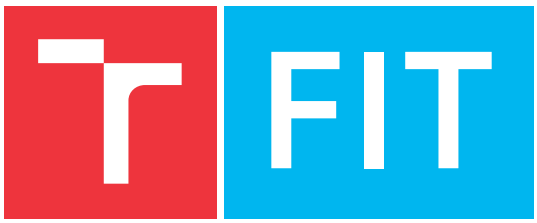


Přenos dat, počítačové sítě a protokoly

DHCP útoky

26. dubna 2018

Autor: Bc. Jiří Richter, xricht19@stud.fit.vutbr.cz

Fakulta Informačních Technologií
Vysoké Učení Technické v Brně

Obsah

Kapitola 1

Úvod

Ve světe IP sítí je bez pochyby za jeden z klasických útoků považován Denial of service (DoS), tedy zneschopnění internetové služby vykonávat svoji činnost. Může se jednat o různé typy služeb, například: webový server, e-mailový server, DHCP server a další. V druhé kapitole se zaměřím na popis útoku podvržení DHCP serveru. Ve třetí kapitole popíši implementaci tohoto útoku, demonstuji jeho činnost v praxi a popíši způsoby jak se tomuto útoku bránit.

Kapitola 2

Podvržení DHCP serveru

V této kapitole se zaměřím na popis útoku — Podvržení DHCP serveru. Útok umožňuje přesměrovat veškerou komunikaci mezi lokální sítí a internetem přes útočníkem stanovený uzel — výchozí bránou.

Útok je možné realizovat na lokální síti, která komunikuje pomocí protokolu IPv4. Útok není typicky prováděn na sítích komunikujících na protokolu IPv6, protože tento protokol nevyžaduje použití DHCP serveru v lokální síti. Protokol IPv6 implementuje bezstavovou konfiguraci — tedy každý uzel je schopen nastavit parametry sítě samostatně, pouze s informacemi od směrovače (prefix lokální sítě a přes který směrovač lze komunikovat s vnější sítí.)

DHCP server poskytuje zařízením v místní síti konfigurační parametry pro připojení — IP adresu, výchozí bránu, DNS servery, doménu a další. DHCP protokol je postaven na BOOTP protokolu a využívá UDP transportní protokol a IP síťový protokol. [3]

2.1 Princip útoku

Útok se zkládá ze dvou separátních částí. V první části útoku je nutné vyřadit z provozu existující DHCP servery v síti. Druhá část útoku spočívá v provozu vlastního DHCP serveru, který poskytuje zařízením v síti vlastní konfigurační parametry sítě (DoS útok).

2.2 DHCP Starvation

Každý DHCP server disponuju omezenou kapacitou IP adres. Pokud je kapacita vyčerpána, není možné připojit nové zařízení do sítě s tímto DHCP serverem. Pokud existuje v síti více DHCP serverů, není připojení do sítě možné ve chvíli, kdy jsou vyčerpány kapacity všech serverů.

Útok se skládá z vytvoření dostatečného množství falešných klientů, kteří vyčerpají kapacity IP adres. Každá adresa je zapůjčena k použití na omezenou dobu (např. 10 minut, dle nastavení serveru) a po tu není možné adresu přiřadit novému klientovi, pokud není adresa klientem uvolněna. Každý klient musí provést komunikaci se serverem a získat přiřazenou IP adresu sítě. Úspěšná komunikace mezi klientem a DHCP serverem se skládá ze 4 zpráv:

- DHCP Discover
- DHCP Offer
- DHCP Request

- DHCP Acknowledge

Po připojení do místní sítě zašle klient zprávu DHCP Discover, tato zpráva je zasílána IPv4 multicastem na UDP port 67. Server odpoví zprávou DHCP Offer, která je posílána IPv4 multicastem — klient nemá přidělenou IP adresu — na UDP port 68. Klient odpoví zprávou DHCP Request (vybere jednu zprávu DHCP Offer, pokud jich obdržel více), která obsahuje parametry sítě o které klient žádá — tyto parametry obdržel ve zrávě DHCP Offer — zpráva je zaslána stejným způsobem jako DHCP Discover. Server potvrdí parametry zprávou DHCP Acknowledge a tu zašle steně jako DHCP Offer zprávu. Tím je komunikace úspěšně ukončena a IP adresa na omezenou dobu — dle nastavení serveru — zablokována.[3]

Tímto může být útok ukončen s úspěšně dosažený cílem znemožnit novým klientů připojit se do sítě.

