

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

IPK - 2. projekt

Varianta 2: DHCP Starvation útok

9. dubna 2018

Adam Venger

Obsah

| | | |
|----------|-------------------------|----------|
| 1 | DHCP | 2 |
| 2 | DHCP starvation | 3 |
| 3 | Implementácia | 4 |
| 3.1 | Štruktúra | 5 |
| 3.2 | Špecifiká | 5 |
| 3.3 | Nedostatky | 5 |
| 4 | Demonštrácia | 6 |
| 4.1 | Topológia | 6 |
| 4.2 | Priebeh testu | 6 |
| 4.3 | Výsledky | 7 |

1 DHCP

[1] **Dynamic Host Configuration Protocol** poskytuje konfiguračné parametre pre konfiguráciu klientov v sieti. Jeho úlohou je dynamicky priradiť IP adresy zariadeniam, ktoré o to požiadajú.

Cieľom jeho vytvorenia bolo, aby klient nevyžadoval manuálnu konfiguráciu pre pripojenie k sieti a aby sieť nevyžadovala manuálnu konfiguráciu pre pripojenie klienta.

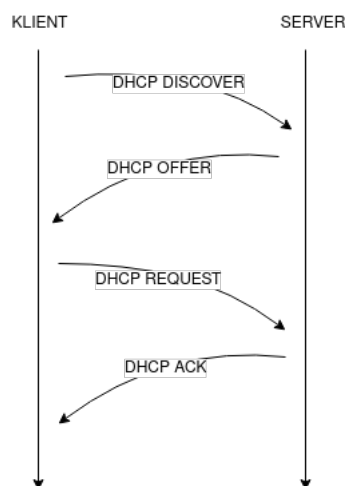
DHCP garantuje že špecifická IP adresa nebude využívaná viacerými zariadeniami v sieti v rovnakom čase.

DHCP podporuje 3 mechanizmi pre alokáciu IP adres.

- Automatická - DHCP priradí klientovi IP adresu permanentne
- Dynamická - DHCP priradzuje klientovi IP adresu len dočasne
- Manuálna - IP adresa je klientovi priradená administrátorom a DHCP ju doručí klientovi.

DHCP starvation útok využíva slabiny dynamickej alokácie.

Bežné pridelenie IP adresy vyzerá nasledovne.



1. Klient zašle broadcastom `DHCP DISCOVER` správu v ktorej je jeho MAC adresa, a náhodne vygenerované číslo transakcie, ktoré ju identifikuje
2. Server (alebo viacero serverov) zašle `DHCP OFFER` v ktorej je voľná, ponúkaná IP adresa
3. Klient potvrdí výber adresy pomocou správy `DHCP REQUEST`
4. Server potvrdí pridelenie adresy pomocou správy `DHCP ACK`

2 DHCP starvation

[2] Princíp útoku spočíva vo vyčerpaní adresného priestoru pridelovaného DHCP serverom. Tento DHCP server prideli všetky IP adresy zo svojho IP poolu falošným zariadeniam ktoré vytvára útočník. Využíva sa na zamedzenie prístupu k sieti, alebo ako prvý krok k „Man in the middle“ útoku.

Existuje viac spôsobov ako tento útok uskutočniť:

- Najjednoduchší je pomocou zasielania DHCP DISCOVER správ.
 - V správe uvedieme MAC adresu falošného zariadenia a DHCP server ponúkne IP adresu tomuto zariadeniu.
 - Je aj najmenej efektívnejší. Pretože sme požiadavku na IP adresu nepotvrdili, server rezervuje IP adresu vo väčšine prípadov maximálne na pár minút. Preto po skončení útoku efekt pretrvá len týchto pár minút.
 - Dá sa voči nemu aj ľahšie ubrániť vhodným nastavením DHCP serveru.
- Ďalší spôsob má viac krokov.
 1. Zasielanie DHCP DISCOVER správ
 2. Prijatie DHCP OFFER správy od serveru v ktorej je ponúkaná IP adresa
 3. Zaslanie DHCP REQUEST správy v ktorej potvrdíme požiadavku na konkrétnu IP adresu
 4. Prijatie DHCP ACK správy. V nej server potvrdzuje pridelenie IP adresy pre zariadenie.

Posledný krok nie je nutne dôležitý, túto správu čítať nemusíme.

