# DHCP Útoky

Bc. Juraj Joščák
xjosca00

17.4.2018

## 1. Úvod

Cieľom projektu bolo naštudovať problematiku a realizovať vybrané DHCP útoky v prostredí reálnej alebo emulovanej siete. Konkrétne ide o tieto typy útokov:

- DHCP Starvation - Vyčerpanie adresného poolu legitímneho DHCP serveru
- DHCP Spoofing - Vytvorenie falošného DHCP serveru, ktorý bude klientom ponúkať podvrhnuté sieťové parametre.

Ako implementačný jazyk bol zvolený C++. Projekt bol napísaný testovaný primárne na operačnom systéme Linux. Terčom útoku bola sieť simulovaná pomocou nástroja VirtualBox.

## 2. Teória

### protokol DHCP

Protokol DHCP umožňuje automatickú konfiguráciu počítačov pripojených do siete. Používa sa hlavne na nastavenie IP adresy, masky podsiete, predvolenej brány a adresy DNS servera. DHCP systém sa skadá zo servera a niekoľkých klientov. Hlavné správy posielané pomocou DHCP sú:

**Discover** - pošle klient broadcastom po pripojení do siete. Oznamuje tým, že je v sieti nový a žiada ohlásenie serveru.

**Offer** - pošle server po prijatí Discover paketu. Oznamuje tým klientovi ktorá IP adresa z jeho adresného poolu je k dispozícii, svoju vlastnú IP adresu a iné informácie.

**Request** - touto správou klient žiada o pridelenie konkrétnej IP adresy. Môže ísť o adresu, o ktorej sa dozvedel z Offer paketu, alebo o adresu, ktorú už klient mal pridelenú, ale jej platnosť vypršala.

**ACK/NACK** - touto správou server schvaľuje/zamieta žiadosť klienta o pridelenie IP adresy. Po prijatí ACK je komunikácia medzi klientom a serverom ukončená, daná IP adresa definitívne prestáva byť k dispozícii v poole serveru (na určený čas) a klient môže túto adresu používať.

Existuje ešte niekoľko možných DHCP správ, povinné sú však len tieto štyri.

### DHCP starvation

Útok typu DHCP starvation spočíva vo vyčerpaní adresného poolu DHCP serveru. Každý ďalší klient pripojený do siete už teda nedostane žiadnu IP adresu.

Princíp spočíva v generovaní veľkého množstva DHCP-Request správ s podvrhnutými MAC adresami. Server teda vidí requesty z veľkého množstva zariadení, hoci v skutočnosti ide o jediné zariadenie útočníka.

### DHCP spoofing

Spoofing je závislý na úspešnom vykonaní starvation. Po vyčerpaní poolov všetkých legitímnych serverov sú tieto efektívne mimo prevádzku, nereagujú na Discover pakety nových klientov. To môže útočník využiť a vytvoriť vlastný, falošný DHCP server, ktorý bude klientom ponúkať vlastné sieťové parametre.

