به نام خالق هستی بخش

راهنمای نصب و کاربری ابزار آزمون ارزیابی امنیت تجهیزات سوئیچینگ شبکه (Yersinia)

❖ مراحل نصب Yersinia در کالی لینوکس

1) git clone https://github.com/tomac/yersinia /opt/yersinia
2) cd /opt/yersinia
3) apt install autoconf libgtk-3-dev libnet-dev libgtk2.0-dev
4) sudo apt-get -y install pcapfix
5) apt-get install libpcap-dev
6) /.autogen.sh
7) make && make install
8) /.configure
9) sudo yersinia –I # Interactive mode for yersinia

#Enjoy Yersinia In Graphical modes

❖ Dependency / وابستگی ها

yersinia have the following dependencies:

libatk1.0-0
libc6
libgdk-pixbuf2.0-0
libglib2.0-0
libgtk2.0-0
libncurses6
libnet1
libpango-1.0-0
libpcap0.8
libtinfo6

یک بار هر کدام از پکیج های فوق را با دستور Apt install –y package-name پس از انجام مراحل نصب Yersinia که در بالا ذکر شده است نصب نمایید:

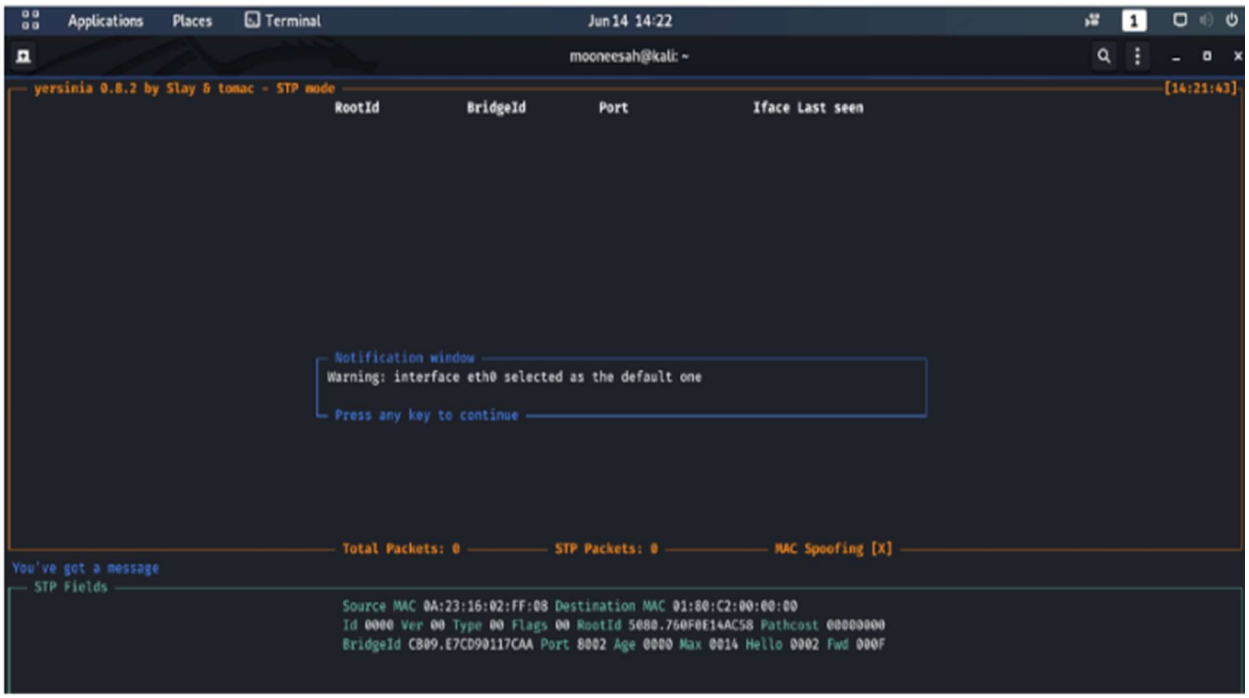
Apt install –y libatk1.0-0
Apt install –y libc6
Apt install –y libgdk-pixbuf2.0-0
Apt install –y libglib2.0-0
Apt install –y libgtk2.0-0
Apt install –y libncurses6
Apt install –y libnet1
Apt install –y libpango-1.0-0
Apt install –y libpcap0.8
Apt install –y libtinfo6

اکنون ابزار Yersinia آماده استفاده در محیط Interactive است

❖ **راهنمای کاربری Yersinia در محیط Interactive :**

با دستور Yersinia -I وارد محیط Interactive ابزار Yersinia شوید:

root㉿ kali)-[~] Yersinia –I



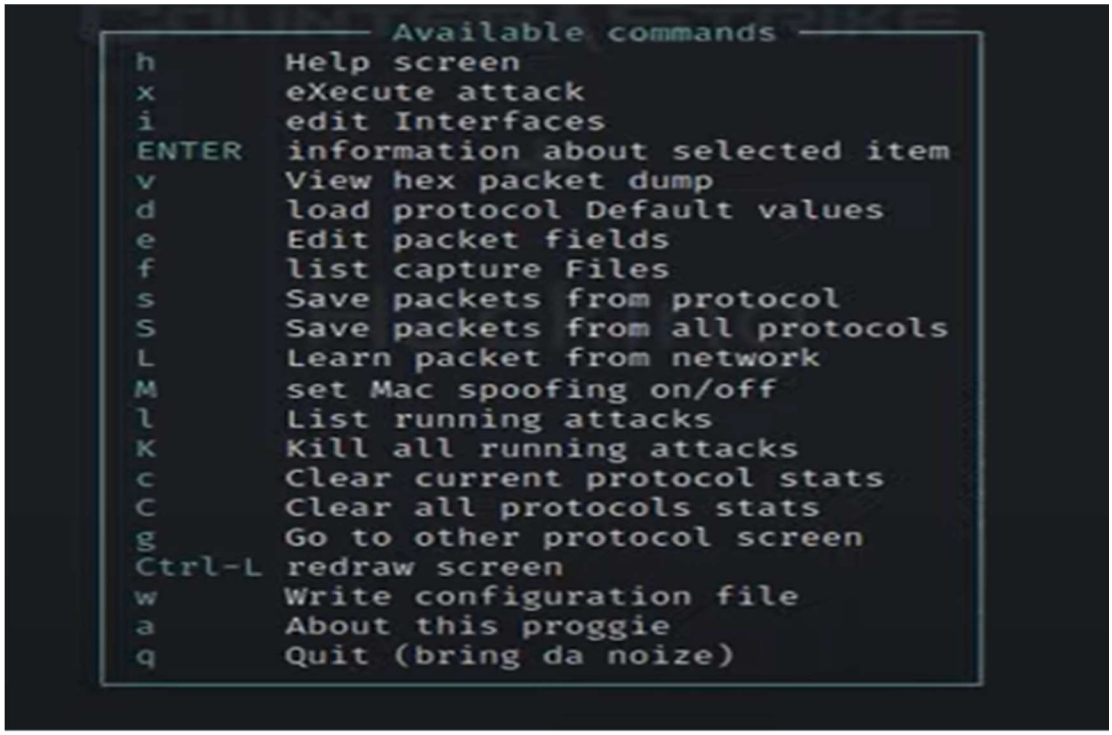
۱- در ابتدا گزینه انتخاب اولین کارت شبکه فعال که معمولا با eth0 نمایش داده می شود ظاهر می شود که با زدن یک کلید ضمن انتخاب این اینترفیس وارد محیط اصلی Interactive Yersinia می شویم.