2.3 Rogue DHCP server

Po vyčerpání adres právého DHCP serveru v místní síti, je spušteň útočníkův falešný DHCP server. Ten poskytuje novým klientům falešné parametry pro připojení do místní sítě. To umožňuje útočníkovi přesměrovat komunikaci nových klientů přes jím definovaný uzel, případně podstrčit vlastní DNS server a tím zcela změnit cíl komunikace místního klienta s vnějším internetem.

Protože útočníkův falešný DHCP server plní na místní síti funkci DHCP serveru, musí být schopen přijímat zprávy DHCP Discover a DHCP Request a posílat zprávy DHCP Offer a DHCP Acknowledge.

2.4 Obrana proti útoku

Protože je poměrně jenoduché útok provést, je nutné se proti němu bránit. Obrana spočívá v zabránění vyčerpání IP adres na legitimním DHCP serveru.

Jedním z možných způsobů zabránění vyčerpání adres je průběžné posílání ARP zpráv s IP adresou, s dotazem zda ji někdo aktivně používá. Pokud DHCP server, který tuto zprávu odeslal neobrdží odpověď, považuje tuto IP adresu za nepoužívanou a poskytne ji novému klientovi k dispozici. Tento způsob obrany byl pozorován na routeru *Asus RT-AC68U*[1].

Dalším způsobem obrany, který brání jak vyčerpání IP adres, tak provozu falešného serveru na místní síti je DHCP Snooping. Jedná se o bezpečnostní opatření na L2 (linkové) vrstvě, kde jsou všechny porty — kromě portu, kde jsou připojeny switche a DHCP server — označené jako nedůvěryhodné. Fungující DHCP Snooping systém po-té zahazuje tyto druhy zpráv[1][2]:

- Zprávy od DHCP serveru, který není na důvěryhodném portu.
- DHCP zprávy, kde nesouhlasí MAC adresa v DHCP hlavičce a zdrojová MAC adresa.
- DHCP Release a DHCP Decline zprávy, které jsou poslány z jiného portu, než kde probíhala původní komunikace.

[1] https://www.asus.com/cz/Networking/RTAC68U/

Kapitola 3

Implementace

V této kapitole popisuji ukázkovou implementaci DHCP útoku na vyčerpání IP adres legitimního serveru a vytvoření a provoz vlastního DHCP serveru. V rámci projektu byly vytvořeny 2 programy vykonávající tuto funkci. Program **pds-dhcpstarve** provádí DHCP Starvation útok (popsaný v kapitole 2.2) na legitimní server. Po-té je spuštěn program **pds-dhcprogue** (popsaný v kapitole 2.3), který slouží jako útočníkův DHCP server a poskytuje falešné parametry sítě.

3.1 DHCP Starvation

Program **pds-dhcpstarve** postupně vytváří velké množství DHCP klientů, kteří se snaží získat IP adresu.

Protože komunikace mezi DHCP klientem a serverem může trvat i několik vteřin, není vhodné generovat klienty postupně — vyčerpání by v tom případě trvalo několik minut při 255 dostupných adresách ale i více než den při 65 536 dostupných adresách. Jak bylo zmíněno v kapitole 2.2, server zapůjčuje IP adresu pouze na omezenou dobu. Pokud nebude útok dostatečně silný, nemusí dojít k vyčerpání adres vůbec. Z toho důvodu jsem navrhl program tak, že v jeden okamžik vytvoří předem stanovený maximální počet klientů, kteří se snaží získat IP adresu. Po-té se každé 2 vteřiny vytvoří další klienti tak, aby existoval vždy maximální počet klientů. Ve chvíli kdy klient selže v získání IP adresy — nedostane od serveru zprávu DHCP Offer nebo DHCP Acknowledge v časovém limitu — sníží se maximální počet aktivních klientů o 1, až na limit 1 funkční klient. Naopak, pokud klient uspěje v získání IP adresy, zvýší se maximální počet aktivních klientů o 1, až na limit maximální počet klientů. Všechny výše uvedené parametry je možná nastavit v souboru *pds-dhcpstarve.h*.