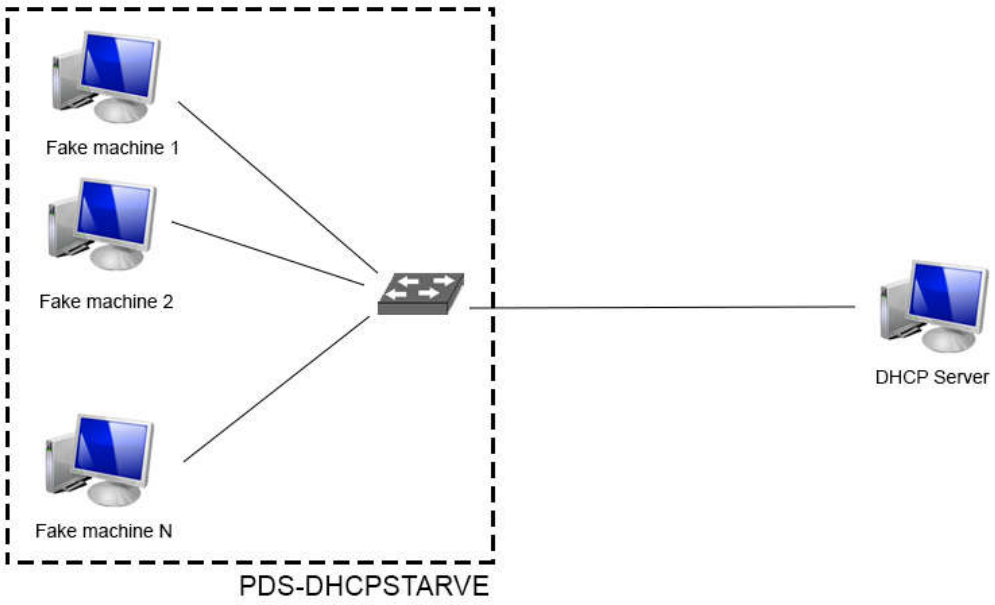
Užitočné je napríklad nastaviť IP adresu útočníka ako predvolenú bránu. Tak budú klienti odosielať útočníkovi všetky pakety, ktoré mali byť smerované zo siete von. Útočník z nich potom môže vyčítať citlivé dáta.

## 3. Implemetácia

Na sieťovú komunikáciu boli použité raw sockety. Možno tak meniť informácie nie len na v samotnom DHCP pakete, ale aj v hlavičkách UDP, IP a Ethernet.

### Starvation

pds-dhcpstarve vytvára veľké množstvo falošných klientov. Každý z nich dokáže samostatne reagovať na DHCP správy a má náhodne vygenerovanú MAC adresu. Táto MAC adresa sa používa už na úrovni L2. pds-dhcpstarve sa teda v podstate tvári ako prepínač, za ktorým je veľké množstvo zariadení.



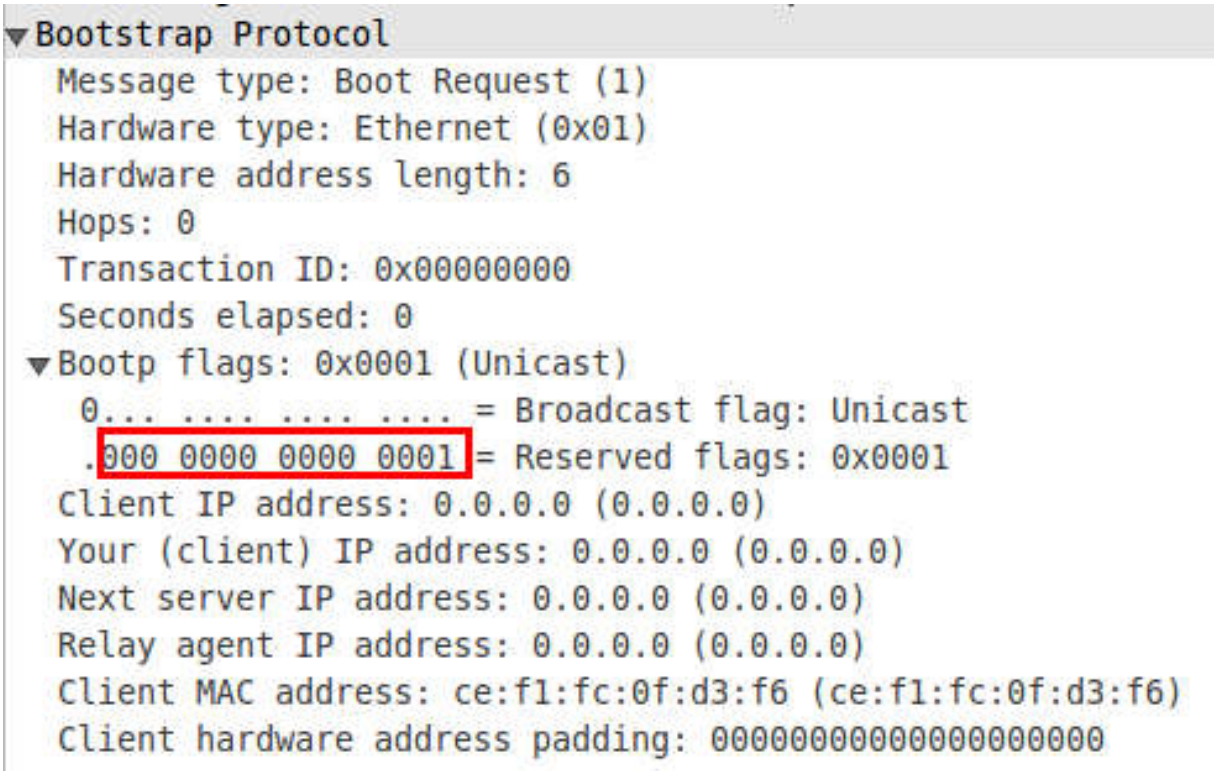
Po vytvorení falošný klient odošle najprv Discover paket a čaká na Offer. Po jeho prijatí pošle Request a nastaví si IP adresu. Až potom je vytvorený ďalší falošný klient. Falošných klientov sa teda vytvorí presne toľko, koľko bolo voľných adries v poole serveru.

