

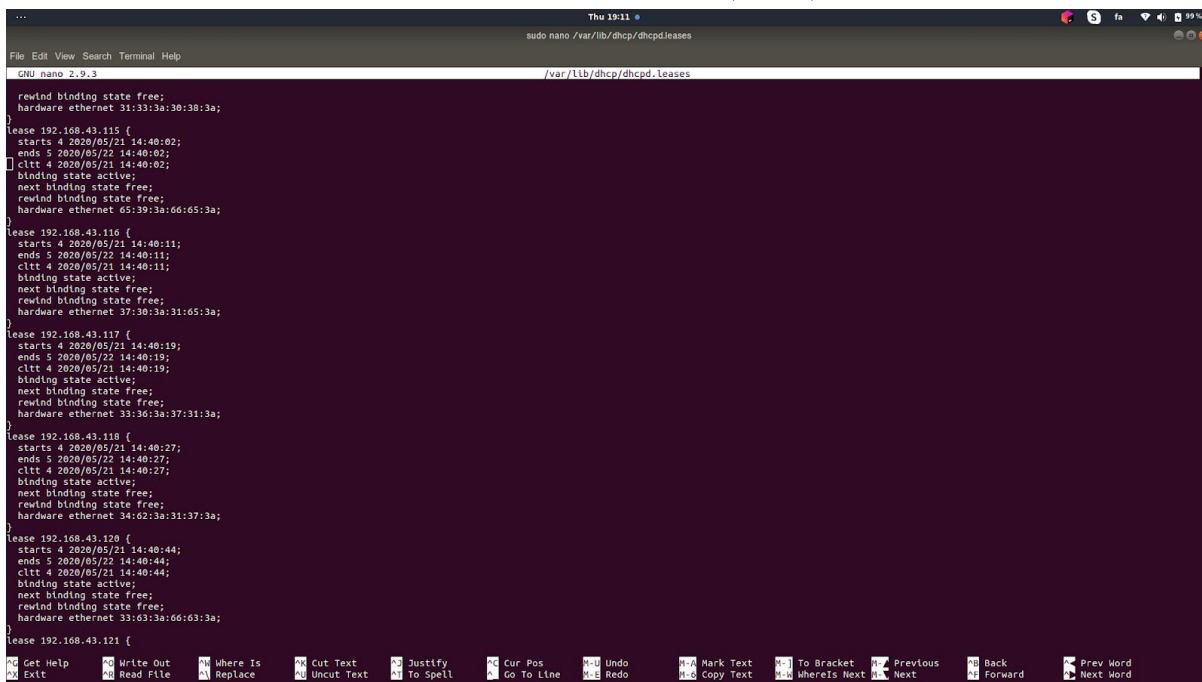
1- ابتدا طبق مراحل توضیح داده شده ics-dhcp-server را نصب کردم و فایل کانفیگ را به صورت زیر کامل کردم.

```
authoritative;

default-lease-time 86400;
max-lease-time 86400;

subnet 192.168.43.0 netmask 255.255.255.0{
    range 192.168.43.100 192.168.43.150;
    option routers 192.168.43.1;
    option domain-name-servers 192.168.43.1;
    option domain-name "local";
}
```

سپس از طریق اسکریپت ضمیمه شده که با کتابخانه scapy نوشته شده حمله را انجام دادم و نتایج زیر را در فایل var/lib/dhcp/dhcpd.lease مشاهده کردم که تمام ادرس های اختصاص داده شده:

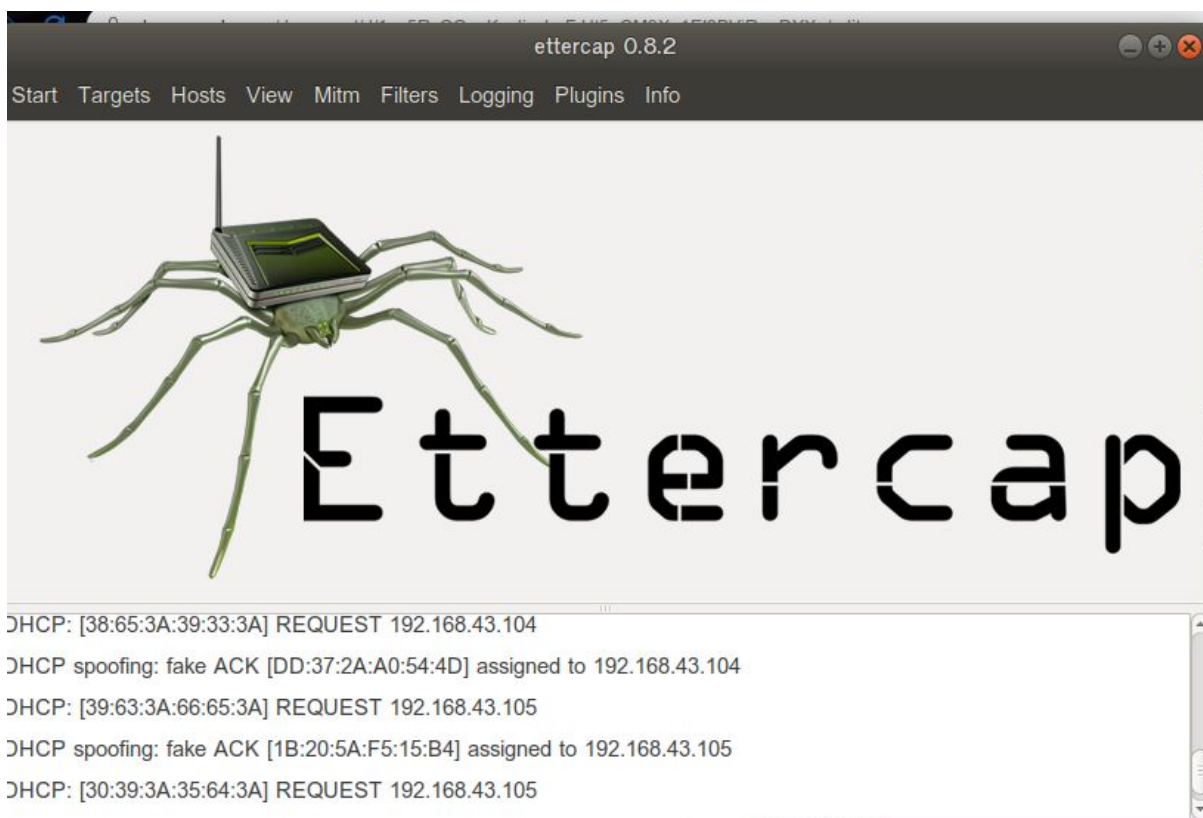


```
... Thu 19:11
sudo nano /var/lib/dhcp/dhcpd.lease
GNU nano 2.9.3 /var/lib/dhcp/dhcpd.lease

rewind binding state free;
hardware ethernet 31:33:3a:30:38:3a;
}
Lease 192.168.43.115 {
  starts 4 2020/05/21 14:40:02;
  ends 5 2020/05/22 14:40:02;
  cltt 4 2020/05/21 14:40:02;
  binding state active;
  next binding state free;
  rewind binding state free;
  hardware ethernet 65:39:3a:66:65:3a;
}
Lease 192.168.43.116 {
  starts 4 2020/05/21 14:40:11;
  ends 5 2020/05/22 14:40:11;
  cltt 4 2020/05/21 14:40:11;
  binding state active;
  next binding state free;
  rewind binding state free;
  hardware ethernet 37:30:3a:31:65:3a;
}
Lease 192.168.43.117 {
  starts 4 2020/05/21 14:40:19;
  ends 5 2020/05/22 14:40:19;
  cltt 4 2020/05/21 14:40:19;
  binding state active;
  next binding state free;
  rewind binding state free;
  hardware ethernet 33:36:3a:37:31:3a;
}
Lease 192.168.43.118 {
  starts 4 2020/05/21 14:40:27;
  ends 5 2020/05/22 14:40:27;
  cltt 4 2020/05/21 14:40:27;
  binding state active;
  next binding state free;
  rewind binding state free;
  hardware ethernet 34:62:3a:31:37:3a;
}
Lease 192.168.43.120 {
  starts 4 2020/05/21 14:40:44;
  ends 5 2020/05/22 14:40:44;
  cltt 4 2020/05/21 14:40:44;
  binding state active;
  next binding state free;
  rewind binding state free;
  hardware ethernet 33:63:3a:66:63:3a;
}
Lease 192.168.43.121 {
```

بعد از انجام کامل کد وقتی با گوشی به مودم وصل شدم ایپی نشان داده شده خارج از محدوده ایپی dhcp server بود.