Tento spôsob má viac výhod:

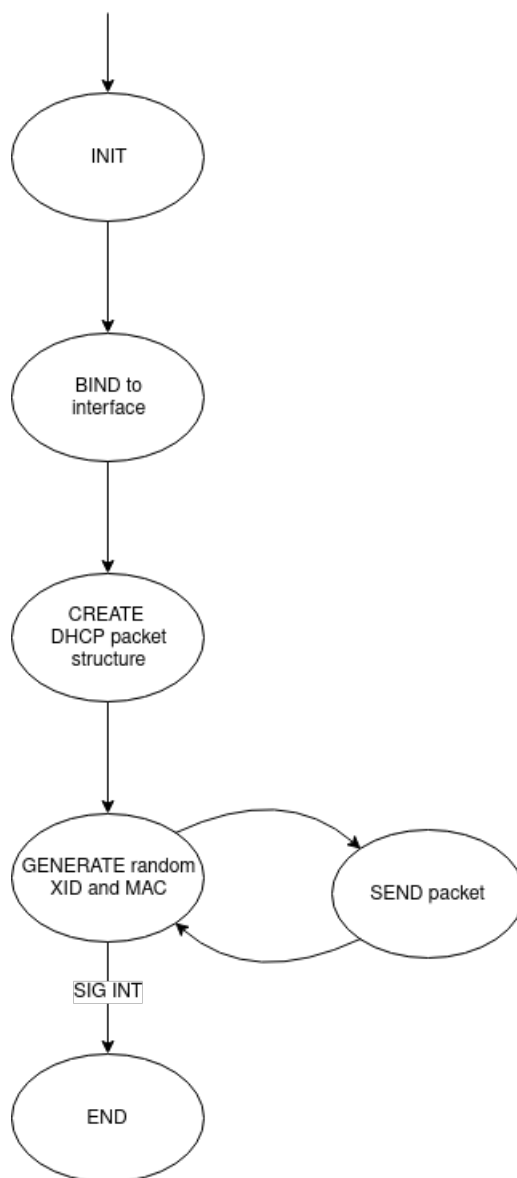
- Server nám prideli adresu na dlhší čas, typicky až na 24 hodín.
- Vyžiadanie adresy týmto spôsobom pre server vyzerá legitímne a je ťažšie sa voči nemu ochrániť.

3 Implementácia

[1]

V mojej implementácii využívam UDP socket, ktorý sa naviaže na rozhranie zadané ako parameter pri spustení.

Samotný útok prebieha tak, že v nekonečnom cykle zasielam DHCP DISCOVER packety, ktoré obsahujú náhodne generovanú MAC adresu.



3.1 Štruktúra

Keďže využívam UDP socket, IP adresa odosielateľa je viditeľná v IP hlavičke ako `Source`. Pre odstránenie tohto nedostatku je potrebné využívať RAW socket.

3.2 Špecifiká

Účinnosť útoku je závislá na konfigurácii DHCP serveru.

Program musí byť spúšťaný s root právami.

UDP socketu nastavujem `REUSE` flag. Dôvod je znovuspustiteľnosť programu bez toho aby som zatváral použitý socket.

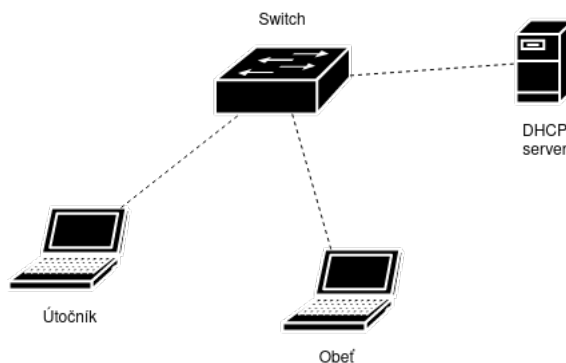
3.3 Nedostatky

Pri zasielaní len DHCP DISCOVER správ sa spolieham na to, že po tom čo DHCP server ponúkne IP adresu, tak ju na určitý čas rezervuje a nebude ju ponúkať znova žiadnemu inému žiadateľovi.

4 Demonštrácia

Na testovanie som využíval virtualizačný nástroj VirtualBox.