Pokiaľ server nereaguje na Discover, pokus sa opakuje a noví falošní klienti sa nevytvárajú. Taktiež sa skontrolujú už existujúci klienti. Ak platnosť IP adresy vypršala, daný klient sa vymaže a je nahradený novým.

## Spoofing

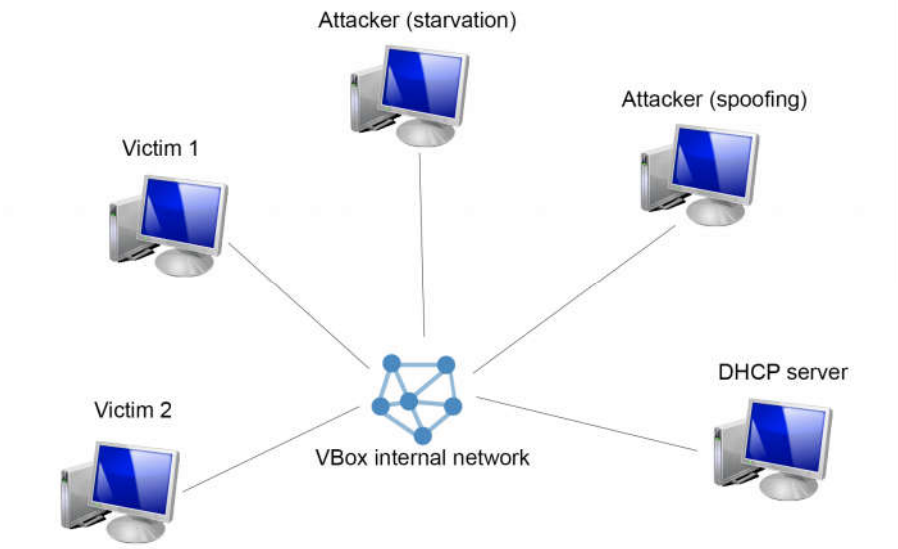
Falošný DHCP server pds-dhcprogue pracuje jednoducho v nekonečnej slučke, kde čaká a odpovedá na prichádzajúce Discover a Offer správy. Prijímanie správ je non-blocking, nie je teda nutné vytvárať nový proces pre každého komunikujúceho klienta. V každej iterácii cyklu sa tiež skontroluje, či niektorej IP adrese nevypršala platnosť. Ak áno, uvoľní sa.