DHCP klient implementuje 4 typy zpráv. Zpracovává zprávy DHCP Offer a DHCP Acknowledge a zasílá zprávy DHCP Discover a DHCP Request. Zprávy jsou vytvářeny a zpracovávány dle *rfc 2131* [3].

3.2 DHCP Rogue server

Program **pds-dhcprogue** jsem implementoval jako DHCP server, kterému je možno nastavit rozsah IP adres k přidělení, výchozí bránu, dns server, doménu a dobu zapůjčení IP adresy.

DHCP server byl vytvořen dle specifikace uvedené v *rfc 2131* [3]. Server naslouchá na portu 67 na příchozí zprávy od klientů. Klient může kontaktovat server z několika důvodů:

- Nový klient — server obdrží zprávu DHCP Discover, na kterou odpovídá zprávou DHCP Offer s parametry sítě a volnou IP adresou. Adresa je blokována po dobu uvedenou v souboru *pds-dhcprogue.h*. Výchozí hodnota je 120 sekund.
- Jednající klient — server obdrží zprávu DHCP Requests od klienta, kterému poslal DHCP Offer.
- Init-reboot state — server obdrží DHCP Request od klienta, kterému dříve přidělil IP adresu a který se na čas odmlčel.
- Renewing — server obdrží DHCP Request od klienta, který má přidělenou IP adresu a chce prodloužit dobu zapůjčení IP adresy. Odpověď je posílána Unicast zprávou DHCP Acknowledge
- Rebinding — server obdrží DHCP Request od klienta, který měl v minulosti IP adresu ale již vypršela doba zapůjčení. Klient žádá o adresu, kterou dříve používal.

Na serveru jsem implementoval ještě tyto další typy zpráv:

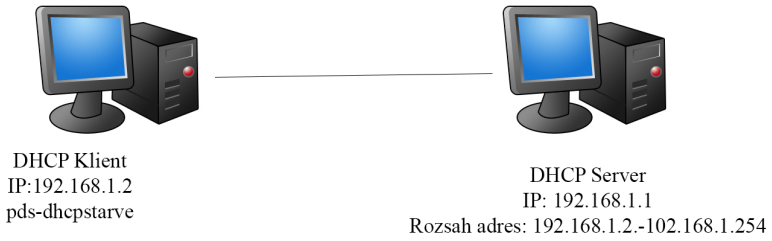
- DHCP Decline — odmítnutí IP adresy klientem, protože už je využívána. Server označí adresu jako nepoužitelnou.
- DHCP Release — server uvolní IP adresu přidělenou klientovi, což mu umožní ji znovu použít.
- DHCP Inform — server odpoví zprávou DHCP Acknowledge, kde zasílá parametry místní sítě. Ve zprávě není obsažena žádná IP adresa k přidělení.

Protože server také musí uvolňovat adresy přidělé klientům — pokud vyprší doba zapůjčení — je neustále nutné kontrolovat přidělené adresy. Tuto funkcionalitu jsem implementoval sekvečně k obsluze klientů. Aby vlivem kontroly adres nedocházelo ke zpoždění obsluhy klientů, v souboru *pds-dhcprogue.h* lze nastavit počet adres (z rozsahu adres k zapůjčení), u kterých se má zkontrolovat, zda nevypršela doba zapůjčení, mezi každým pokusem obsloužit klienta. Toto číslo by se mělo zvolit v závislosti na době zapůjčení IP adresy a množství adres k zapůjčení. Pokud je doba zapůjčení krátká a velký rozsah adres k zapůjčení, je nutné kontrolovat více adres mezi obsluhou klienta.

