Yersinia is a network tool designed to take advantage of some weakness in different network protocols. It pretends to be a solid framework for analyzing and testing the deployed networks and systems.

It consists of various layer-2 attacks exploiting the weaknesses of different layer-2 protocols. Thus a pentester can identify the vulnerabilities in the deep layer 2 of the network. During pentests, yersinia is used to initiate attacks on layer-2 devices like switches, dhcp servers spanning tree protocols etc. Currently yersinia supports :

- Spanning Tree Protocol (STP)
- Cisco Discovery Protocol (CDP)
- Dynamic Trunking Protocol (DTP)
- Dynamic Host Configuration Protocol (DHCP)
- Hot Standby Router Protocol (HSRP)
- IEEE 802.1Q
- IEEE 802.1X
- Inter-Switch Link Protocol (ISL)
- VLAN Trunking Protocol (VTP)

Yersinia Homepage: http://www.yersinia.net/

WARNING !!! Some of the modes in Yersinia creates a Denial Of Service(DOS). Be Careful ! Use only on a test network or with a prior permission.

Options

```
-h, --help              Help screen.
-V, --Version           Program version.
-G                      Start a graphical GTK session.
-I, --interactive       Start an interactive ncurses session.
-D, --daemon            Start the network listener for remote
admin  (Cisco  CLI  emulation).
-d                      Enable debug messages.
-l logfile              Save the current session to the file logfile. If
logfile exists, the data will be appended at the end.

-c conffile             Read/write configuration variables from/to conffile.
-M                      Disable MAC spoofing.
```

GTK GUI

```
      The  GTK GUI (-G) is a GTK graphical interface with all of the
yersinia powerful features and a professional 'look and feel'.
```

NCURSES GUI

```
       The ncurses GUI (-I) is a ncurses (or curses) based
console  where  the user can take advantage of yersinia powerful features.
 Press 'h' to display the Help Screen and enjoy your session :)
```

NETWORK DAEMON

```
       The  Network Daemon (-D) is a telnet based server (ala Cisco mode)
that listens by default in port 12000/tcp waiting for
incoming  telnet  connections. It supports  a  CLI  similar  to  a  Cisco
device where the user (once authenticated) can display different settings
and  can  launch  attacks without  having yersinia  running in her own
machine (especially useful Windows users).
```

