCP klienta a DHCP server v UDP hlavičke 67 a 68 a pod. [4]

4.1 DHCP Discover Message

Spomenutý DHCP Starvation útok používa na vyčerpanie adresového poolu DHCP Discover Messages. Ich formát vyzerá nasledovne: [1]



4.2 Zaujímave časti implementácie

```
/* Prototypes */
//Creates ETHERNET header
int create_ether_header();

//Creates IP header
struct iphdr * create_ip_header();

//Creates UDP header
struct udphdr * create_udp_header();

//Creates Discover Message Payload
dhcp_packet * create_dhcp_msg_payload(unsigned char *client_mac_addr);
```

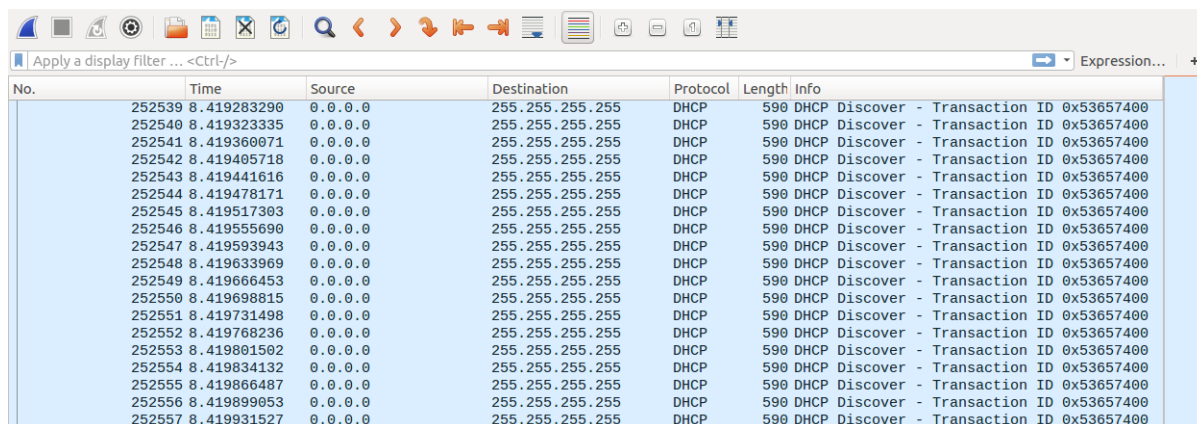
Vyššie spomenuté funkcie realizujú vytvorenie DHCP Discover Message v príslušnom formáte. Následne `char buffer[1024]` reprezentuje štruktúru DHCP Discover Message s príslušnými hlavičkami Ethernet, IP, UDP a Message Payload.

```
/* Function that generates MAC Address*/
unsigned char * generate_mac_address(unsigned char *client_mac_addr);
```

Dôležitá funkcia, ktorá náhodne vytvorí MAC adresu, ktorou simuluje rôznych klientov, ktorí posielajú DHCP Discover Messages, aby sa vyčerpali adresový pool DHCP servera.

5 Demonštrácia DHCP útoku

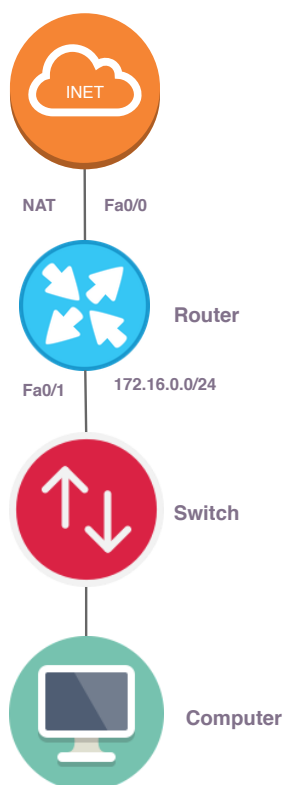
Zasielanie DHCP Discover Messages v cykle. Demonštruje zahlcovanie DHCP Servera DHCP Discover správami. Kontrola zasielania paketov v programe Wireshark.