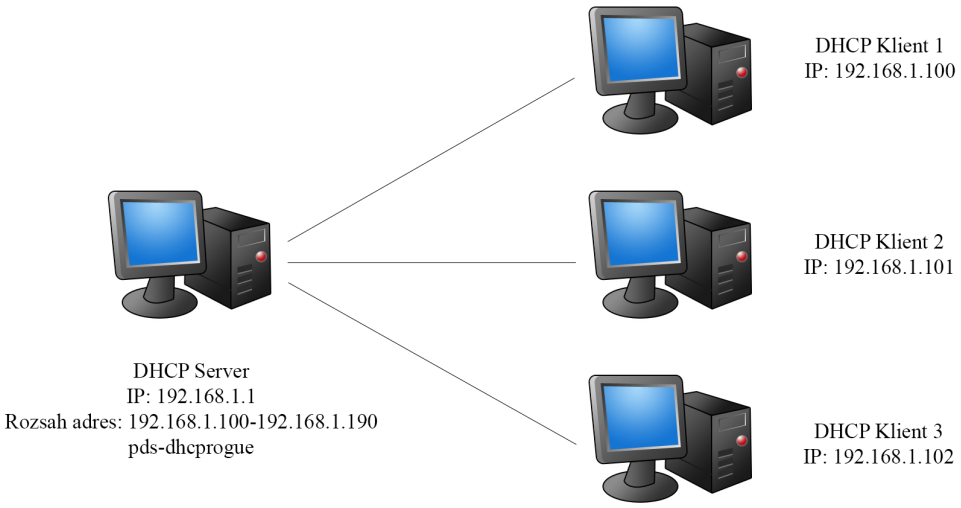
Kapitola 4

Demonstrace činnosti

V této kapitoli jsou uvedeny ukázky testovací sítě a výstupy demonstrující činnosti programů **pds-dhcpscanner** a **pds-dhcprogue**.



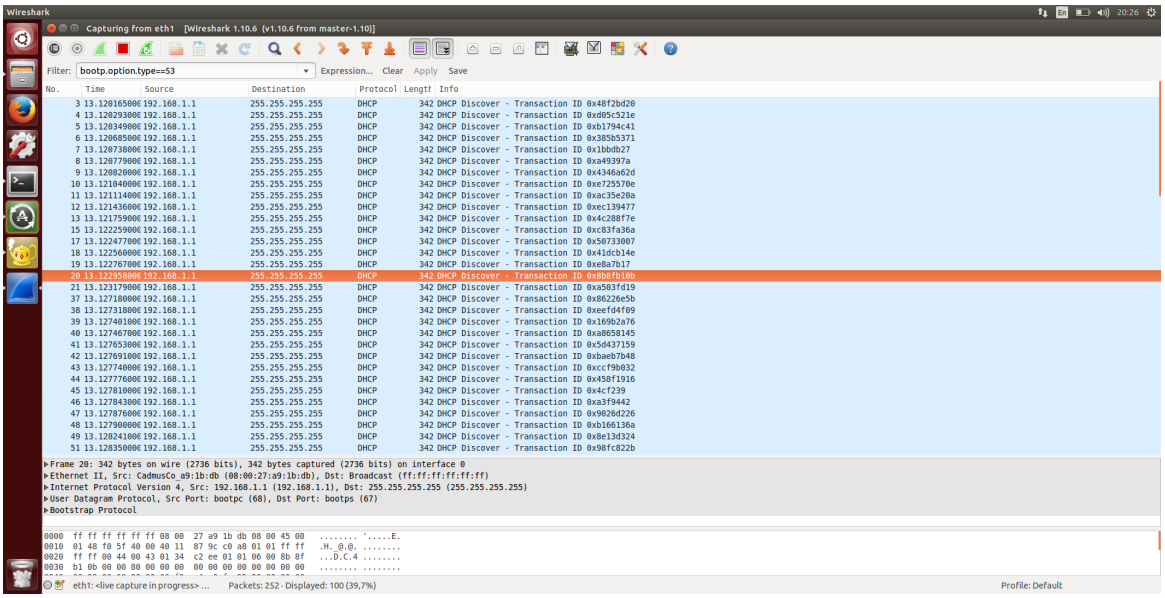
Obrázek 4.1: Schéma zapojení sítě pro testování **pds-dhcpstarve**.