۲- پس از آن می توان با زدن دکمه های زیر پروتوکل مد نظر را برای انجام تست ارزیابی امنیت انتخاب نماییم:

- ✓ با زدن دکمه F1 می توان وارد مد پروتوکل CDP شویم
- ✓ با زدن دکمه F2 می توان وارد مد پروتوکل DHCP شویم
- ✓ با زدن دکمه F3 می توان وارد مد پروتوکل 802.1Q شویم
- ✓ با زدن دکمه F4 می توان وارد مد پروتوکل 802.1X شویم
- ✓ با زدن دکمه F5 می توان وارد مد پروتوکل DTP شویم
- ✓ با زدن دکمه F6 می توان وارد مد پروتوکل HSRP شویم
- ✓ با زدن دکمه F7 می توان وارد مد پروتوکل ISL شویم

- ✓ با زدن دکمه F8 می توان وارد مد پروتوکل MPLS شویم
- ✓ با زدن دکمه F9 می توان وارد مد پروتوکل STP شویم
- ✓ با زدن دکمه F10 می توان وارد مد پروتوکل VTP شویم
- ✓ با زدن دکمه F11 می توان صفحه را Full Screen نمود و با زدن مجدد آن صفحه به حالت قبل باز می گردد

۳- پس از انتخاب مد پروتوکل مد نظر اکنون با زدن دکمه h در این محیط، راهنمای جدول امکانات هر پروتوکل باز می‌گردد. لازم به توضیح است نمایش این منو تنها برای مشاهده گزینه‌ها و کلیدهای Short-Cut اجرای هر گزینه می‌باشد و هنگام مشاهده این جدول راهنما، امکان اجرای گزینه‌ها میسر نیست و با زدن دکمه q می توان از این منو خارج و به مد پروتوکل بازگردیم.



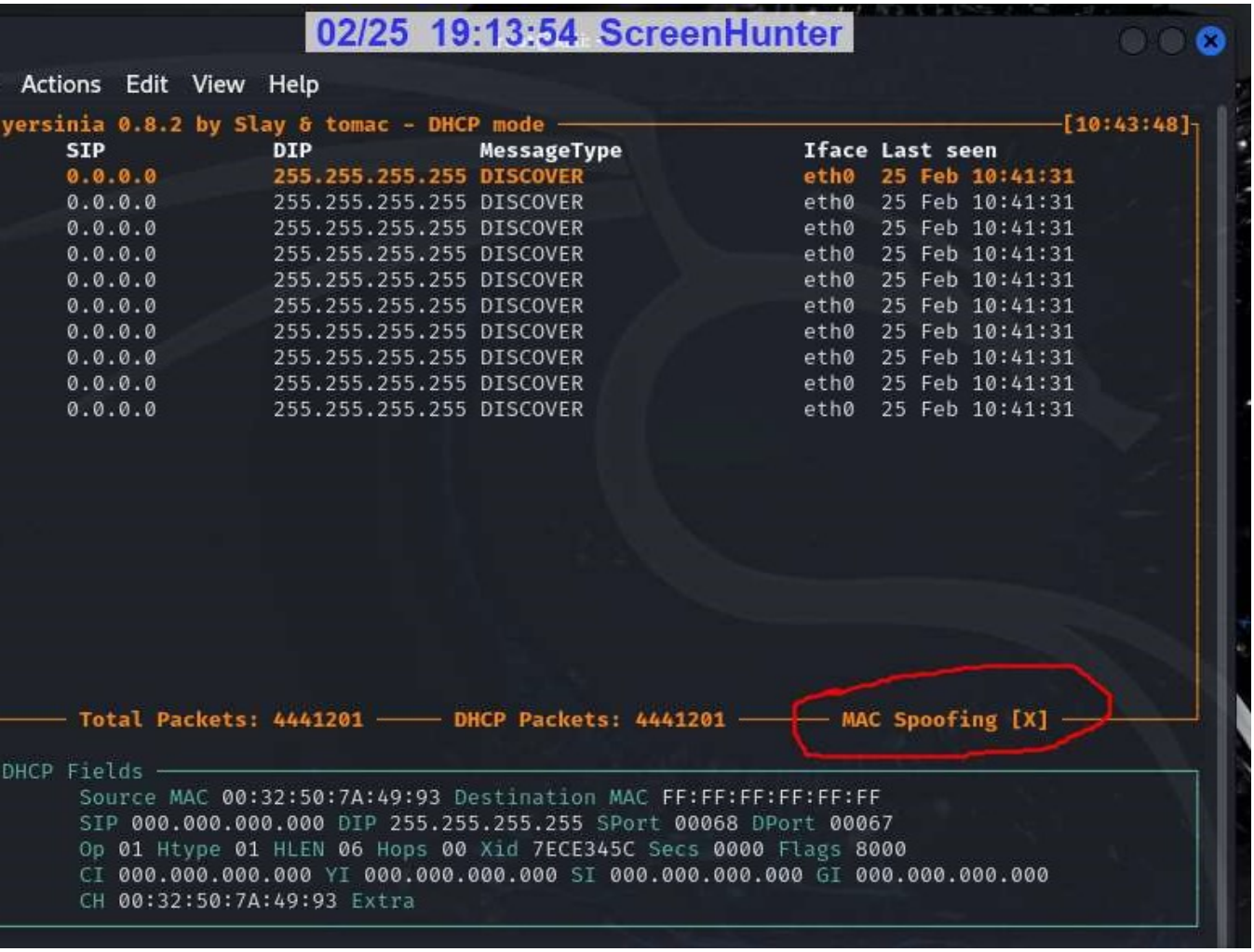
۴- در مد هر پروتوکل :

