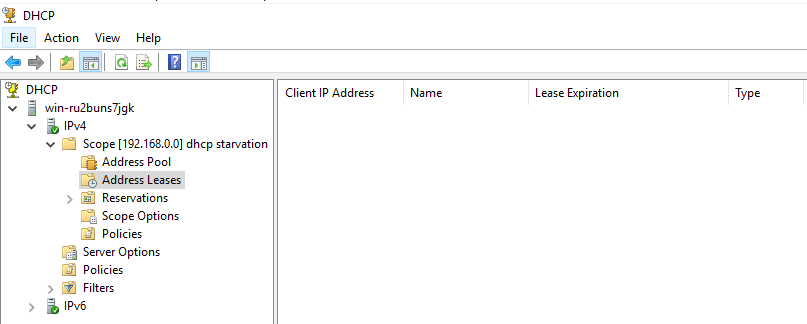
DHCP hakkerointeja on muutama erilainen, tässä käydään läpi DHCP starvation ja Rogue DHCP

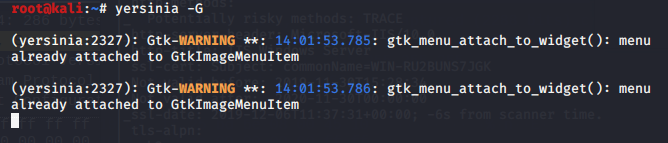
# DHCP Starvation

DHCP starvation ideana on lähettää DHCP palvelimelle niin paljon dhcp kyselyitä, että sen osoitteet loppuvat, eivätkä se voi enää jakaa oikeita osoitteita laitteille jotka niitä tarvitsevat.

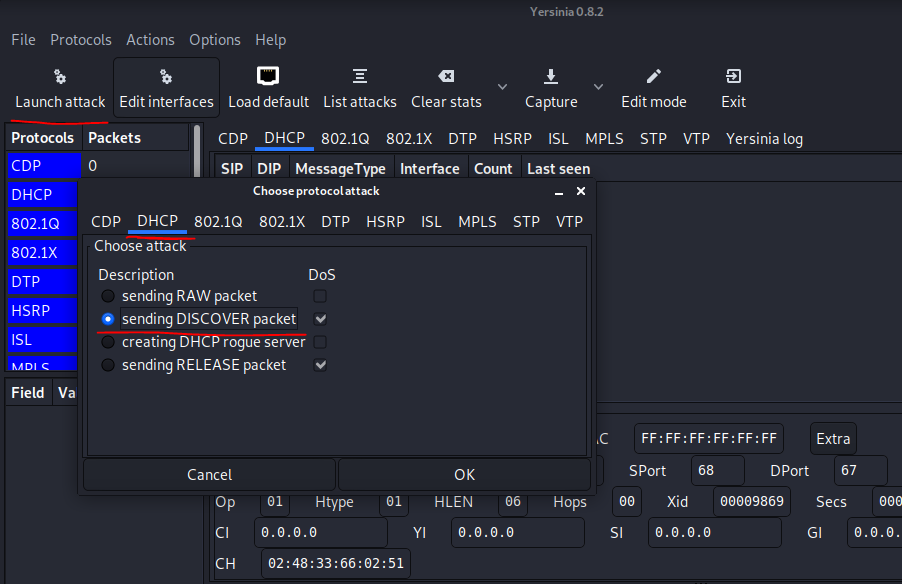
Tässä on laitettu pystyyn DHCP palvelin SRV2016 koneelle. Se jakaa osoitteita 192.168.0.50 – 192.168.0.251. Eli yhteensä 201 osoitetta.