Yersinia Home page : http://www.yersinia.net/

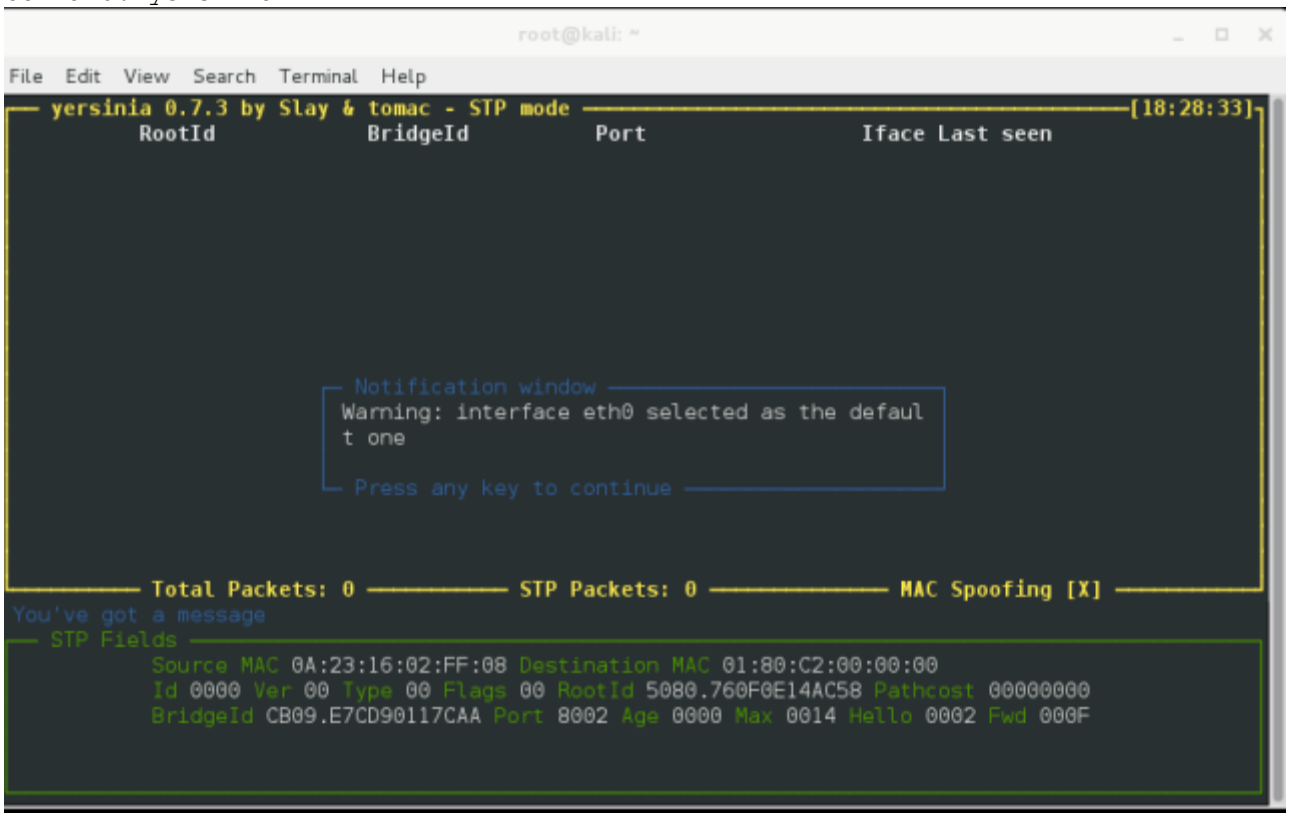
Lab 1 : DHCP Salvation using Yersinia NCurses mode

In this lab we flood the dhcp server with dhcp discover packets with spoofed mac address. So the dhcp server grants different ip addresses to all requests and fills up the dhcp pool. There after a new legitimate client requesting an ip address will not receive it. This is known as DHCP Salvation.

For this demo we have a kali linux machine(attacker) and a backtrack machine(target) on a network range 192.168.2.0/24. The dhcp server is running at 192.168.2.1 and has a pool of 254 ips form 192.168.2.1-254.