a) با زدن دکمه x می توان وارد منوی تست نفوذ و اجرای گزینه‌ها شد
b) پس از اجرای هر تست می‌توان با زدن دکمه v پکت‌ها را مشاهده نمود
c) با زدن دکمه i می‌توان وارد منوی انتخاب کارت شبکه‌ها شد و اینترفیس مورد نظر را انتخاب نمود
d) با زدن دکمه d می‌توان مقادیر پیش فرض هر پروتوکل را انتخاب نمود و فیلدها به مقادیر پیش فرض بر می گردند
e) دکمه‌های s برای ذخیره سازی پکت‌های یک پروتوکل و S برای ذخیره سازی پکت‌های همه پروتوکل‌ها در صورت اجرای همزمان چند تست مورد استفاده قرار می‌گیرد
f) دکمه e برای ویرایش فیلدهای پکت ها می‌باشد به عنوان مثال در مد پروتوکل DHCP با زدن این دکمه منوی زیر پنجره اصلی جهت تغییر .. ,Source MAC , Destination MAC فعال و می‌توان مقادیر این فیلدها را

بر اساس نیاز تغییر داد. پس از تایپ مقادیر جدید می توان با ۲ بار زدن کلید e از مد ویرایش فیلدها خارج شویم

g) با زدن دکمه f می‌توان لیست فایل‌های capture شده پکت‌ها را مشاهده نمود

h) با زدکن M می‌توان قابلیت MAC Spoofing را فعال و یا غیرفعال نمود. نتیجه کار در گزینه MAC Spoofing در کادر زیر پنجره اصلی قابل مشاهده است



```
yersinia 0.8.2 by Slay & tomac - DHCP mode ─────────────────────────────[10:43:48]┐
      SIP              DIP             MessageType               Iface Last seen
      0.0.0.0          255.255.255.255 DISCOVER                  eth0  25 Feb 10:41:31
      0.0.0.0          255.255.255.255 DISCOVER                  eth0  25 Feb 10:41:31
      0.0.0.0          255.255.255.255 DISCOVER                  eth0  25 Feb 10:41:31
      0.0.0.0          255.255.255.255 DISCOVER                  eth0  25 Feb 10:41:31
      0.0.0.0          255.255.255.255 DISCOVER                  eth0  25 Feb 10:41:31
      0.0.0.0          255.255.255.255 DISCOVER                  eth0  25 Feb 10:41:31
      0.0.0.0          255.255.255.255 DISCOVER                  eth0  25 Feb 10:41:31
      0.0.0.0          255.255.255.255 DISCOVER                  eth0  25 Feb 10:41:31
      0.0.0.0          255.255.255.255 DISCOVER                  eth0  25 Feb 10:41:31
      0.0.0.0          255.255.255.255 DISCOVER                  eth0  25 Feb 10:41:31

───── Total Packets: 4441201 ──── DHCP Packets: 4441201 ──── MAC Spoofing [X] ─────┘
DHCP Fields ─────────────────────────────────────────────────────────────────────
      Source MAC 00:32:50:7A:49:93 Destination MAC FF:FF:FF:FF:FF:FF
      SIP 000.000.000.000 DIP 255.255.255.255 SPort 00068 DPort 00067
      Op 01 Htype 01 HLEN 06 Hops 00 Xid 7ECE345C Secs 0000 Flags 8000
      CI 000.000.000.000 YI 000.000.000.000 SI 000.000.000.000 GI 000.000.000.000
      CH 00:32:50:7A:49:93 Extra
```

i) با زدن دکمه l (L کوچک) می‌توان لیست تست‌های اجرا شده را مشاهده نمود. برای خروج از دکمه q استفاده شود زیرا با زدن دکمه Enter تست متوقف می‌شود. در صورت اجرای همزمان چند تست می توان با دکمه‌های اشاره گر بالا و پایین، گزینه مد نظر را انتخاب و با زدن دکمه Enter آن را قطع نمود. برای خروج می‌توان از دکمه q استفاده کرد

j) با زدن دکمه k می‌توان تمامی تست ها را متوقف نمود

k) با زدن دکمه c می‌توان وضعیت صفحه پروتوکل را پاک نمود و لیست پکت‌های جدید را مشاهده کرد

l) با زدن دکمه C صفحه وضعیت همه پروتوکل‌های در حال تست پاک می‌شود

m) با زدن دکمه g می‌توان صفحه لیست پروتوکل‌ها را مشاهده نمود و به جای استفاده از دکمه‌های F2 و F3 و .. از این صفحه برای انتخاب مد پروتوکل‌ها استفاده کرد