2- ابتدا برنامه ettercap را اجرا کردم سپس اینترفیس مد نظر را انتخاب کردم و برنامه را در حالت mitm در حالت dhcp spoofing را انتخاب کرده و سپس ip range را برابر ip range مربوط به dhcp server قرار دادم که برابر 192.168.43.1 بود سپس سابنت 255.255.255.0 و dns سرور 8.8.8.8 قرار دادم و اسکریپت مربوط به حمله dhcp starvation را اجرا کردم و مشاهده کردم که برنامه به درستی عملیات man in the middle را انجام داده و ip fake تولید میکند.



3.1- ابتدا وارد مد config شده سپس دستور زیر را وارد میکنیم:

```
ip dhcp snooping
```

پس از آن دستور زیر را برای vlan که میخواهیم مکانیزم بر روی آن اجرا شود وارد میکنیم:

```
ip dhcp snoop vlan 10
```

سپس باید پورت متصل به سرور dhcp را وارد به عنوان اینترفیس مورد اعتماد وارد کنیم پس در مد config وارد

اینترفیس مربوطه میشویم و سپس آنرا به عنوان اینترفیس مورد اعتماد معرفی میکنیم متلا پورت 22 :

```
int g0/22
```

```
ip dhcp snooping trust
```

4.1- در این حمله از همان مکانیزمی که در دستور کار توضیح داده شده استفاده کردم به این صورت که اول کل

شبکه های موجود رو بررسی کردم.

```
mohammad@mohammad-X556UQ ~$ sudo ip route  
default via 192.168.43.200 dev wlp3s0 proto dhcp metric 20600
```

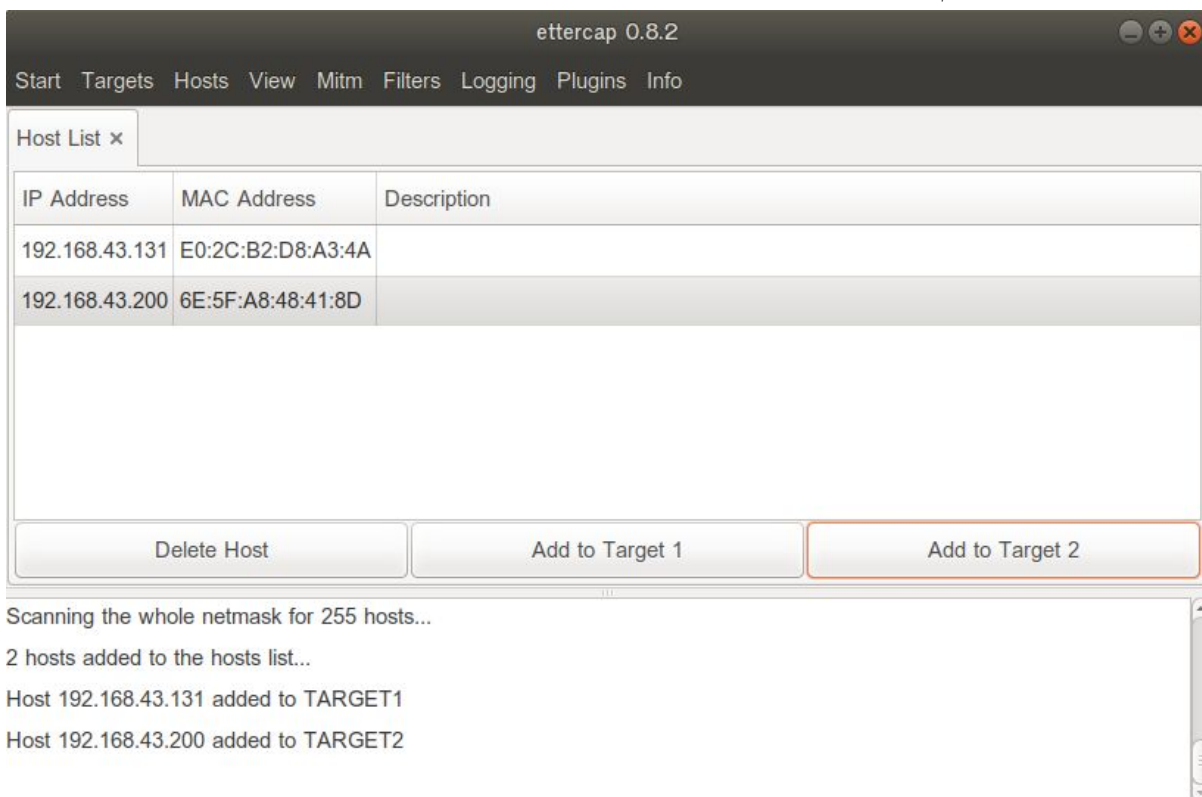
در مرحله بعدی از طریق دستور netdiscover هاست های موجود در این محدوده را بررسی کردم:

```
Thu 22:14
sudo nmapdiscover -r 192.168.43.0

File Edit View Search Terminal Help
Currently scanning: Finished! | Screen View: Unique Hosts
4 Captured ARP Req/Rep packets, from 2 hosts. Total size: 168

-----
IP           At MAC Address  Count  Len  MAC Vendor / Hostname
-----
192.168.43.200 6e:5f:a8:48:41:8d 3      126  Unknown vendor
192.168.43.131 e0:2c:b2:d8:a3:4a 1       42  Lenovo Mobile Communication (Wuhan) Company Limited
```