Step 1 : Launch yersinia in interactive mode.

```
Command: yersinia -I
```

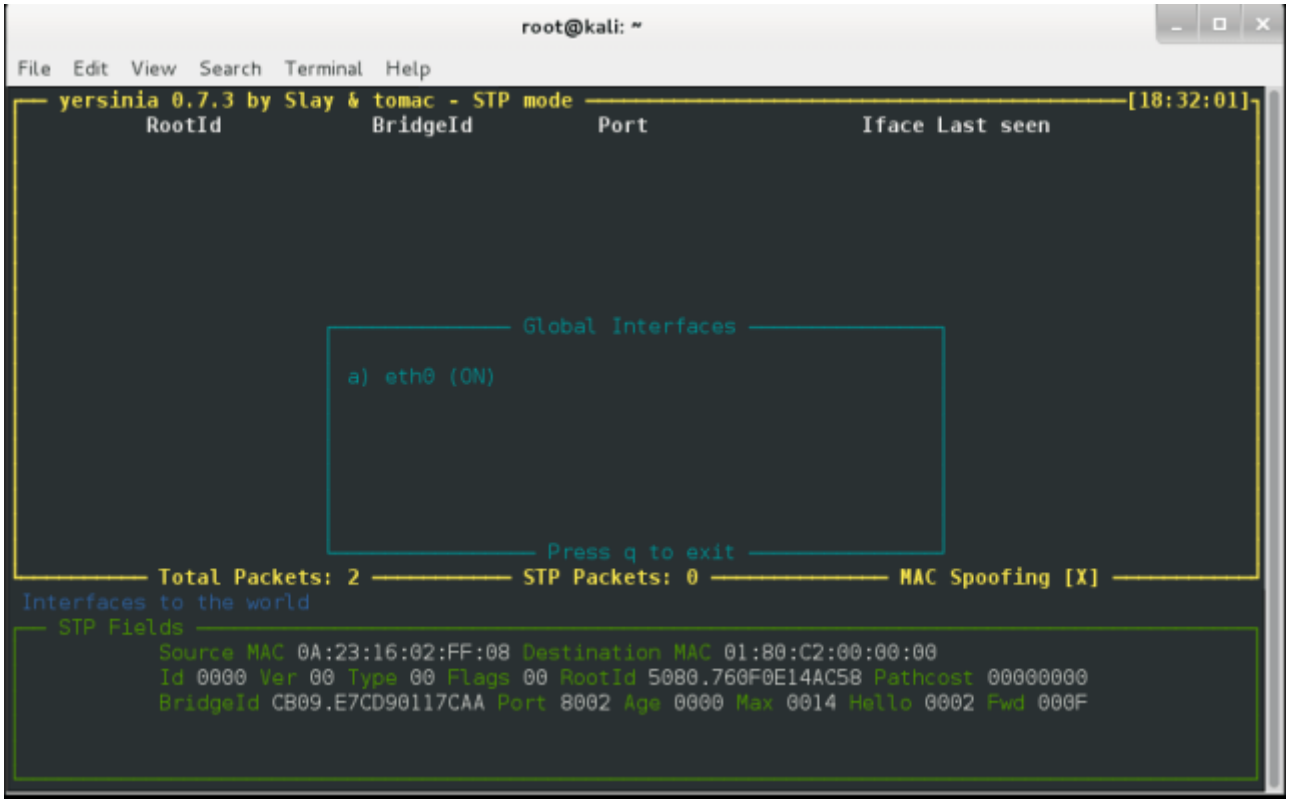


Yersinia NCurses mode

Step 2: Press h for help. Then change interface to eth0(or your default interface)