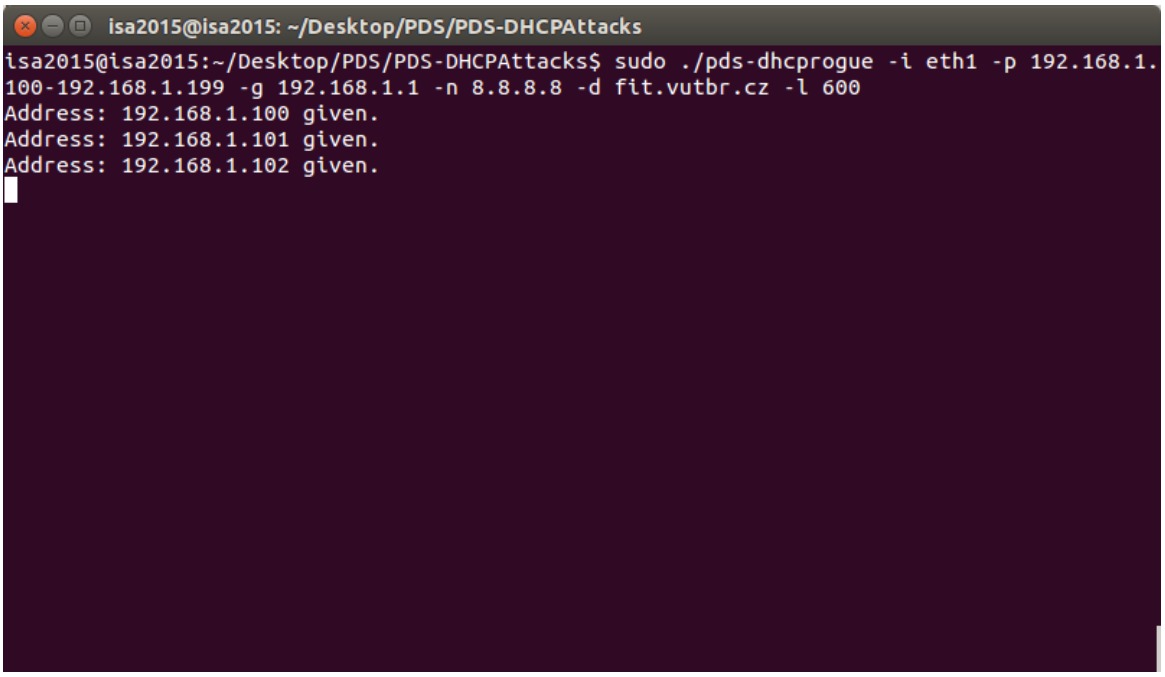
Obrázek 4.2: Schéme zapojení sítě pro testování **pds-dhcprogue**.

```
isa2015@isa2015: ~/Desktop/PDS/PDS-DHCPAttacks
isa2015@isa2015:~/Desktop/PDS/PDS-DHCPAttacks$ sudo ./pds-dhcpstarve -i eth1
Interface: eth1
Thread 1:IP address:192.168.1.113, obtained!
Thread 2:IP address:192.168.1.114, obtained!
Thread 7:IP address:192.168.1.115, obtained!
Thread 11:IP address:192.168.1.116, obtained!
Thread 15:IP address:192.168.1.117, obtained!
Thread 3:IP address:192.168.1.118, obtained!
Thread 4:IP address:192.168.1.119, obtained!
Thread 16:IP address:192.168.1.120, obtained!
Thread 17:IP address:192.168.1.121, obtained!
Thread 26:IP address:192.168.1.122, obtained!
Thread 5:IP address:192.168.1.123, obtained!
Thread 6:IP address:192.168.1.124, obtained!
Thread 20:IP address:192.168.1.125, obtained!
Thread 19:IP address:192.168.1.126, obtained!
Thread 18:IP address:192.168.1.127, obtained!
Thread 23:IP address:192.168.1.128, obtained!
Thread 29:IP address:192.168.1.129, obtained!
Thread 31:IP address:192.168.1.130, obtained!
Thread 33:IP address:192.168.1.131, obtained!
Thread 32:IP address:192.168.1.132, obtained!
Thread 22:IP address:192.168.1.133, obtained!
Thread 21:IP address:192.168.1.134, obtained!
```