The image shows a Wireshark packet capture window. The top toolbar includes icons for file operations, network analysis, and display filters. Below the toolbar, a display filter is set to 'Expression...'. The main packet list table shows a series of DHCP Discover packets. Each packet has a number, time, source IP (0.0.0.0), destination IP (255.255.255.255), protocol (DHCP), length (590), and info (DHCP Discover - Transaction ID 0x53657400). The packets are numbered from 252539 to 252557, with times ranging from 8.419283290 to 8.419931527.

No.	Time	Source	Destination	Protocol	Length	Info
252539	8.419283290	0.0.0.0	255.255.255.255	DHCP	590	DHCP Discover - Transaction ID 0x53657400
252540	8.419323335	0.0.0.0	255.255.255.255	DHCP	590	DHCP Discover - Transaction ID 0x53657400
252541	8.419360071	0.0.0.0	255.255.255.255	DHCP	590	DHCP Discover - Transaction ID 0x53657400
252542	8.419405718	0.0.0.0	255.255.255.255	DHCP	590	DHCP Discover - Transaction ID 0x53657400
252543	8.419441616	0.0.0.0	255.255.255.255	DHCP	590	DHCP Discover - Transaction ID 0x53657400
252544	8.419478171	0.0.0.0	255.255.255.255	DHCP	590	DHCP Discover - Transaction ID 0x53657400
252545	8.419517303	0.0.0.0	255.255.255.255	DHCP	590	DHCP Discover - Transaction ID 0x53657400
252546	8.419555690	0.0.0.0	255.255.255.255	DHCP	590	DHCP Discover - Transaction ID 0x53657400
252547	8.419593943	0.0.0.0	255.255.255.255	DHCP	590	DHCP Discover - Transaction ID 0x53657400
252548	8.419633969	0.0.0.0	255.255.255.255	DHCP	590	DHCP Discover - Transaction ID 0x53657400
252549	8.419666453	0.0.0.0	255.255.255.255	DHCP	590	DHCP Discover - Transaction ID 0x53657400
252550	8.419698815	0.0.0.0	255.255.255.255	DHCP	590	DHCP Discover - Transaction ID 0x53657400
252551	8.419731498	0.0.0.0	255.255.255.255	DHCP	590	DHCP Discover - Transaction ID 0x53657400
252552	8.419768236	0.0.0.0	255.255.255.255	DHCP	590	DHCP Discover - Transaction ID 0x53657400
252553	8.419801502	0.0.0.0	255.255.255.255	DHCP	590	DHCP Discover - Transaction ID 0x53657400
252554	8.419834132	0.0.0.0	255.255.255.255	DHCP	590	DHCP Discover - Transaction ID 0x53657400
252555	8.419866487	0.0.0.0	255.255.255.255	DHCP	590	DHCP Discover - Transaction ID 0x53657400
252556	8.419899053	0.0.0.0	255.255.255.255	DHCP	590	DHCP Discover - Transaction ID 0x53657400
252557	8.419931527	0.0.0.0	255.255.255.255	DHCP	590	DHCP Discover - Transaction ID 0x53657400

Demonštrácia projektu prebehla na nasledujúcej fyzickej topológii, ktorá overila jej funkčnosť. Vyčerpanie adresového poolu legítimneho DHCP servera bolo úspešné.



Demonštrácia vyčerpania adresného poolu na topológii. Demo screenshot.