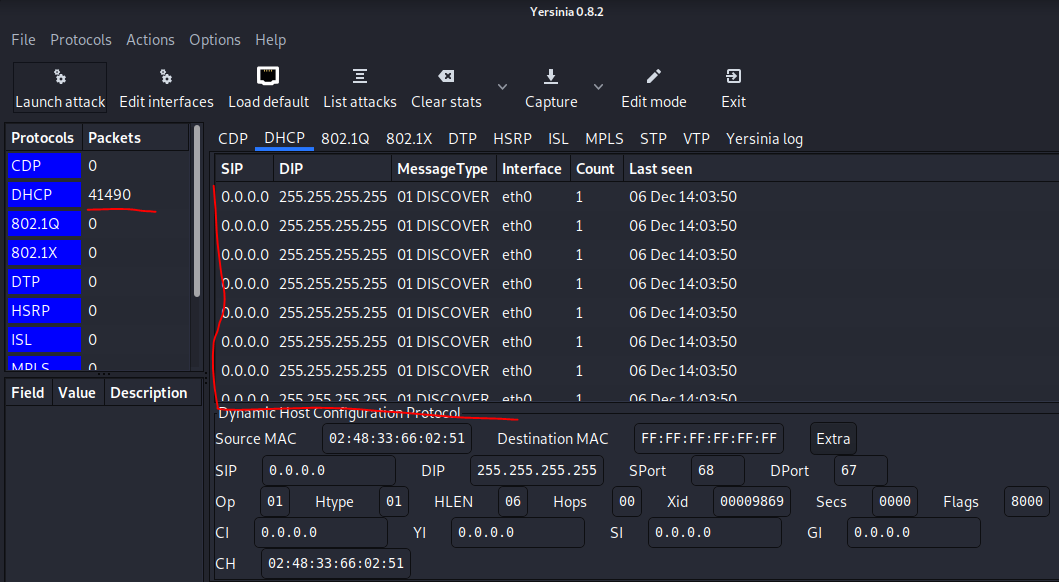
Avaa Yersinian graafinen käyttöliittymä komentoriviltä käsin.



Launch Attack > DHCP > sending DISCOVER packets > OK.



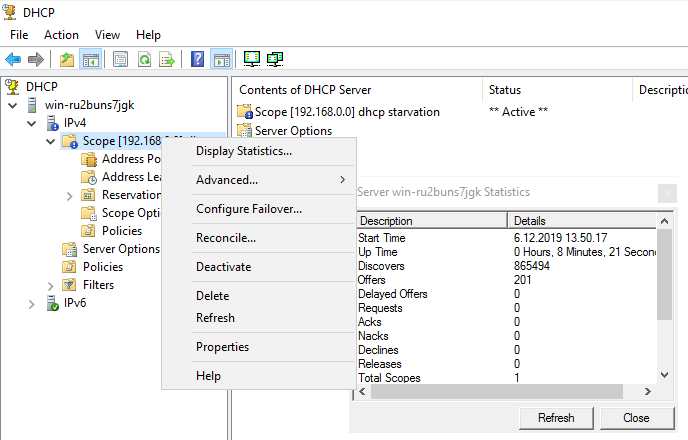
Yersinia aloittaa DHCP pyyntöjen lähettämisen verkkoon. **Yersinia lähettää DHCP pyynnöt tekaistuista MAC-osoitteista joita ei oikeasti ole olemassakaan.** Tämä kuva otettiin 5 sekuntia hyökkäyksen käynnistämisesta ja nyt jo kyselyitä on tullut 41490.



Hyökkäyksen saat lopetettua poistumalla ohjelmasta Exit napista.

Tältä hyökkäys näittäisi palvelimella. Avaa Display statistics ja näet että kyselyitä on tullut jo melkein miljoona parissa minuutissa ja kaikki 201 osoitetta on tarjottu. Ne EIVÄT näy Address leases kohdassa koska mikään Yersinian lähettämistä paketeista ei tullut oikealta laitteelta joka olisi voinut vastata palvelimelle. Jos jokin oikeasti osoitetta tarvitse pyytäisi sellaista nyt, se ei voisi sitä saada.

Huomaa myös kuinka IPv4 kohdassa on sininen huutomerkki.



