Fakulta informačních technologií

Vysoké Učení Technické v Brně

Projekt do předmětu IPK

DHCP Starvation útok

Autor:
Hynek Bernard
xberna16

Datum: 9.4. 2018

Obsah

1 Zadání

[1] Nastudovat problematiku DHCP útoků a relevantní informace uvést v projektové dokumentaci.

[2] Naprogramovat aplikace realizující DHCP Starvation útok, který by vyčerpal adresní pool legitimního DHCP serveru.

[3] Demonstrovat činnost aplikací v podmínkách Vaší vlastní testovací sítě.

2 Problematika

Je zapotřebí vyčerpat adresní pool DHCP serveru na tolik, aby se již nemohl připojit žádný další klient.

2.1 DHCP Protokol

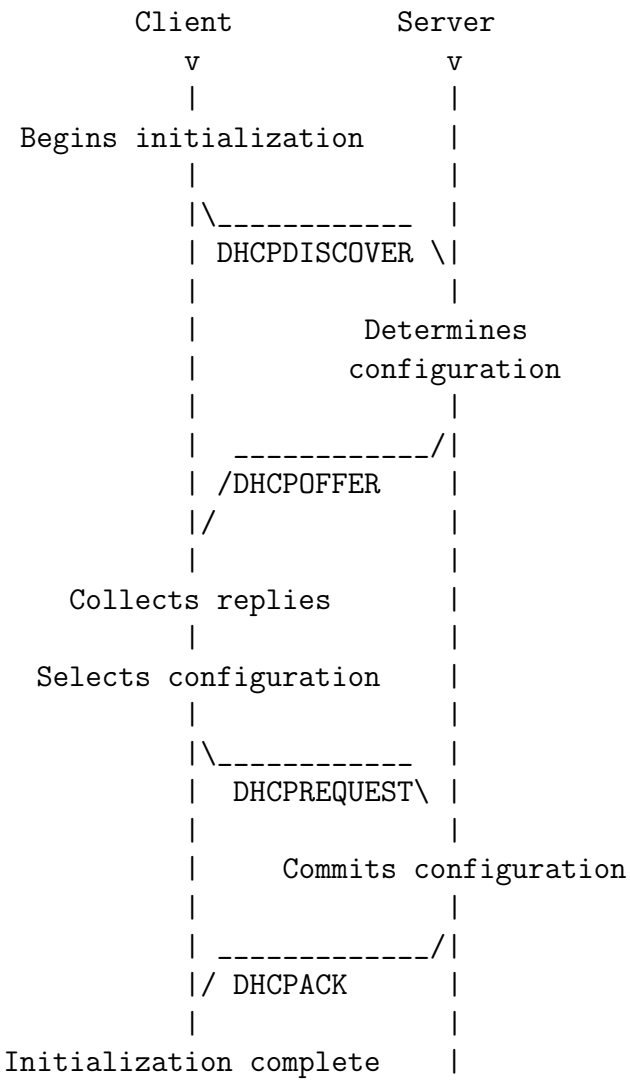
2.1.1 Popis

DHCP je protokol který slouží k poskytování konfiguračních informací zařízením na TCPIP síti. Formát DHCP zpráv je založen na formátu BOOTP, rozšiřuje ho o možnost automatické alokace IP adres a dalších konfiguračních nastavení a je zpětně kompatibilní s BOOTP. DHCP server má za úkol poskytovat klientům v lokální síti konfigurační parametry, mezi kterými je například i IP adresa. Po obdržení správných parametrů přes DHCP by měl být klient schopný výměny packetů s jakýmkoliv hostitelem na internetu.

2.1.2 Nastavení klienta

Nejdříve klient pošle DHCPDISCOVER na broadcast interface a čeká na odpověd serveru který by mu měl odpovědět DHCPOFFER zprávou ve které je adresa kterou klientovi nabízí. Na tu klient může reagovat zprávou DHCPREQUEST, ve které odešle své hostname a adresu o kterou žádá, také si od serveru může vyžádat doplňující informace o serveru a síti. Pokud byla komunikace úspěšná, server odešle klientovi zprávu DHCPACK jako potvrzení že má přidělenou IP adresu, jinak odešle zprávu DPCPNAK.

Klient může po znovupřipojení zažádat o stejnou adresu, nemusí již posílat DHCPDISCOVER ale může rovnou odeslat zprávu DHCPREQUEST, ovšem nemusí mu být už přidělena pokud je již zabrána.
Příklad komunikace mezi klientem a serverem:



2.2 Útok na DHCP server

Podstatou útoku je zahlcení serveru DHCPDISCOVER zprávami, aby nabídl všechny adresy dostupné v konfiguraci falešným klientům. Díky tomu už

nebude mít žádnou další volnou adresu k nabídnutí novému klientovi. Reálně se tento útok využívá pokud chce útočník nasadit vlastní falešný DHCP server, který by odkazoval klienty na komunikaci skrz jeho zařízení a tím mohl být "man in the middle".

3 Implementace

3.1 Popis

Program se zprvu rozvětví na 3 procesy ve kterých je nekonečný cyklus:

První má za úkol odesílat na interface každou vteřinu DHCPDISCOVER.