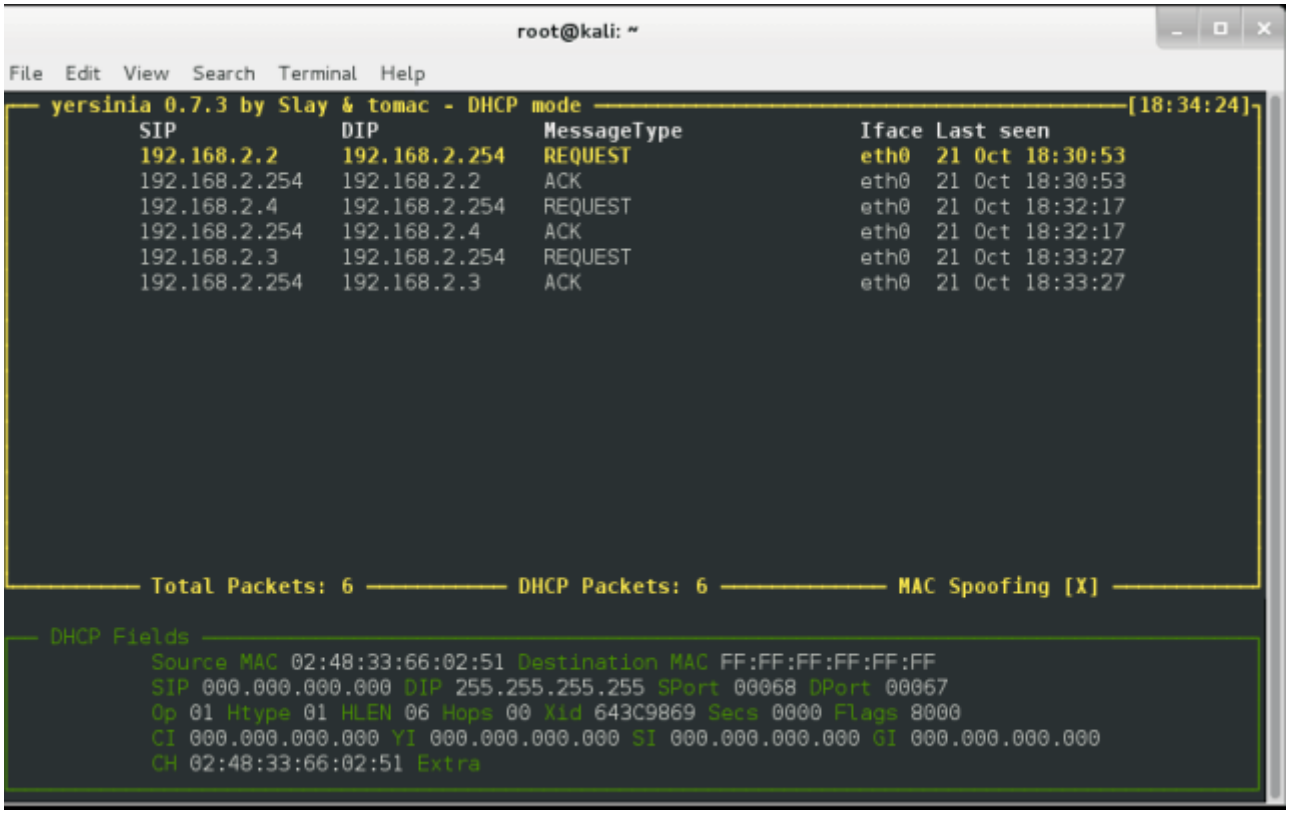
Yersinia Options

Press “i” to select the edit interfaces option



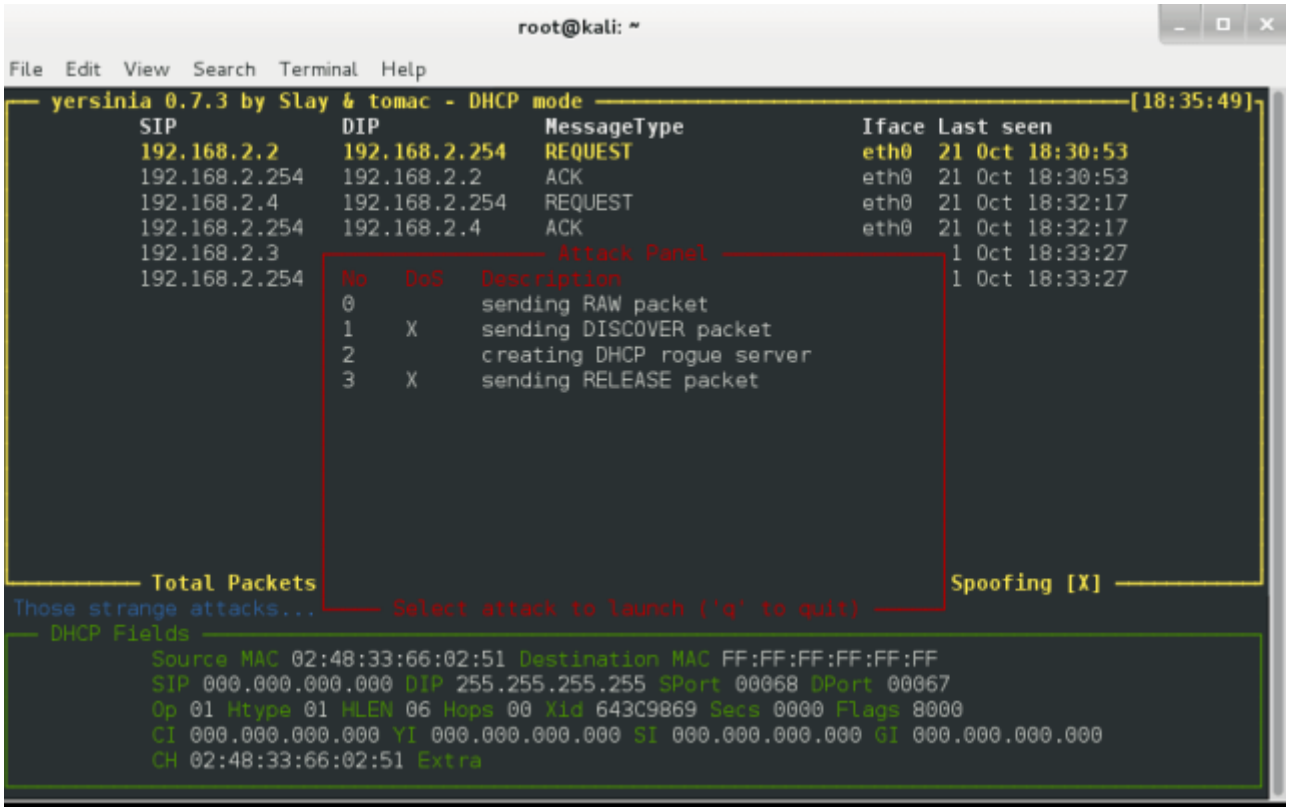
Selecting Interface