n) با زدن دکمه a می‌توان اطلاعاتی از این نسخه مشاهده کرد

o) با زدن دکمه q هم از برنامه Yersinia Interactive خارج می‌شوید

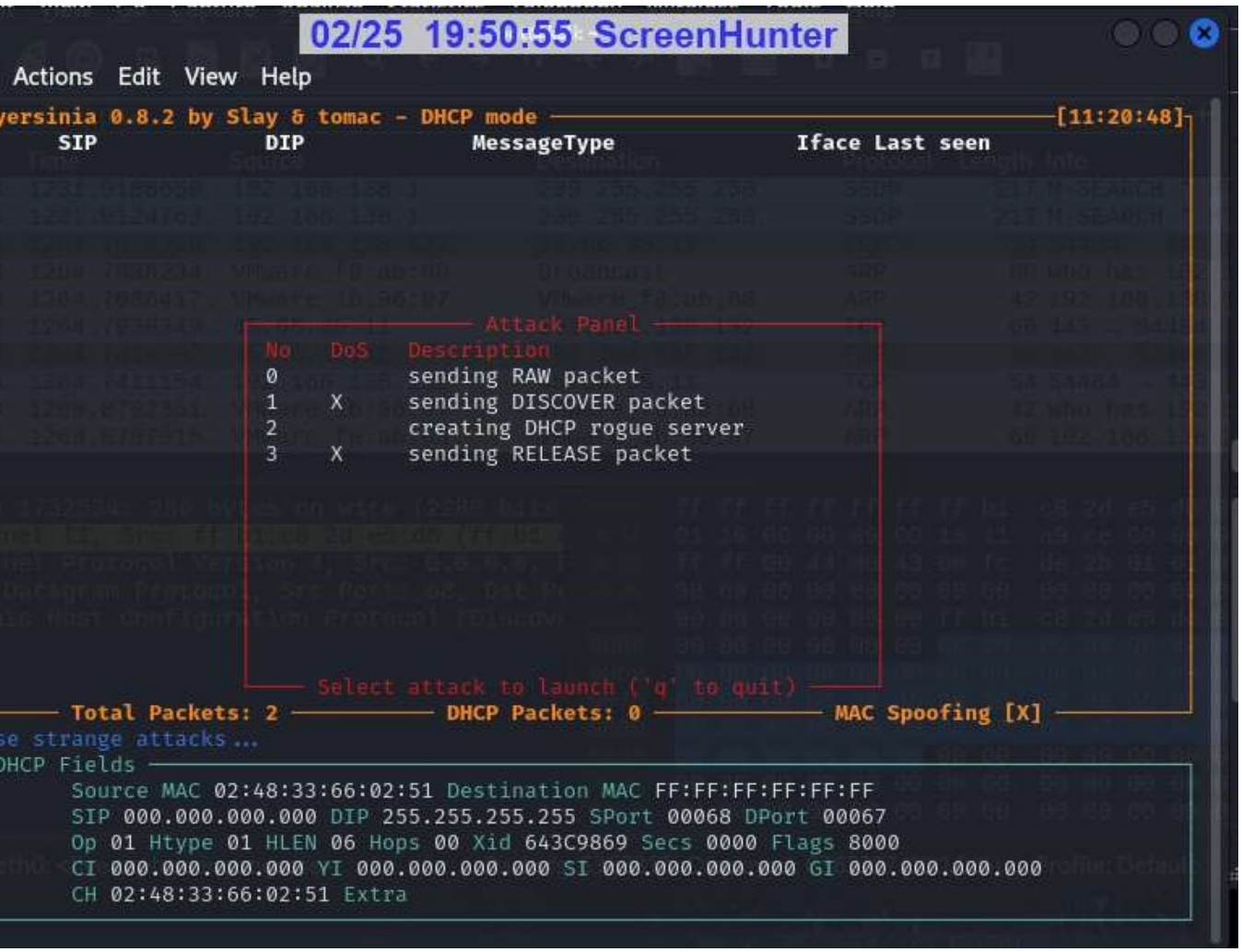
۵– مثال هایی از اجرای دستورات و تست های نفوذ در مد Interactive

❖ DHCP PenTEST

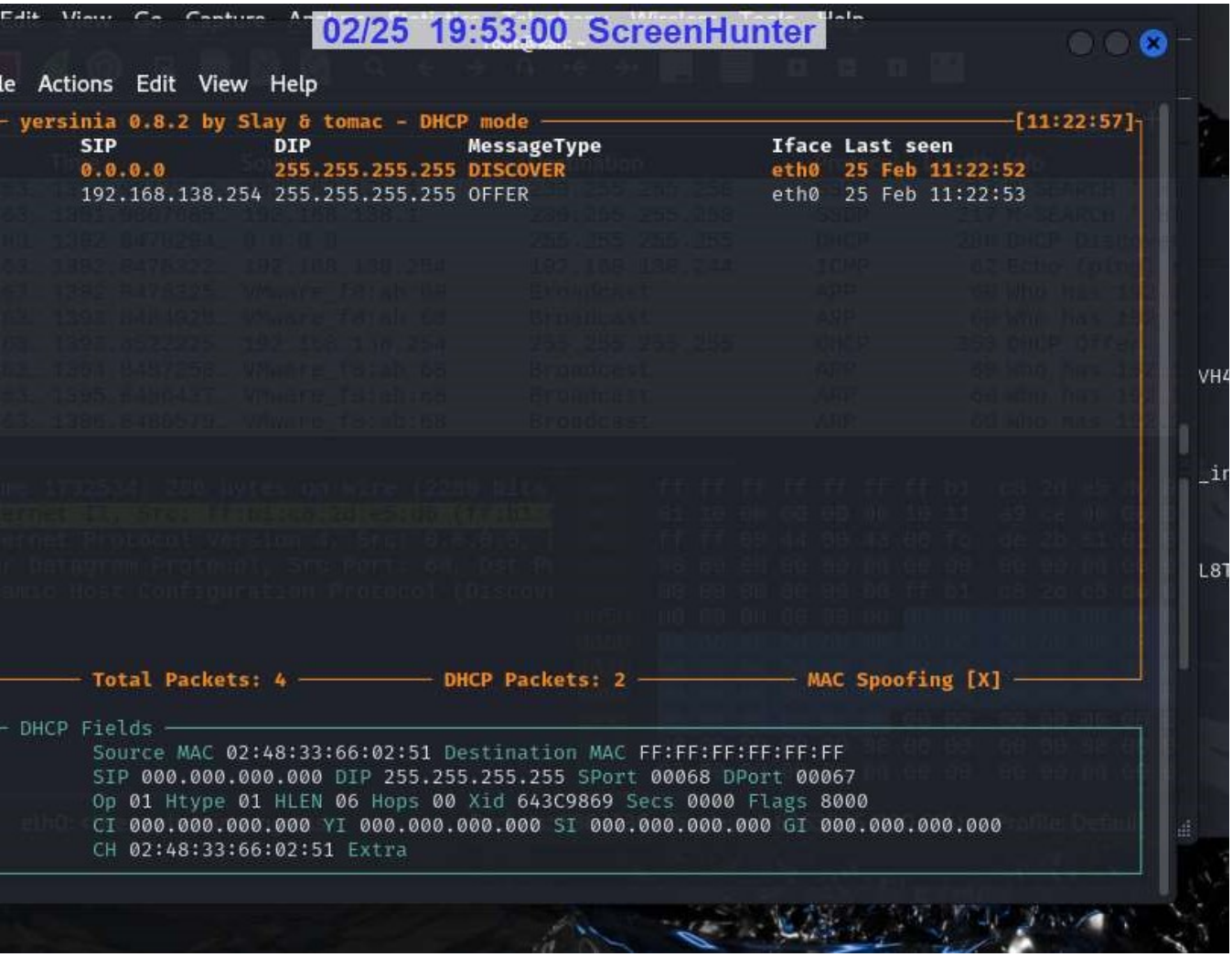
ابتدا با زدن گزینه F2 وارد مد پروتوکل DHCP می‌شویم . قبل از انجام تست در یک ترمینال دیگر با اجرای دستور زیر برنامه Wireshark را انتخاب نموده اینترفیس ورودی را برای Capture روی eth0 تنظیم نموده و اماده دریافت پکت‌ها می‌شویم

