# 1.1 Objasnite čemu služi protokol ARP i 2.2 prikažite to korištenjem primjera s dva računala povezanih na jedan switch. U primjeru koristite proizvoljne (ali realistične) IP i MAC adrese.

uputa [pcenito o arpu, dodao sam vise stvari, permutacija rijeci je dosta]

1.1 Protokol ARP služi za pretvaranje 32 bitnih IP adresa u 48 bitne MAC adrese. Jednostavnije rečeno, koristimo ga za dinamičko otkrivanje MAC adresa, kako IP adrese koristimo za logičko adresiranje MAC adrese služe za fizičko.

uputa [

pc1 : 192.168.x.y pc2 : 192.168.x.z

x e [1,100] y e [ 1, 250] z e [1,250] , y != z

mac1,2 : <https://miniwebtool.com/mac-address-generator/>

]

1.2

Računalo 1 :

IP = 192.168.1.1,

MAC = 6B:71:27:30:35:F3

Računalo 2 :

IP = 192.168.1.2,

MAC = 85:0D:E0:9C:7D:D1

uputa [komunikacija preuzeta iz chatGpta, malo je opsirnija]

Korak 1: računalo 1 projverava ima li u ARP spremištu MAC

adresa od računala 2. Ona ne postoji jer se komunikacija još

nije uspostavila.

Korak 2: računalo 1 šalje broadcast ARP zahtijev sa pitanjem tko

ima adresu 192.168.1.2 uključujući svoje preslikavanje.

Korak 3: preklopnik dobiva ARP zahtijev i šalje ga svim spojenim

uređajima osim onog koji je poslao.

Korak 4: računalo 2 projverava poklapa li se tražena IP adresa sa

njegovom. Ako je odgovor potvrdan, računalo 2 šalje svoju

MAC (85:0D:E0:9C:7D:D1) adresu preko ARP odgovora.

Korak 5: preklopnik dobiva ARP odgovor i prosljeđuje ga računalu

1.

Korak 6: računalo 1 prima odgovor i sprema ga u priručnu memoriju.

Sada može direktno slati pomoću MAC adrese.

Text

Description automatically generated

# 3. Otvorite IMUNES topologiju zadatak1/mitm.imn iz repozitorija vježbi i proučite IP i MAC adrese pojedinih čvorova u topologiji. Pokrenite eksperiment gumbom Experiment->Execute i snimajte promet na sučelju eth0 čvora PC. Na proizvoljan način stvorite ARP poruke slične onima koje ste opisali u prošlom zadatku. Na koju MAC adresu se šalje prvi ARP paket kojeg ste snimili (u polje odgovora upišite MAC adresu u ispravnom formatu)? Proučite tko sve dobije taj paket. Kad ste gotovi s radom na topologiji, ugasite eksperiment gumbom Experiment->Terminate.

ovo sam prepisao s disca

# 

FF:FF:FF:FF:FF:FF

# 4. Na koji način NAT čini lokalnu mrežu sigurnom?

By using NAT, devices on the local network are not

directly accessible from the internet, making it more

difficult for attackers to target them. In addition,

NAT provides a level of protection against denial-of-service

(DoS) attacks, as the router or gateway can limit the number of

connections from the internet to the local network.

NAT povezuje privatne IP adrese lokalne mreže sa javnima.

Povećava sigurnost tako da skriva IP adrese uređaja u mreži i

stavlja dodatni sloj sigurnosti. Njime se sprečava neovlašten

pristup i štit od raznih napada.

Postavlja limit na broj konekcija i tako sprečava DoS napad.

# 5. Objasnite zašto WEP više ne bi trebao biti u upotrebi sa stajališta sigurnosti?

One of the main vulnerabilities of WEP is that it uses a static encryption key that

is shared among all devices on the network. This makes it easy for attackers to

capture and decrypt network traffic. Additionally, WEP uses a weak encryption algorithm

(RC4), which can also be easily cracked.

Koristi statički enkripcijski ključ za sve uređaje koji se spajaju

na mrežu. Lako je snimiti i dekriptirati mrežni promet. Koristi

RC4 algoritam koji je lako probiti.

Preza -->

Ovo je primjer krive upotrebe kriptografije jer pomoću gotovog

alata aircrack-ng je moguće doći do dijeljene tajne.