VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

POČÍTAČOVÉ KOMUNIKACE A SÍTĚ
2017/2018

projekt č. 2, varianta 2:

DHCP Starvation útok

Alena Tesařová (xtesar36) Brno, 9. dubna 2018

Obsah

1 POPIS PROJEKTU

1.1 Teorie

Účelem projektu bylo nasimulovat DHCP útok, který využívá skutečnosti, že každý DHCP server má přesně definovaný počet IP adres, které může přidělit zařízením. Útočník pak vybere všechny volné IP adresy tak, že použije velké množství falešných MAC adres.

Žádost o IP adresu probíhá v několika fázích. Nejprve klient musí vyslat DHCPDISCOVER zprávu na fyzické vrstvě, kterou pošle všem zařízení na stejném subnetu (pomocí broadcastu) a čeká, až mu nějaký server odpoví (existuje timeout doba, po kterou čeká na odpověď). Server odpoví zprávou DHCPOFFER, která zahrnuje dostupnou síťovou adresu. Klient si z (teoreticky mnoha) nabídek vybere jednu IP adresu a o tu požádá paketem DHCPREQUEST, kde je již specifikováno, který DHCP server si klient vybral a jakou IP adresu. Ke správnému ukončení spojení a svázání IP adresy musí server zareagovat odpovědí DHCPACK, která obsahuje konfiguraci parametrů pro klienta. Pokud server nedokáže zkontrolovat správnost IP adresy, pošle zprávu DHCPNACK. Výsledku rezervování IP adresy říkáme pronájem adresy. Každý DHCP server má určenou maximální dobu pronájmu tedy dobu, po kterou může klient využívat IP adresu. Po vypršení doby se celý proces opakuje, procesu prodloužení doby pronájmu adres se říká *renew*.

1.1.1 Další zprávy v komunikaci

DHCPDECLINE – klient zjistil, že tato adresa již existuje

DHCPRELEASE – klient se vzdává pronájmu

SHCPINFORM – klient zjišťuje lokální konfiguraci

1.1.2 Ochrana proti útoku

Jelikož je útok známý, administrátoři sítí se umí bránit. Zmíním dvě nejzákladnější prevence útoku. První způsobem obrany je zabezpečení portu brány, které spočívá v omezení počtu možných MAC adres na jeden port. Pokud dojde k vyčerpání limitu, port se uzavře a při opětovném požádání o IP adresu z jiného zařízení posílá SNMP trap (podle nastavení konfigurace serveru).

DHCP snooping

Druhý princip spočívá v rozdělování portů brány na důvěryhodné a nedůvěryhodné. Jako důvěryhodné musíme označit porty DHCP serveru a porty, kterými jsou propojeny switche. Zároveň se může vytvářet DHCP Snooping Binding Database, kde jsou informace o přidělených IP adresách společně s MAC adresami. Pokud přijde paket z nedůvěryhodného portu, tak je paket zahozen.

1.2 Implementace

Implementovala jsem útok nekonečným posíláním DHCPDISCOVER. Útok realizuji ve skriptu *ipk-dhcpdiscover.c*, kde se nachází nekonečná smyčka a v ní generování random MAC adresy a posílání DISCOVER. K posílání používám ROW sockety, který využívají UDP.

Rozdělení podle modulů:

ipk-dhcpdiscover.c – zpracování argumentů, logický běh celého programu

dhcp.c – funkce pro tvoření a odesílání DHCPDISCOVER

udp.c – funkce pro skládání a inicializování UDP paketu

1.2.1 DHCPDISCOVER

Klient vysílá DHCPDISCOVER zprávu na cílovou adresu 255.255.255.255, anebo si může přímo požádat o naposledy známou IP adresu (pokud je klient připojen stále na stejné síti, server může garantovat přiřazení požadované IP adresy). Dále DHCP protokol vyžaduje, aby zpráva měla následující parametry:

OP – typ zprávy (1 = BOOTREQUEST, 2 = BOOTREPLY)

HTYPE – typ adresy hardwaru (pro Ethernet 1)

HLEN – velikost adresy (pro Ethernet MAC adresa má délku 6 bajtů)

HOPS – používá se při komunikaci přes relay agenta

XID – identifikační číslo transakce (náhodné číslo, které si vymyslí klient)

FLAGS – příznaky (pro příznak broadcast se nastavuje první bit na 1)

CIADDR – klientova IP adresa

YIADDR – adresa, která mi bude přiřazena

SIADDR – IP adresa serveru

GIADDR – IP adresa brány

CHADDR – fyzická adresa klienta

Magic cookie – čtyři čísla (99,130,83,99)

DHCP options – např. typ zprávy (DISCOVER/REQUEST), specifikující parametry atd.