root㉿ kali)-[~] wireshark

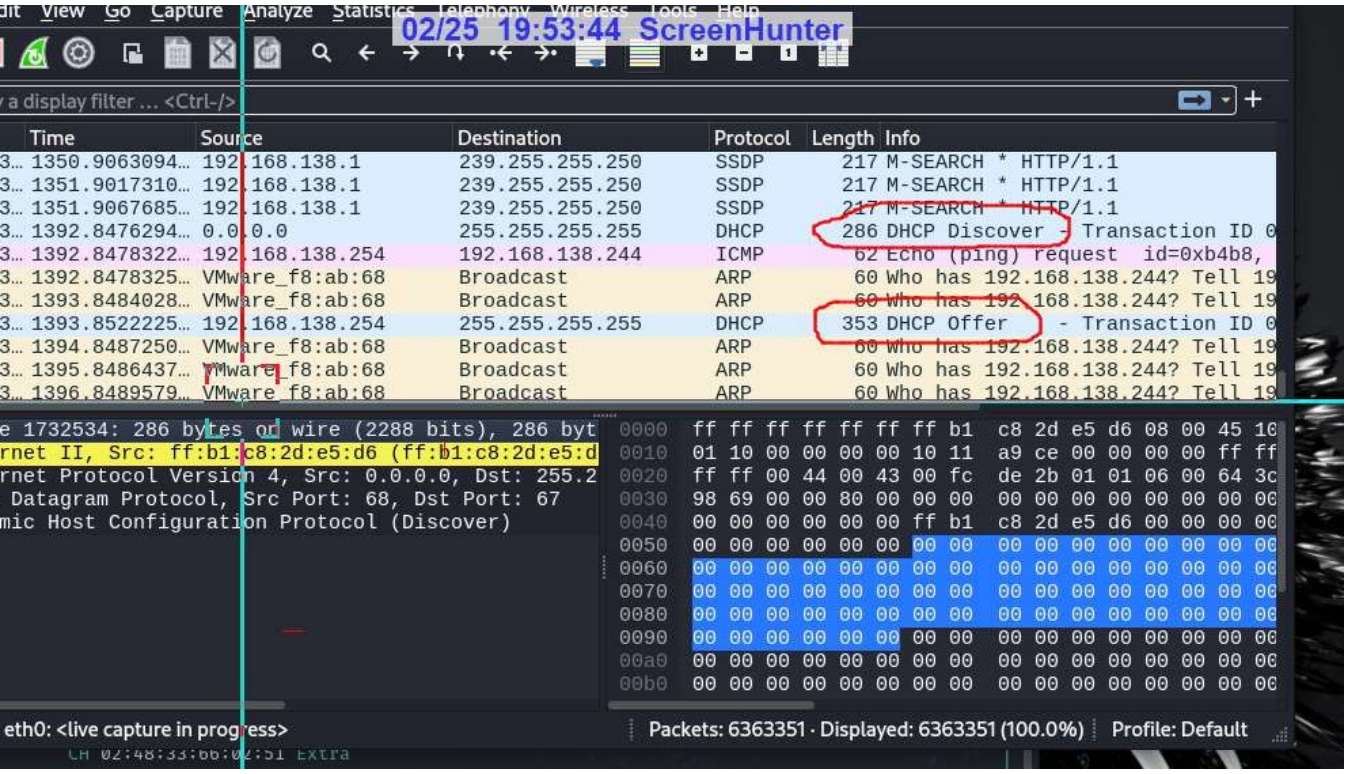
سپس در ترمینال Yersinia با زدن دکمه x منوی گزینه ها را انتخاب می کنیم



اکنون با زدکن دکمه ۰ می توان sending RAW packet را برای دریافت اطلاعات اولیه از DHCP Server اجرا کنیم. در پنجره status مربوط به پروتوکل هم می‌توان پکت‌های ارسال و دریافت شده را مشاهده نمود