172.16.0.221	8714.bd41.ef56	Apr 06 2018 12:30 PM	Automatic
172.16.0.222	c028.75a7.69ae	Apr 06 2018 12:30 PM	Automatic
172.16.0.223	2b28.a2e7.2496	Apr 06 2018 12:30 PM	Automatic
172.16.0.224	9b59.69fa.e11e	Apr 06 2018 12:30 PM	Automatic
172.16.0.225	c563.0d90.d625	Apr 06 2018 12:30 PM	Automatic
172.16.0.226	cc5d.398a.9f29	Apr 06 2018 12:30 PM	Automatic
172.16.0.227	e05f.5156.06bb	Apr 06 2018 12:30 PM	Automatic
172.16.0.228	0431.e3a7.1908	Apr 06 2018 12:30 PM	Automatic
172.16.0.229	3db4.61a6.af42	Apr 06 2018 12:30 PM	Automatic
172.16.0.230	c474.a5d1.047b	Apr 06 2018 12:30 PM	Automatic
172.16.0.231	f6d0.d92f.5a78	Apr 06 2018 12:30 PM	Automatic
172.16.0.232	583b.d7aa.91dd	Apr 06 2018 12:30 PM	Automatic
172.16.0.233	6595.0e48.3c27	Apr 06 2018 12:30 PM	Automatic
172.16.0.234	5079.dcb2.1f8b	Apr 06 2018 12:30 PM	Automatic
172.16.0.235	f4e3.ff9a.b403	Apr 06 2018 12:30 PM	Automatic
172.16.0.236	15aa.d3ee.da2e	Apr 06 2018 12:30 PM	Automatic
172.16.0.237	6632.693d.dcfa	Apr 06 2018 12:30 PM	Automatic
172.16.0.238	1a41.8f29.8acc	Apr 06 2018 12:30 PM	Automatic
172.16.0.239	50da.452c.8c65	Apr 06 2018 12:30 PM	Automatic
172.16.0.240	b781.48b6.1bfd	Apr 06 2018 12:30 PM	Automatic
172.16.0.241	b930.a78d.1f81	Apr 06 2018 12:30 PM	Automatic
172.16.0.242	bb85.b424.c390	Apr 06 2018 12:30 PM	Automatic
172.16.0.243	1edd.d2ad.065c	Apr 06 2018 12:30 PM	Automatic
172.16.0.244	7957.36bf.83c3	Apr 06 2018 12:30 PM	Automatic
172.16.0.245	243b.446c.f15f	Apr 06 2018 12:30 PM	Automatic
172.16.0.246	69ab.8f11.38ae	Apr 06 2018 12:30 PM	Automatic
172.16.0.247	92f3.3446.17f7	Apr 06 2018 12:30 PM	Automatic
172.16.0.248	d735.d4a9.e2db	Apr 06 2018 12:30 PM	Automatic
172.16.0.249	055c.323b.1bb5	Apr 06 2018 12:30 PM	Automatic
172.16.0.250	fe3f.f042.abe2	Apr 06 2018 12:30 PM	Automatic
172.16.0.251	a115.8d31.26c5	Apr 06 2018 12:30 PM	Automatic
172.16.0.252	dfb8.b813.ffc6	Apr 06 2018 12:30 PM	Automatic
172.16.0.253	0ad6.04df.7fe6	Apr 06 2018 12:30 PM	Automatic
172.16.0.254	ba84.42ec.bf5d	Apr 06 2018 12:30 PM	Automatic
Router#			

6 Referencie

- [1] Netmanias *Understanding the Basic Operations of DHCP* [online]. 2018-04-09 Dostupné na: https://www.netmanias.com/en/post/techdocs/5998/dhcp-network-protocol/understanding-the-basic-operations-of-dhcp#_ftn1
- [2] *Rogue DHCP Server* [online]. 2018-04-09 . Dostupné na: https://en.wikipedia.org/wiki/Rogue_DHCP
- [3] *DHCP Starvation attacks and DHCP spoofing attacks* [online].[cit. 2018-04-09]. Dostupné na: <http://www.omnisecu.com/ccna-security/dhcp-starvation-attacks-and-dhcp-spoofing-attacks.php>
- [4] *Sending raw Ethernet packets from a specific interface in C on Linux* [online].[cit. 2018-04-09]. Dostupné na: <https://austinmarton.wordpress.com/2011/09/14/sending-raw-ethernet-packets-from-a-specific-interface-in-c-on-linux/>