# Rogue DHCP

Rogue DHCP on muun kuin verkonomistajan hallinnoima DHCP palvelin. Esim. kirjaston langattomassa verkossa voisi olla kirjaston jokin laite (reititin tai palvelin) joka jakaa asiakkaille osoitteita. Oletuksena kuitenkin mikä tahansa laite voi jakaa osoitteita verkossa.

Oikea DHCP palvelin voisi jakaa esim GW 192.168.0.1 ja DNS 192.168.0.2 jotta asiakkaat pääsevät nettiin. Vihulainen voisi laittaa pystyy omaan DHCP palvelimensa joka jakaisikin GW 192.168.0.254 ja DNS 8.9.10.11. Asiakkaat pääsisivät edelleen nettiin, mutta jaetussa 192.168.0.254 osoitteessa voisi olla mm. vihulaisen Wireshark tai muu vastaava joka näkee kaiken liikenteen joka kulkee sen läpi. Vihulaisen hallinnoimassa DNS palvelimessa taas voisi olla zone ja tietue jotka ohjaavat asiakkaan joka yrittää kirjautua pankkiinsa, jonnekin ihan muualle, mikä näyttää pankin nettisivulta mutta ei ole sitä. Sitten asiakas syöttäisi pankkitietonsa sivustolle (joka oikeasti on myös vihulaisen pystyttämä) ja saatettaisiin varastaa.

# Suojautuminen

Nämä ohjeet on tehty virtuaaliympäristössä (VirtualBox), joten DHCP starvation ja rogue DHCP suojautuminen tehdään Packet Tracer harjoituksina (samat tietenkin toimisivat myös oikeilla laitteilla ja vastaavat ominaisuudet löytyvät eri valmistajilta).

DHCP starvation hyökkäyksiä voidaan estää konfiguroimalla reitittimen työasemaportteihin port-security. Tämä toimii koska kuten edellä nähtiin, Kali linuxin Yersinia lähettää kaikki DHCP pyynnöt samalta koneelta ja kone on kytketty vain yhteen porttiin. Jos DHCP pyyntöjä tulee 41490 kappaletta muutamassa sekunnissa yhtä monesta MAC-osoitteesta, voitaisiin yksinkertaisesti määritää port-security joka sallii portin käytön vain yhdelle MAC-osoitteelle.

## Port-security

Tehdään kaikista porteista, joihin kytketään päätelaitteita (tietokoneita, puhelimia, kameroita jne) access portit ja määritetään niihin port-security

**Switch(config)#int range fa0/1-20**

**Switch(config-if-range)#switchport mode access**

**Switch(config-if-range)#switchport port-security**

**Switch(config-if-range)#switchport port-security violation shutdown**

**Switch(config-if-range)#switchport port-security maximum 1**

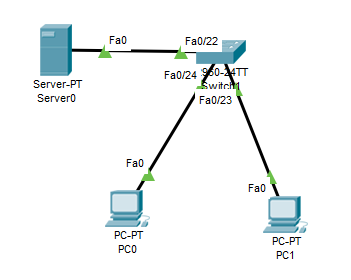
**Switch(config-if-range)#switchport port-security mac-address sticky**

## DHCP snooping

Port-security toiminto ei ehkäise Rogue DHCP ongelmaa. Sitä varten löytyy DHCP snooping toiminto, jota voi myös käyttää DHCP starvation hyökkäystä vastaan.

DHCP snooping ideana on, että verkolle määritetään sallittu DHCP palvelin/palvelimet, ja jos jokin muu DHCP palvelin yrittää jakaa osoitteita, sen ei sallita. Huomio, että dhcp snooping on vlan kohtainen, eli jos käytössäsi on useampi vlan, joudut määrittämään dhcp snooping niille kaikille.

Tässä kytkimen portiin fa0/22 kytketty DHCP palvelin sallitaan jakaa osoitteita. Jos tämä palvelin siirrettäisiin mihin tahansa muuhun porttiin, se ei enää voisi jakaa osoitteita.



**Switch(config)#ip dhcp snooping vlan 1**

**Switch(config)#int fa0/22**

**Switch(config-if)#ip dhcp snooping trust**