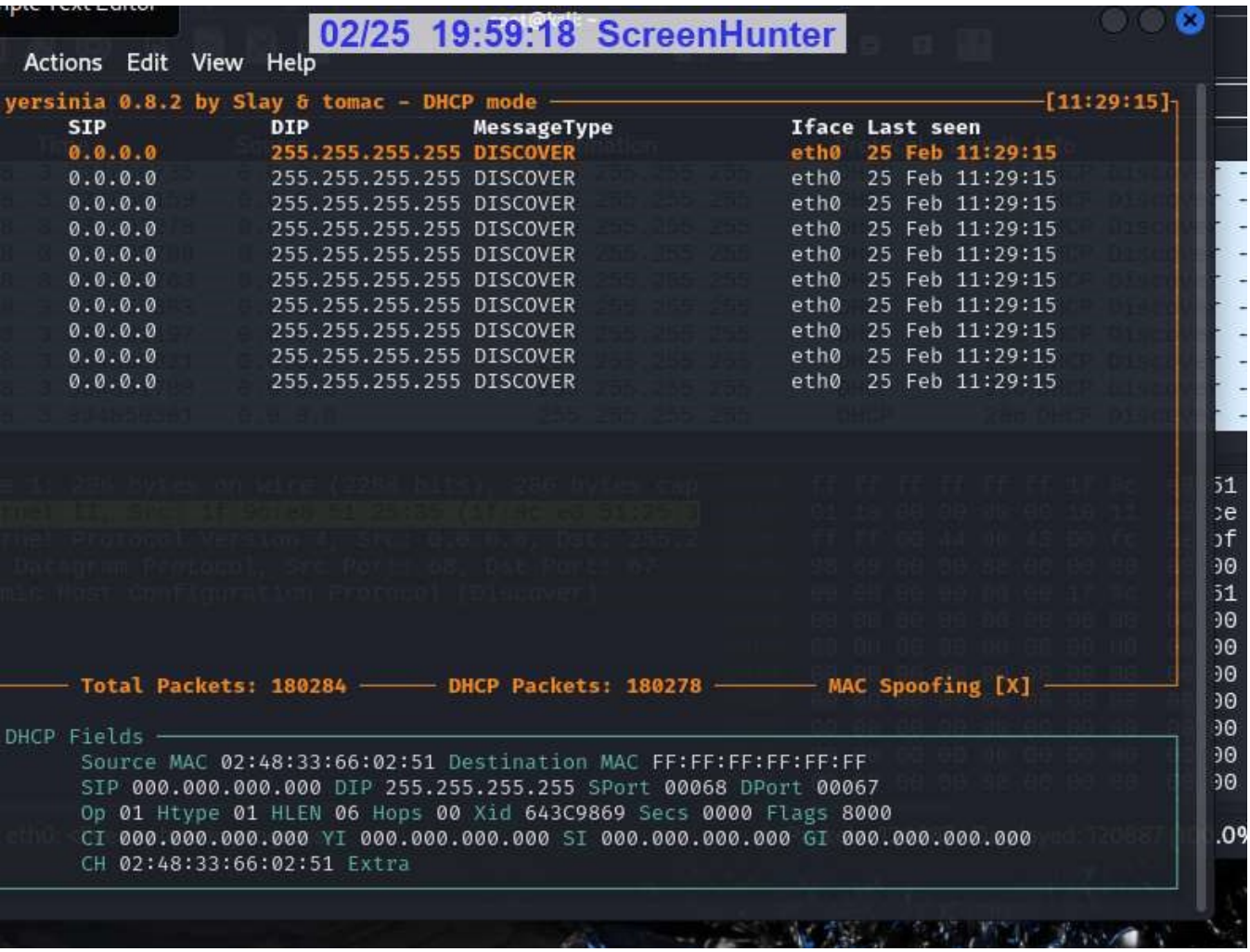
سپس در پنجره وایرشارک می توان پکت‌های DHCP Discovery و DHCP Offer را که با اجرای sending RAW packet ارسال و دریافت شده است را مشاهده نمود



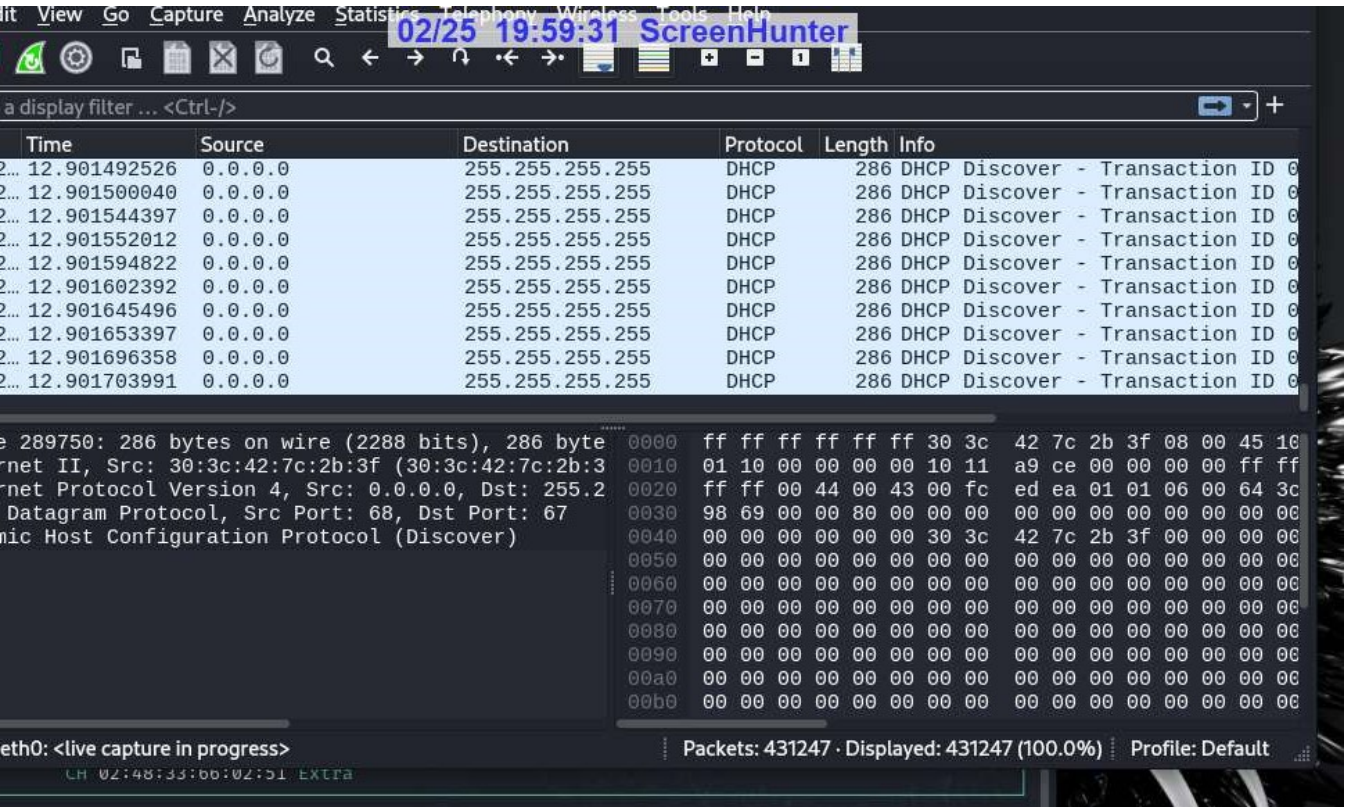
```
  Time              Source            Destination       Protocol Length Info
3… 1350.9063094…  192.168.138.1     239.255.255.250   SSDP      217 M-SEARCH * HTTP/1.1
3… 1351.9017310…  192.168.138.1     239.255.255.250   SSDP      217 M-SEARCH * HTTP/1.1
3… 1351.9067685…  192.168.138.1     239.255.255.250   SSDP      217 M-SEARCH * HTTP/1.1
3… 1392.8476294…  0.0.0.0           255.255.255.255   DHCP      286 DHCP Discover - Transaction ID 0
3… 1392.8478322…  192.168.138.254   192.168.138.244   ICMP       62 Echo (ping) request  id=0xb4b8,
3… 1392.8478325…  VMware_f8:ab:68   Broadcast         ARP        60 Who has 192.168.138.244? Tell 19
3… 1393.8484028…  VMware_f8:ab:68   Broadcast         ARP        60 Who has 192.168.138.244? Tell 19
3… 1393.8522225…  192.168.138.254   255.255.255.255   DHCP      353 DHCP Offer    - Transaction ID 0
3… 1394.8487250…  VMware_f8:ab:68   Broadcast         ARP        60 Who has 192.168.138.244? Tell 19
3… 1395.8486437…  VMware_f8:ab:68   Broadcast         ARP        60 Who has 192.168.138.244? Tell 19
3… 1396.8489579…  VMware_f8:ab:68   Broadcast         ARP        60 Who has 192.168.138.244? Tell 19
```

```
e 1732534: 286 bytes on wire (2288 bits), 286 byt   0000  ff ff ff ff ff ff ff b1  c8 2d e5 d6 08 00 45 10
rnet II, Src: ff:b1:c8:2d:e5:d6 (ff:b1:c8:2d:e5:d   0010  01 10 00 00 00 00 10 11  a9 ce 00 00 00 00 ff ff
rnet Protocol Version 4, Src: 0.0.0.0, Dst: 255.2   0020  ff ff 00 44 00 43 00 fc  de 2b 01 01 06 00 64 3c
 Datagram Protocol, Src Port: 68, Dst Port: 67      0030  98 69 00 00 80 00 00 00  00 00 00 00 00 00 00 00
mic Host Configuration Protocol (Discover)          0040  00 00 00 00 00 00 ff b1  c8 2d e5 d6 00 00 00 00
                                                    0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
                                                    0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
                                                    0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
                                                    0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
                                                    0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
                                                    00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
                                                    00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
eth0: <live capture in progress>     Packets: 6363351 · Displayed: 6363351 (100.0%)   Profile: Default
```