Magic cookie slouží k rozeznání BootP a DHCP zpráv. Protokoly se liší v přidělování IP adres, v BootP musí být klientova fyzická adresa zapsána manuálně v BootP tabulce a v DHCP se přidělování mac adres děje dynamicky.

1.3 Demonstrace činnosti

Na obrázku [1] lze vidět moje topologie. Jak můžete vidět, nachází se zde pouze router plnící funkci DHCP serveru a dva osobní počítače, z nichž jeden zahlcuje server zprávami DHCPDISCOVER a na druhém můžu pozorovat, že není schopen dostat IP adresu. Žádost o novou IP adresu po útoku je na obrázku [4], ping na bránu na obrázku [3]. Na obrázku [4] lze vidět, že server není schopen komunikace po útoku.

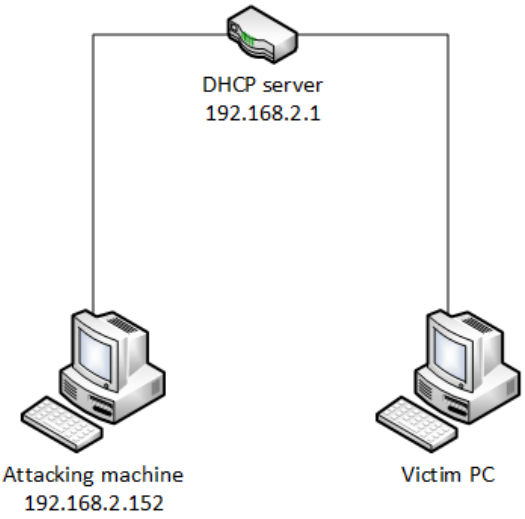
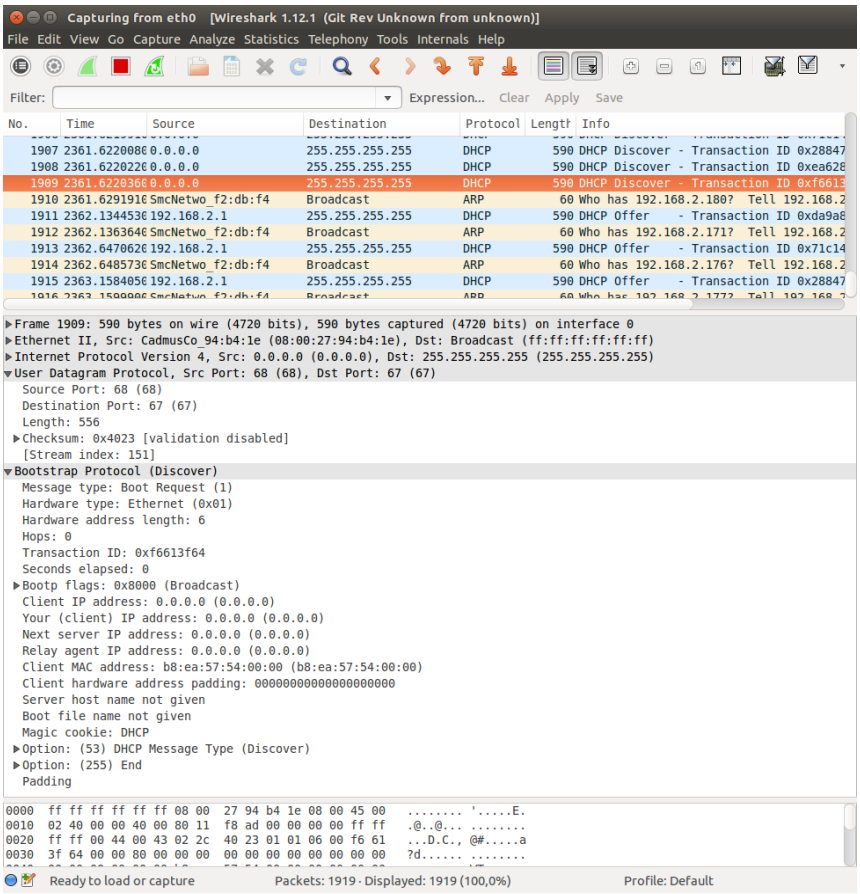


Schéma připojí k DHCP serveru [1]

Na obrázku [2] je zobrazen odesílaná zpráva DISCOVER. Skládám ji ze čtyř vrstev – ethernetová, IP, UDP a DHCP. V ethernetové hlavičce nastavuji zdroj, což je MAC adresa rozhraní, který zadá uživatel, a cílem jsou všechna zařízení. Jelikož ještě nemám přiřazenou žádnou IP adresu, vyplňuji v IP hlavičce zdroj 0 a cíl opět broadcast. V UDP specifikuji port příjemce a odesílatele. Klient komunikuje na portu 68 a server naslouchá na UDP portu 67. DHCP protokol je podrobněji popsán v sekci 1.2.1.