Step 3: Select DHCP mode by pressing F2 key.



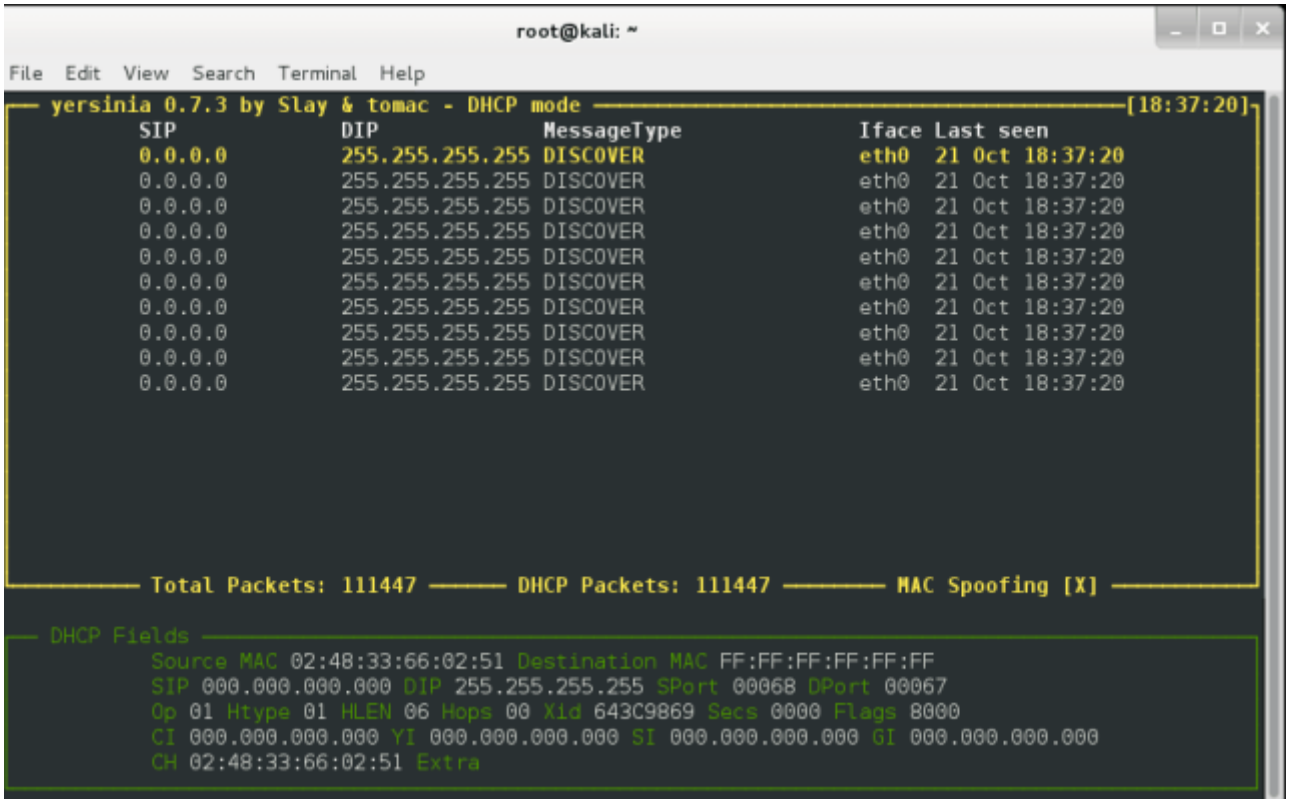
Yersinia in DHCP Mode

Step 4: Execute Attack by pressing x key and then selecting corresponding sub-attack.