در مرحله بعد با استفاده از نرم افزار ettercap اقدام به انجام arp poisoning کردم به این صورت که اول هاست های موجود را شناسایی کردم



و آنها را در دو گروه قرار دادیم سپس تنظیمات مربوط به arp poisoning را انجام دادیم از منوی mitm->arp poisoning و در مرحله بعد بر روی کلید start sniffing کلیک کرده و قادر بودم که تمام ترافیک عبوری را از گوشی خودم که به روتر (مودم) متصل بود رو از طریق برنامه ببینم.

4.2. در یک تراکه نش http هدف اتصال TCP بین کلاینت و سرور است. با استفاده از تکنیک های مختلف ، مهاجم اتصال اصلی TCP را به 2 اتصال جدید تقسیم می کند ، یکی بین کلاینت و مهاجم و دیگری بین مهاجم و سرور. پس از اینکه اتصال TCP برقرار شد حمله کننده مانند یک پروکسی قادر به خواندن درج و تغییر داده ها در ارتباطات برقرار شده است. حمله MITM به دلیل ماهیت پروتکل http و انتقال داده ها که همگی مبتنی بر ASCII هستند بسیار موثر است. به این ترتیب ، امکان مشاهده و مصاحبه در پروتکل http و همچنین در داده های منتقل شده وجود دارد. بنابراین ، برای مثال ، می توانید یک کوکی جلسه را که در حال خواندن عنوان http است را هک کنید. حمله MITM همچنین می تواند از طریق اتصال https با استفاده از همان تکنیک انجام شود. تنها تفاوت در ایجاد دو session مستقل SSL است هر کدام در یک اتصال TCP. مرورگر یک ارتباط SSL با مهاجم برقرار می کند و مهاجم اتصال SSL دیگری با سرور وب برقرار می کند. به طور کلی مرورگر به کاربر هشدار می دهد که گواهی دیجیتالی استفاده شده معتبر نیست ، اما کاربر ممکن است هشدار را نادیده بگیرد زیرا او تهدید را درک نمی کند. که یکی از روش ها برای پیاده سازی این حمله میتواند با arp spoofing باشد به این صورت که در این فرایند اتصال آدرس MAC مهاجم با آدرس IP کاربر حاضر در شبکه محلی با استفاده از پیامهای جعلی ARP است. در نتیجه داده های ارسال شده توسط کاربر به آدرس IP میزبان به جای آن به مهاجم منتقل می شوند و در مرحله بعد مهاجم میتواند از طریق ssl hijacking حمله mitm را پیاده سازی کند