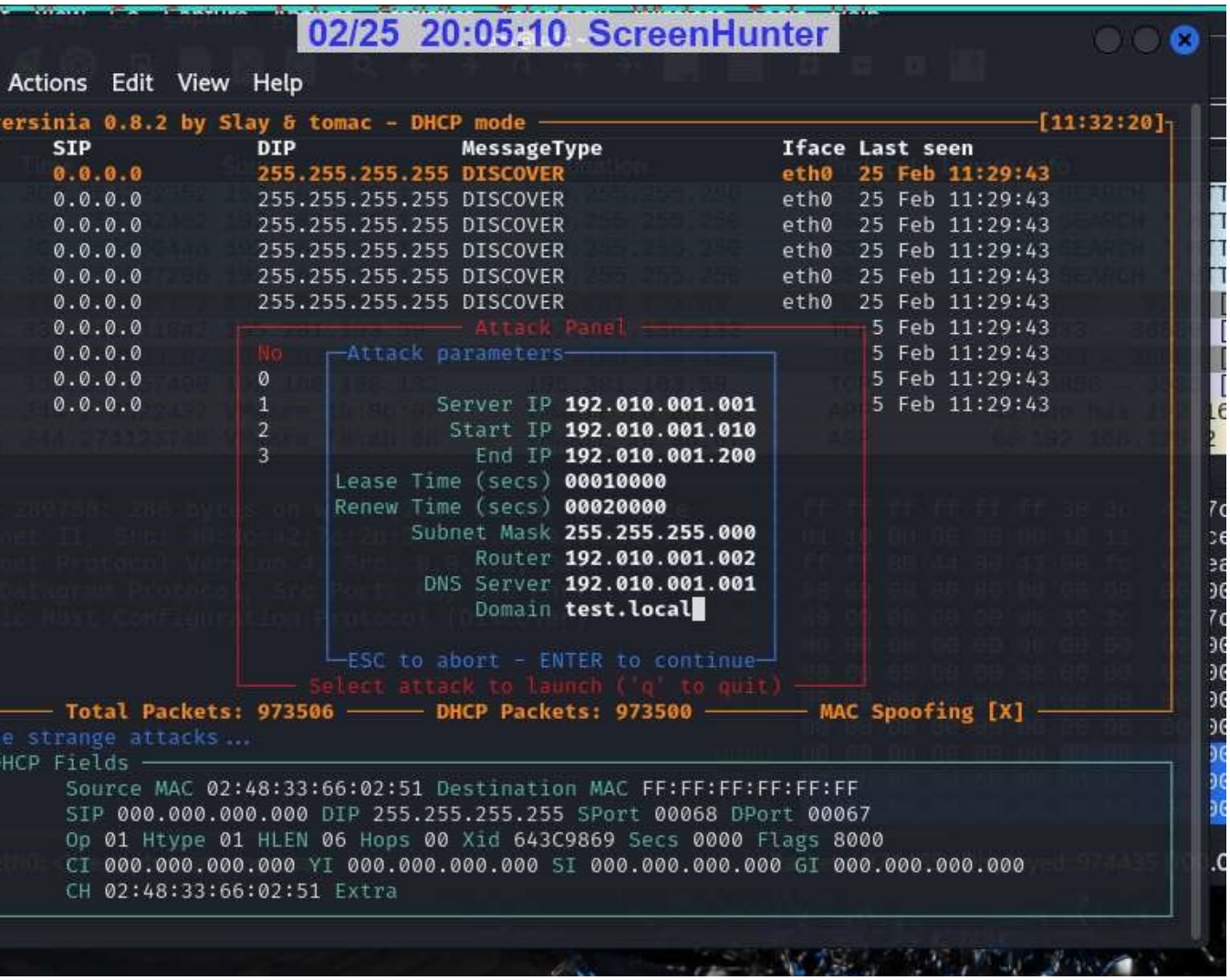
برای اجرای تست DHCP Discovery با زدن گزینه x و سپس دکمه ۱ می‌توان تست را اجرا نمود. وضعیت پکت‌های ارسالی در وایرشارک قابل مشاهده است