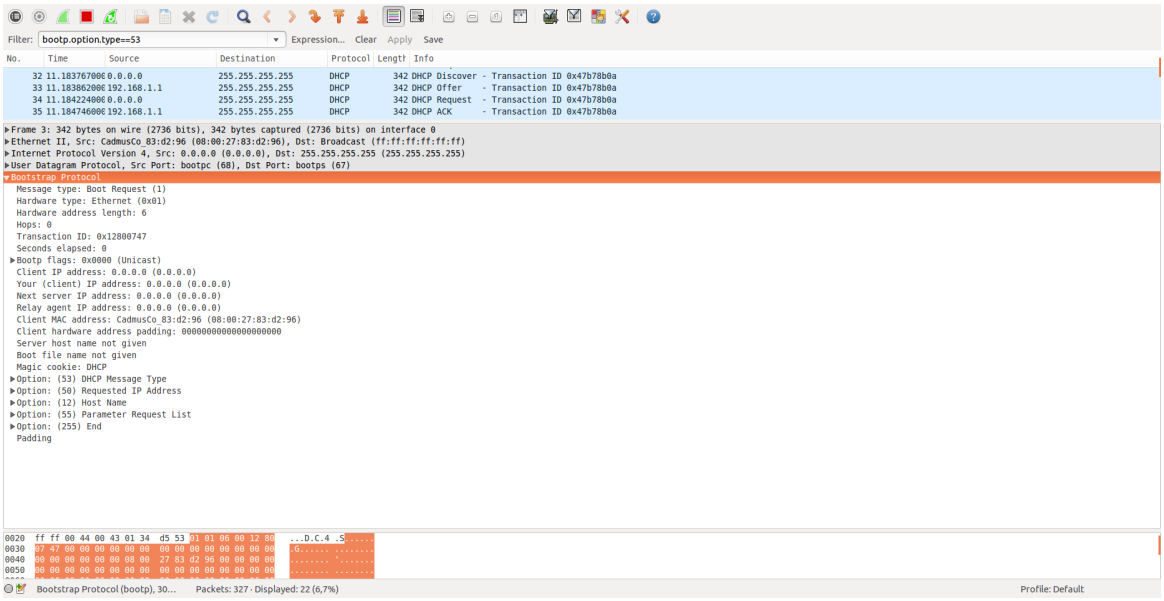
Obrázek 4.3: Ukázka výstupu programu **pds-dhcpstarve**. Jednotlivá vlákna získala IP adresy.



Obrázek 4.4: Ukázka DHCP Discover zpráv, které jsou zasílány jednotlivými vlánky při útoku DHCP vyčerpání adres



Obrázek 4.5: Ukázka výstupu a parametrů spuštění DHCP Rogue serveru. Program **pds-dhcprogue**.



Obrázek 4.6: Ukázka přidělení adresy klientovi od DHCP Rogue serveru.

Kapitola 5

Závěr

Byly rozebrány definice a vlastnosti DHCP útoků, obrana proti těmto útokům a kroky nutné k implementaci. Byly implementovány dva programy — první, demonstrující vyčerpání adresního prostoru legitimního DHCP serveru a druhý, podstrčení falešných parametrů místní sítě novým klientům. Funkčnost byla otestována na testovací místní síti pomocí virtuálních počítačů a DHCP serveru **isc-dhcp-server**.

Literatura

[1] Ethan Banks. *Five Things To Know About DHCP Snooping.* [Online; navštíveno 26.4.2018].

[2] Petr Bouška. *Cisco IOS 13 - DHCP služby na switchi.* [Online; navštíveno 26.4.2018].

[3] R. Droms. *Dynamic Host Configuration Protocol.* [Online; navštíveno 26.4.2018].