Ukázka DHCP paketu ve Wiresharku [2]

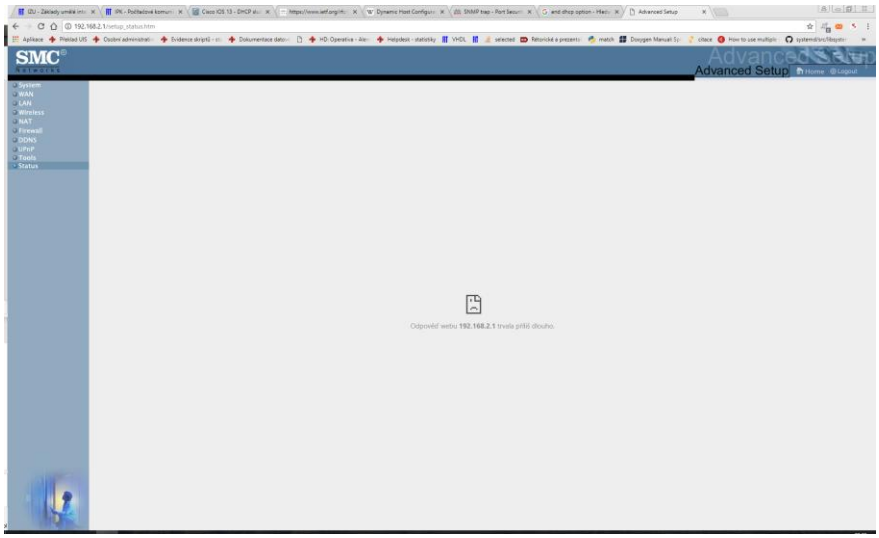
```
isa2015@isa2015: ~/Documents/FIT/2BIT_LS_2018/IPK/2.projekt
^Cisa2015@isa2015:~/Documents/FIT/2BIT_LS_2018/IPK/2.projekt$ ping 192.168.2.1
PING 192.168.2.1 (192.168.2.1) 56(84) bytes of data.
From 192.168.2.175 icmp_seq=1 Destination Host Unreachable
From 192.168.2.175 icmp_seq=2 Destination Host Unreachable
From 192.168.2.175 icmp_seq=3 Destination Host Unreachable
From 192.168.2.175 icmp_seq=4 Destination Host Unreachable
From 192.168.2.175 icmp_seq=5 Destination Host Unreachable
From 192.168.2.175 icmp_seq=6 Destination Host Unreachable
From 192.168.2.175 icmp_seq=7 Destination Host Unreachable
From 192.168.2.175 icmp_seq=8 Destination Host Unreachable
```

ping na bránu po útoku [3]

```
isa2015@isa2015:~/Documents/FIT/2BIT_LS_2018/IPK/2.projekt$ sudo dhclient -v
Internet Systems Consortium DHCP Client 4.2.4
Copyright 2004-2012 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/eth0/08:00:27:94:b4:1e
Sending on   LPF/eth0/08:00:27:94:b4:1e
Sending on   Socket/fallback
DHCPREQUEST of 192.168.2.175 on eth0 to 255.255.255.255 port 67 (xid=0x24d412c4
DHCPREQUEST of 192.168.2.175 on eth0 to 255.255.255.255 port 67 (xid=0x24d412c4
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 3 (xid=0xb68c7341)
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 3 (xid=0xb68c7341)
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 4 (xid=0xb68c7341)
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 11 (xid=0xb68c7341)
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 10 (xid=0xb68c7341)
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 14 (xid=0xb68c7341)
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 14 (xid=0xb68c7341)
```

požádání o novou IP adresu po útoku [4]



Refresh statusu DHCP serveru po útoku [5]

2 BIBLIOGRAFIE

[1] Dynamic Host Configuration Protocol [online]. Bucknell University: R. Droms, 1997 [cit. 2018-04-07]. Dostupné z: https://www.ietf.org/rfc/rfc2131.txt

[2] Dynamic Host Configuration Protocol. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2018-04-09]. Dostupné z: https://cs.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol

[3] DHCP snooping. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2018-04-09]. Dostupné z: https://en.wikipedia.org/wiki/DHCP_snooping

[4] Cisco IOS 13 - DHCP služby na switchi. *Samuraj* [online]. 2008 [cit. 2018-04-09]. Dostupné z: https://www.samuraj-cz.com/clanek/cisco-ios-13-dhcp-sluzby-na-switchi/