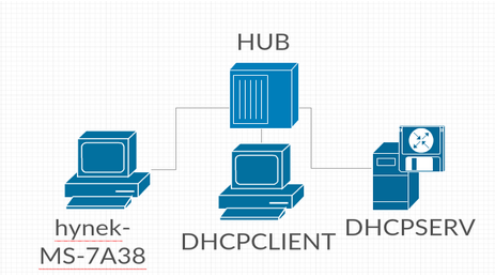
Druhý přijímá DHCPOFFER a obratem na ně posílá DHCPREQUEST

Třetí je už jen pro výpis, odchytává všechny DHCPACK a vypisuje je formátovaně na stdout

4 Demonstrace

4.1 Topologie sítě

Vytvořil jsem na PC virtuální interface s názvem tap0 a poté jsem nainstaloval 2 virtuální počítače(DHCPCLIENT, DHCPSERV) do virtualBoxu. Oba jsem připojil na interface tap0 jako na most a nasimuloval tím zapojení do hubu. Na DHCPSERV jsem nainstaloval DHCP server, nakonfiguroval ho, nastavil mu statickou IP adresu.

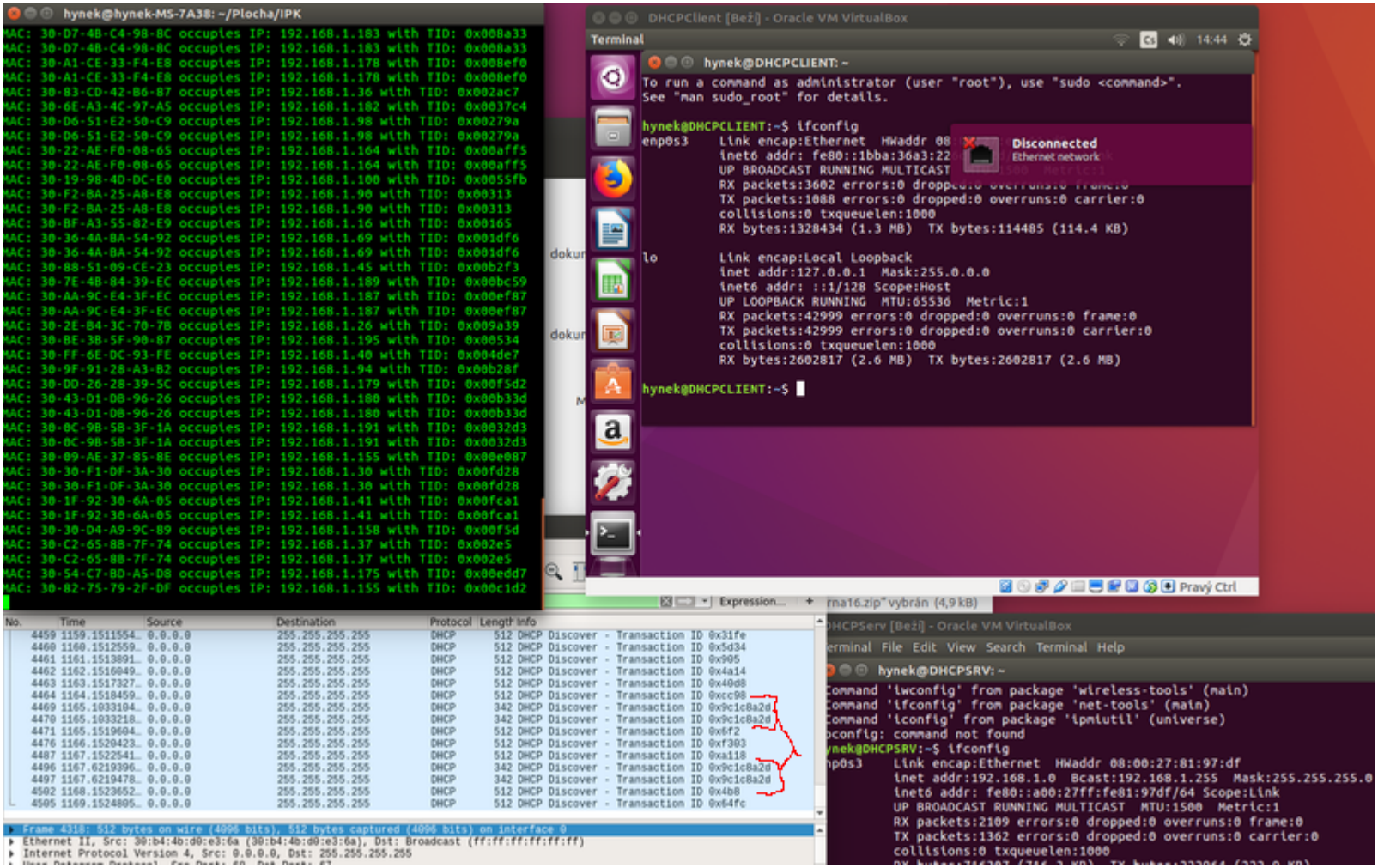


4.2 Simulace útoku

Zapl jsem dhcpd na zařízení DHCPSERV a na hynek-MS-7A38 jsem zapl program a nechal běžet

```
sudo ./ipk-dhcpstarve -i tap0
```

Po 5 minutách jsem zapl zařízení DHCPCLIENT a tomu se již nepodařilo připojit k síti protože byl adresní pool již vyčerpán.
Na screenu je znázorněný DHCPDISCOVER bez odpovědi ve wireshark a DHCPCLIENT ve virtualboxu nepřipojený k síti, v programu mám nastavené aby packety měly délku TID pouze na 2 nejmenších bytech, ubuntu používá pro TID 4 byty, záměr byl jen pro demonstraci a rychlé rozlišení packetů útočníka a klienta ve wireshark. V terminálu nalevo jsou vypsány všechny packety ACK které program přijal



5 Literatura

R. Droms, RFC 2131:Dynamic Host Configuration Protocol, https://tools.ietf.org/html/rfc2131

A. Marton, Sending raw Ethernet packets, https://austinmarton.wordpress.com/2011/09/14/sending-raw-ethernet-packets-from-a-specific-interface-in-c-on-linux/