4.1 Topológia



V sieti boli dve klientské zariadenia a jeden DHCP server. Prvé klientske zariadenie bol útočník, na ktorom bol spustený útok. Druhé klientske zariadenie bola obeť, ktorá sa snažila získať IP adresu

4.2 Priebeh testu

1. Spustil som DHCP server, ktorý bol na adrese 192.168.56.100.
2. Spustil som zariadenie, z ktorého bude prebiehať útok.
3. Na útočiacom zariadení bol spustený program ako `sudo ./ipk-dhcpstarvation -i enp0s8` po dobu asi 5 sekúnd a následne ukončený `Ctrl+C`.
4. Spustil som obeť a tá sa pokúsila neúspešne pripojiť.
5. Obeť skúsila znovu získať IP adresu pomocou `sudo dhclient`, toto bolo opäť neúspešné.

4.3 Výsledky

The image shows a Wireshark network traffic capture window. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains various icons for packet capture and analysis. The filter bar at the top shows the expression `bootp.option.type==53`. The packet list pane displays a table of captured packets:

| No. | Time | Source | Destination | Protocol | Length | Info |
|-------|---------------|----------------|-----------------|----------|--------|--------------------|
| 38068 | 39.313594378 | 192.168.56.101 | 255.255.255.255 | DHCP | 590 | DHCP Discover - Tr |
| 38071 | 39.313874781 | 192.168.56.101 | 255.255.255.255 | DHCP | 590 | DHCP Discover - Tr |
| 38073 | 39.314151416 | 192.168.56.101 | 255.255.255.255 | DHCP | 590 | DHCP Discover - Tr |
| 38076 | 39.314449408 | 192.168.56.101 | 255.255.255.255 | DHCP | 590 | DHCP Discover - Tr |
| 38077 | 39.314577929 | 192.168.56.101 | 255.255.255.255 | DHCP | 590 | DHCP Discover - Tr |
| 38079 | 39.314820775 | 192.168.56.101 | 255.255.255.255 | DHCP | 590 | DHCP Discover - Tr |
| 38087 | 72.540833935 | 0.0.0.0 | 255.255.255.255 | DHCP | 342 | DHCP Discover - Tr |
| 38088 | 75.310667785 | 0.0.0.0 | 255.255.255.255 | DHCP | 342 | DHCP Discover - Tr |
| 38089 | 80.362042784 | 0.0.0.0 | 255.255.255.255 | DHCP | 342 | DHCP Discover - Tr |
| 38090 | 90.639089769 | 0.0.0.0 | 255.255.255.255 | DHCP | 342 | DHCP Discover - Tr |
| 38092 | 102.999629958 | 0.0.0.0 | 255.255.255.255 | DHCP | 342 | DHCP Discover - Tr |
| 38103 | 105.457248540 | 0.0.0.0 | 255.255.255.255 | DHCP | 342 | DHCP Discover - Tr |