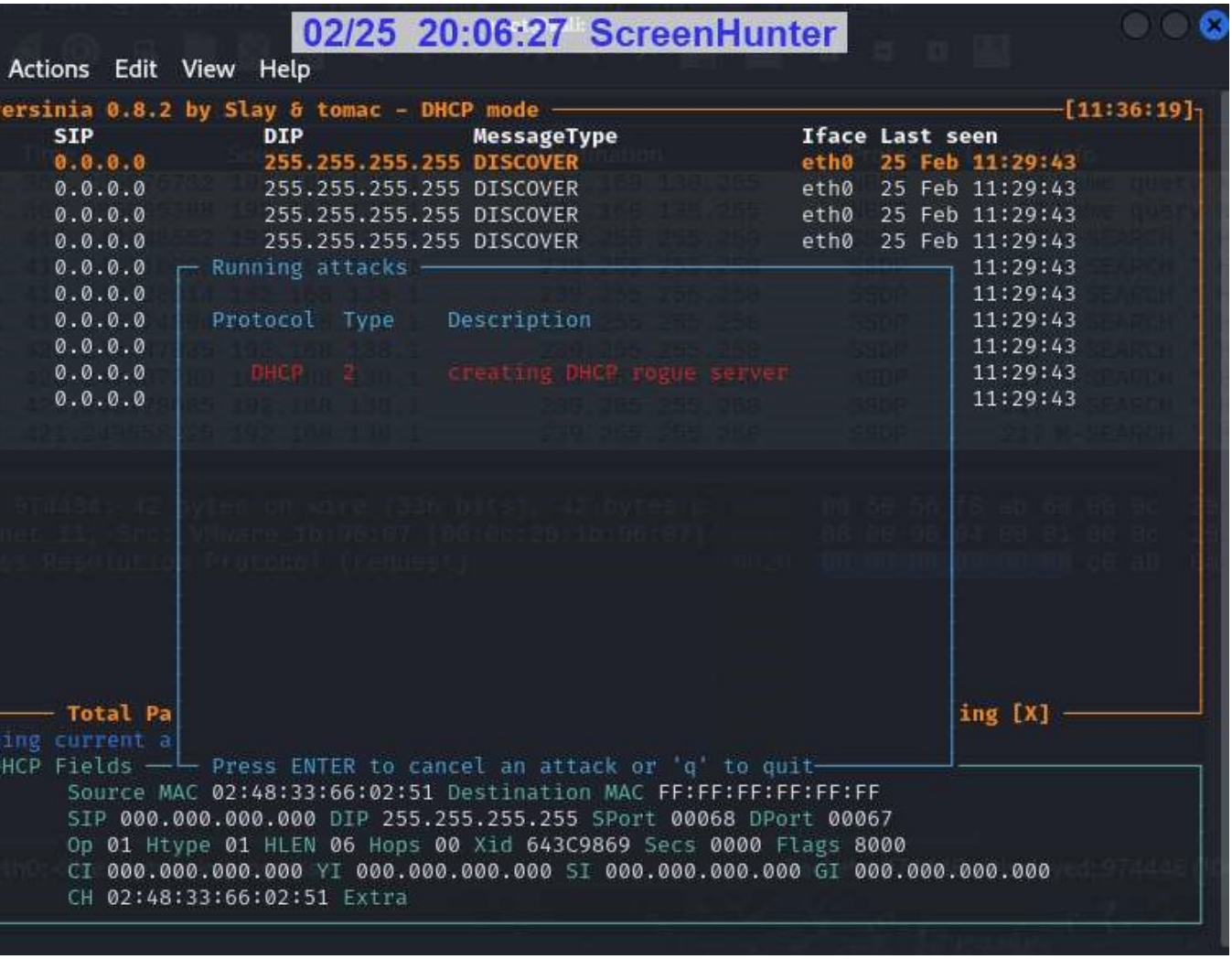
```
yersinia 0.8.2 by Slay & tomac - DHCP mode ------------------------------------[11:29:15]
     SIP            DIP            MessageType                  Iface Last seen
     0.0.0.0        255.255.255.255 DISCOVER                    eth0  25 Feb 11:29:15
     0.0.0.0        255.255.255.255 DISCOVER                    eth0  25 Feb 11:29:15
     0.0.0.0        255.255.255.255 DISCOVER                    eth0  25 Feb 11:29:15
     0.0.0.0        255.255.255.255 DISCOVER                    eth0  25 Feb 11:29:15
     0.0.0.0        255.255.255.255 DISCOVER                    eth0  25 Feb 11:29:15
     0.0.0.0        255.255.255.255 DISCOVER                    eth0  25 Feb 11:29:15
     0.0.0.0        255.255.255.255 DISCOVER                    eth0  25 Feb 11:29:15
     0.0.0.0        255.255.255.255 DISCOVER                    eth0  25 Feb 11:29:15
     0.0.0.0        255.255.255.255 DISCOVER                    eth0  25 Feb 11:29:15
     0.0.0.0        255.255.255.255 DISCOVER                    eth0  25 Feb 11:29:15

----- Total Packets: 180284 ------ DHCP Packets: 180278 ------ MAC Spoofing [X] -------
DHCP Fields
      Source MAC 02:48:33:66:02:51 Destination MAC FF:FF:FF:FF:FF:FF
      SIP 000.000.000.000 DIP 255.255.255.255 SPort 00068 DPort 00067
      Op 01 Htype 01 HLEN 06 Hops 00 Xid 643C9869 Secs 0000 Flags 8000
      CI 000.000.000.000 YI 000.000.000.000 SI 000.000.000.000 GI 000.000.000.000
      CH 02:48:33:66:02:51 Extra
```



برای اجرای تست DHCP Rogue Server با زدن دکمه x صفحه منوی گزینه های DHCP و سپس دکمه ۲ را فشار دهید تا صفحه زیر باز شود سپس با تکمیل فیلدهای نمایش داده شده و تعیین بازه آدرس دهی و سایر فیلدها دستور را اجرا می نماییم



پس از اجرای تست با زدن دکمه I می توان در صفحه لیست تست ها ، از اجرای موفق آن اطمینان حاصل نمود و سپس با تنظیم کارت شبکه یک سیستم بر روی دریافت IP Address به شکل اتوماتیک آن را تست نمود



❖ سایر تست‌ها نیز به همین شکل قابل اجرا می‌باشد

۶– راهنمای کاربری Yersinia در مد Command line :