Zo samotného zadania projektu vyplýva konflikt medzi jeho dvoma časťami. Keďže pds-dhcpstarve má útočiť na všetky DHCP servery v sieti, bude nevyhnutne útočiť aj na pds-dhcprogue, čo je ale neprijateľné, keďže pds-dhcprogue musí fungovať aj pri spustenom pds-dhcpstarve (aby bolo absolútne zaručené, že ostatné servery nefungujú). Tento problém bol vyriešený pomocou poľa príznakov bootp-flags v DHCP pakete. Na väčšinu týchto príznakov štandardné DHCP servery nereagujú a sú vždy nula. pds-dhcpstarve nastaví posledný príznak na 1. podľa toho pds-dhcprogue vie, ktoré pakety prichádzajú od pds-dhcpstarve a má ich ignorovať. Vďaka tomu je pds-dhcprogue úplne imúnny voči pds-dhcpstarve.

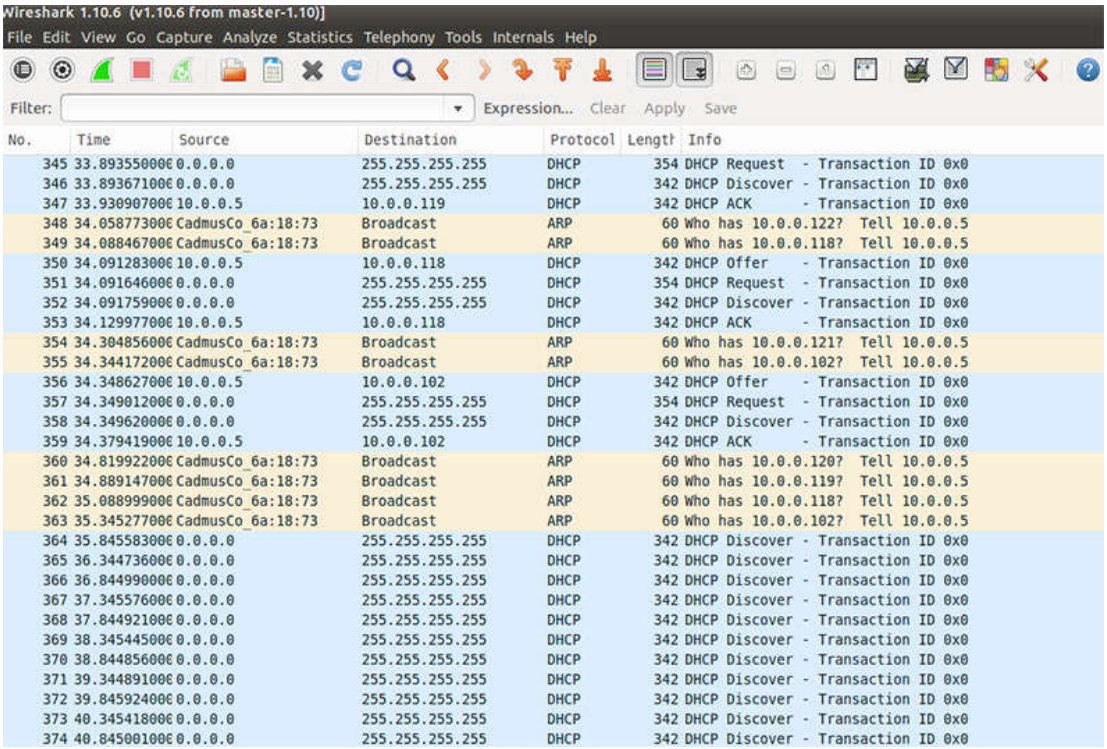


## 4. Demonštrácia činnosti

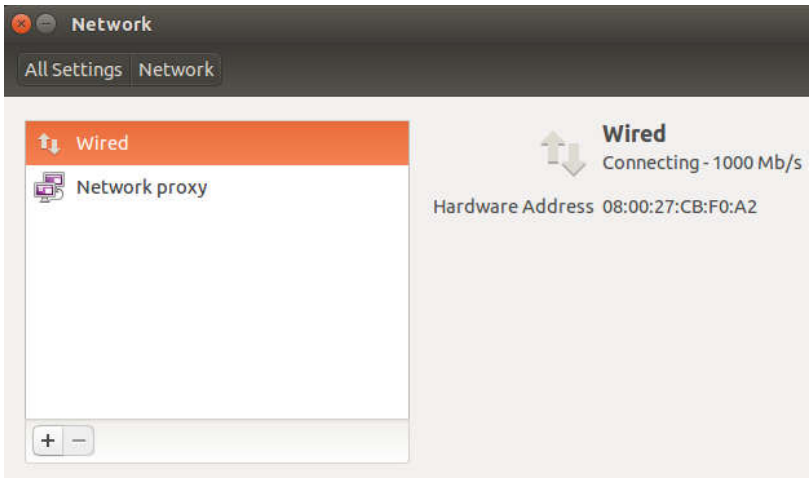
Testovacia sieť bola vytvorená v prostredí VirtualBox. Obsahovala celkom 5 virtuálnych strojov: útočník(starvation), útočník(spoofing), legitímny DHCP server a dve obete. Každý virtuálny stroj bol inštanciou stroja isa2015 dostupného v informačnom systéme. Sieť bola z bezpečnostných dôvodov úplne izolovaná od vonkajšku.



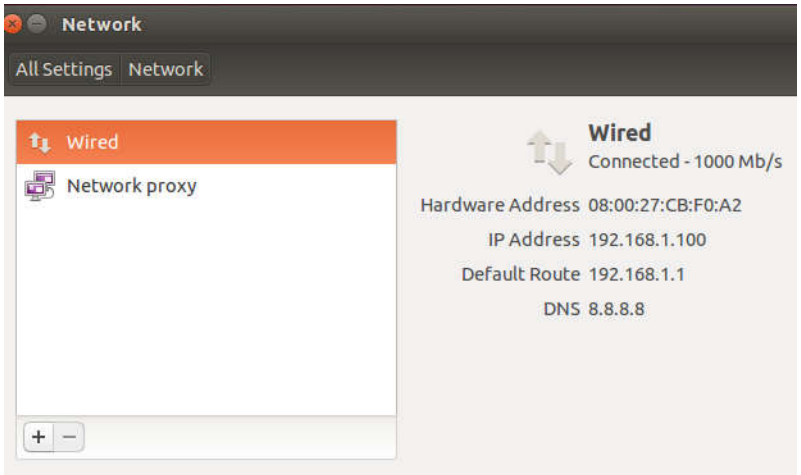