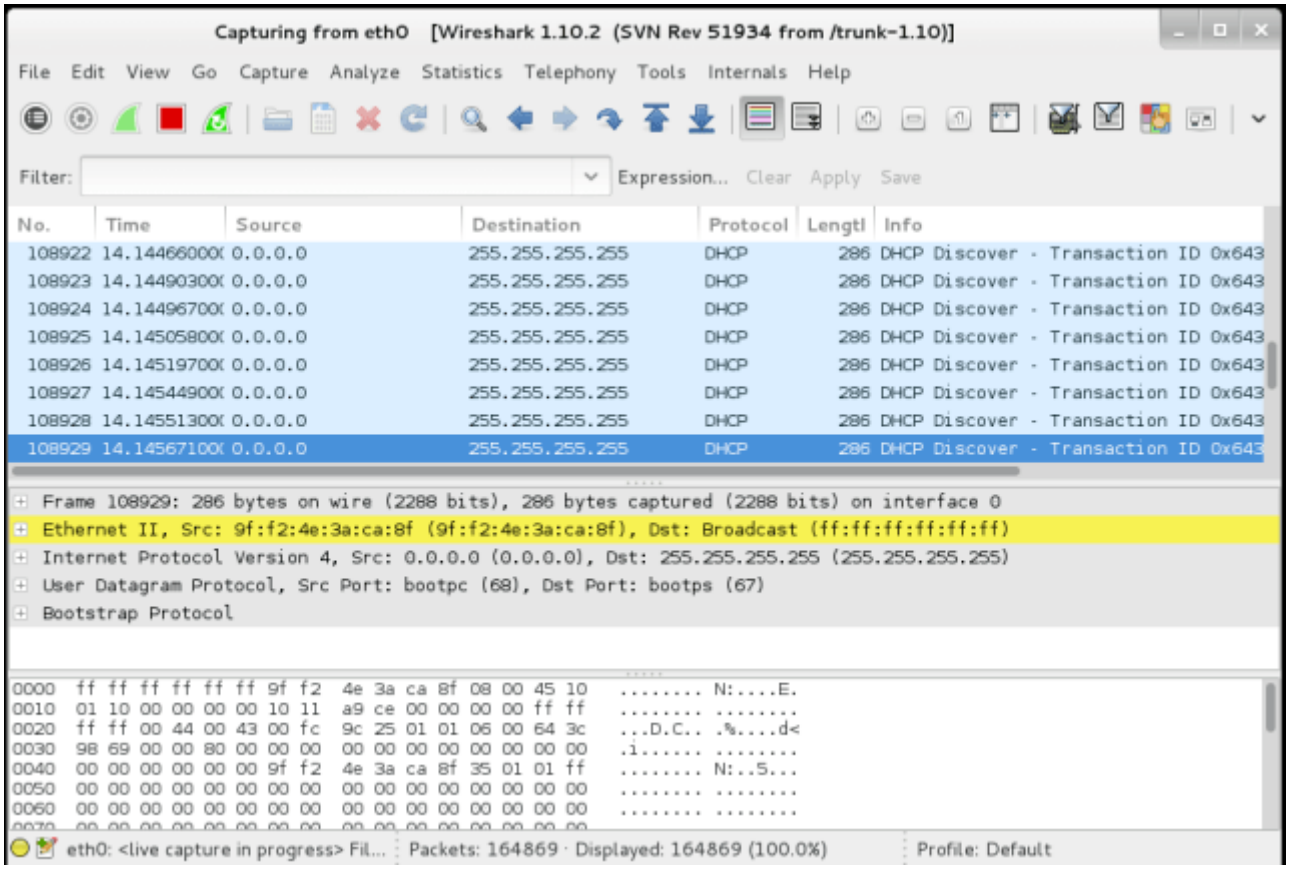
Selecting the type of DHCP attack

Now press 1 key to launch DHCP Discover attack.