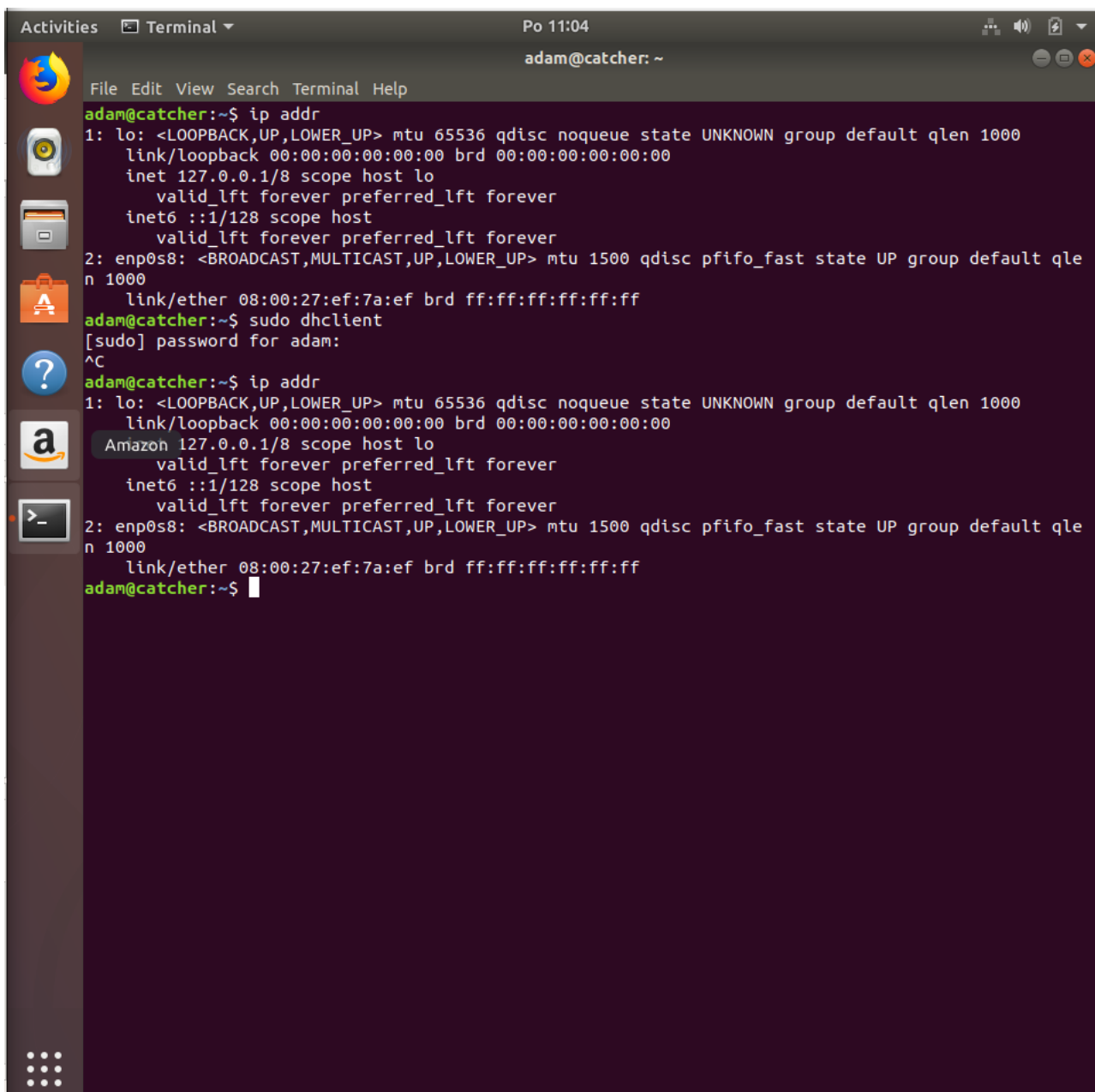
The packet details pane for the selected packet (No. 19) shows the following structure:

- Frame 19: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits) on interface 0
- Ethernet II, Src: PcsCompu_61:b8:f2 (08:00:27:61:b8:f2), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
- Internet Protocol Version 4, Src: 192.168.56.101, Dst: 255.255.255.255
- User Datagram Protocol, Src Port: 68, Dst Port: 67
- Bootstrap Protocol (Discover)

The packet bytes pane shows the raw data in hexadecimal and ASCII format. The ASCII column displays the string `'a....E..@...@...8e...D.C., .J....Ew..t....`.

The status bar at the bottom indicates: `wireshark_enp0s8_20180409110229_gBEB6D`, Packets: 38111 · Displayed: 15972 (41.9%), Profile: Default.

Na obrázku je vidieť DHCP DISCOVER packety, ktoré posielal útočník. Tie odchádzajú z IP adresy 192.168.56.101 a packety DHCP DISCOVER, smerujúce z adresy 0.0.0.0, ktoré odosiela obeť.



The screenshot shows a terminal window titled "adam@catcher: ~" with a menu bar (File, Edit, View, Search, Terminal, Help) and a status bar (Po 11:04). The terminal displays the following commands and output:

```
adam@catcher:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:ef:7a:ef brd ff:ff:ff:ff:ff:ff
adam@catcher:~$ sudo dhclient
[sudo] password for adam:
^C
adam@catcher:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:ef:7a:ef brd ff:ff:ff:ff:ff:ff
adam@catcher:~$
```

Obeť sa neúspešne pokúšala získať IP adresu.

Nastavenie DHCP serveru spôsobilo, že klient sa bol schopný pripojiť až po reštarte serveru.

Reference

- [1] R. Droms. Dynamic Host Configuration Protocol. RFC 2131.
- [2] Matej Šipkovský. DoS útok z vnútra siete na DHCP server.