Ako legitímny DHCP server bol použitý štandardný linuxový isc-dhcp-server. Ako možno vidieť na obrázku, po vyčerpaní adresného poolu prestáva reagovať na Discover pakety. Vyčerpanie poolu o 50 adresách trvalo celkom 14 sekúnd. Tento čas je závislý hlavne na rýchlosti siete, spracovanie a generovanie paketov v rámci jedného počítača je neporovnateľne rýchlejšie a to aj na virtuálnom stroji.



Obete sa správajú podľa predstáv. Po pripojení do siete počas behu pds-dhcpstarve nie sú schopné získať od servera IP adresu. Ako náhle je však spustený pds-dhcprogue, získajú od neho sieťové parametre úplne bez problémov:




```
sudo ./pds-dhcprogue -i eth0 -p 192.168.1.100-192.168.1.199 -g 192.168.1.1 -n 8.8.8.8 -d example.com -l 3600
```



# Zdroje


- Bezpečnosť na LAN pod lupou: DHCP spoofing | SecIT.sk. SecIT.sk | Vírusy, bezpečnosť počítača a operačný systém [online]. Copyright © SecIT.sk [cit. 17.04.2018]. Dostupné z: https://secit.sk/sk/content/bezpecnost-na-lan-pod-lupou-dhcp-spoofing
- C Language Examples of IPv4 and IPv6 Raw Sockets for Linux. Dave's Website [online]. Dostupné z: http://www.pdbuchan.com/rawsock/rawsock.html
- The TCP/IP Guide - DHCP Message Format. Welcome to The TCP/IP Guide! [online]. Dostupné z: http://www.tcpipguide.com/free/t_DHCPMessageFormat.htm