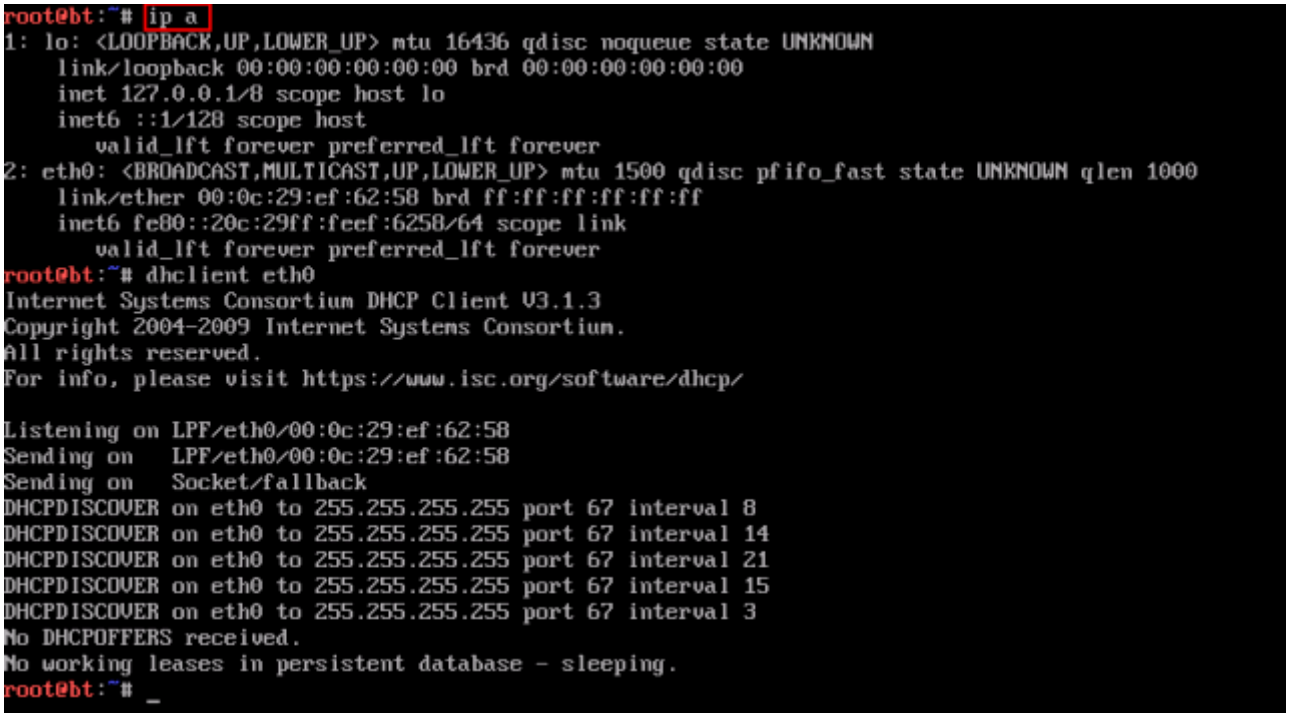
Numerous DHCP Discover Packets being sent.

In this you can see all dhcp discover packets being sent from our attacker system. Also check the same on wireshark.



DHCP Discover requests being sent seen in Wireshark.

Now wait for 1 minute and try to connect a new client to the network(here a backtrack machine). Any machine (VM or Real) connected to the same network as in that of the attacker machine's selected interface of attack is in(here Kali linux machine with eth0 interface), will do.



Client Machines denied of IP address.

Here you can see that no default ip was there. Then dhclient(tool for getting ip from DHCP server) was run, but no lease was found. Meaning all ips in the dhcp pool are filled up