



Počítačové komunikace a sítě – 2. projekt

DHCP Starvation útok

Úvod

V této dokumentaci je popsána problematika DHCP útoku a řešení druhého úkolu.

Problematika DHCP útoku

DHCP server se stará o přiřazování IP adres pro připojené počítače v síti. V případě DHCP starvation útoku se útočník snaží vyčepat všechny volné IP adresy, aby žádný další počítač neobdržel vlastní IP. Tento útok se provádí zahlcováním DHCP serveru Discovery zprávami.

Popis řešení DHCP útoku

Pro své řešení jsem využil UDP sokety. Vytvořil jsem strukturu, která formátem odpovídá DHCP zprávě. Obsahem pak byla data odpovídající pro Discover zprávu. Program zasílá v cyklu nové discover zprávy, kde v každé iteraci se navyšuje MAC adresa a id transakce o 1, aby se každá zpráva brala jako jedinečná. Program pak koční až po signálu SIGINT.

Demonstrace činnosti

Ve VirtualBoxu jsem vytvořil DHCP server na adrese 192.168.56.101:67. Komunikaci odposlouchávala na virtuálním orzhraní vboxnet0 aplikace Wireshark. Pro demonstraci jsem zadal pouze 10 žádostí, a čekal, zda server odpoví OFFER zprávou.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.56.1	192.168.56.101	DHCP	290	DHCP Discover - Transaction ID 0x1
2	0.000052049	192.168.56.1	192.168.56.101	DHCP	290	DHCP Discover - Transaction ID 0x2
3	0.000069980	192.168.56.1	192.168.56.101	DHCP	290	DHCP Discover - Transaction ID 0x3
4	0.000086212	192.168.56.1	192.168.56.101	DHCP	290	DHCP Discover - Transaction ID 0x4
5	0.000101427	192.168.56.1	192.168.56.101	DHCP	290	DHCP Discover - Transaction ID 0x5
6	0.000116281	192.168.56.1	192.168.56.101	DHCP	290	DHCP Discover - Transaction ID 0x6
7	0.000132007	192.168.56.1	192.168.56.101	DHCP	290	DHCP Discover - Transaction ID 0x7
8	0.000147242	192.168.56.1	192.168.56.101	DHCP	290	DHCP Discover - Transaction ID 0x8
9	0.000162482	192.168.56.1	192.168.56.101	DHCP	290	DHCP Discover - Transaction ID 0x9
10	0.000177948	192.168.56.1	192.168.56.101	DHCP	290	DHCP Discover - Transaction ID 0xa
11	0.001328353	192.168.56.101	192.168.56.10	DHCP	344	DHCP Offer - Transaction ID 0x1
12	0.001855386	192.168.56.101	192.168.56.11	DHCP	344	DHCP Offer - Transaction ID 0x2
21	0.004116600	192.168.56.101	192.168.56.10	DHCP	344	DHCP Offer - Transaction ID 0x1
22	0.004461048	192.168.56.101	192.168.56.11	DHCP	344	DHCP Offer - Transaction ID 0x2
47	1.004004657	192.168.56.101	192.168.56.12	DHCP	344	DHCP Offer - Transaction ID 0x3
48	1.004245709	192.168.56.101	192.168.56.13	DHCP	344	DHCP Offer - Transaction ID 0x4
49	1.004487999	192.168.56.101	192.168.56.14	DHCP	344	DHCP Offer - Transaction ID 0x5
50	1.004696301	192.168.56.101	192.168.56.15	DHCP	344	DHCP Offer - Transaction ID 0x6
51	1.005853944	192.168.56.101	192.168.56.16	DHCP	344	DHCP Offer - Transaction ID 0x7
52	1.006315877	192.168.56.101	192.168.56.17	DHCP	344	DHCP Offer - Transaction ID 0x8
53	1.006476836	192.168.56.101	192.168.56.12	DHCP	344	DHCP Offer - Transaction ID 0x3
54	1.006532107	192.168.56.101	192.168.56.13	DHCP	344	DHCP Offer - Transaction ID 0x4
55	1.006653295	192.168.56.101	192.168.56.14	DHCP	344	DHCP Offer - Transaction ID 0x5