

PROFESSIONAL TRAINING REPORT
At
SATHYABAMA INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)

Submitted in partial fulfillment of the requirements for the award of
Bachelor of Technology Degree in

Information Technology

By

KESHIHAA M
(Reg. No. 39120053)

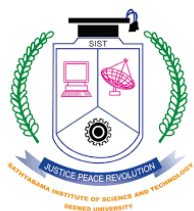


DEPARTMENT OF INFORMATION TECHNOLOGY
SCHOOL OF COMPUTING

**SATHYABAMA INSTITUTE OF
SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)**

(Established under Section 3 of UGC Act, 1956)
Jeppiaar Nagar, Rajiv Gandhi Salai, Chennai - 600119
www.sathyabamauniversity.ac.in

APRIL 2022



SATHYABAMA
INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE
UNIVERSITY)

Accredited with Grade “A” by NAAC

(Established under Section 3 of UGC Act, 1956)

JEPPIAAR NAGAR, RAJIV GANDHI SALAI

CHENNAI– 600119

www.sathyabama.ac.in

DEPARTMENT OF INFORMATION TECHNOLOGY

BONAFIDE CERTIFICATE

This is to certify that this Project Report is the bonafide work of **KESHIHAA M**
(Reg. No: 39120053) who carried out the project entitled “**DHCP STARVATION**
USING YERSINIA” under my supervision from Feb 2022 to April 2022.

Internal Guide

Dr. S Revathy, M.E., Ph.D.,

Head of the Department

Dr. R Subhashini, M.E., Ph.D.,

Submitted for Viva voce Examination held on _____

Internal Examiner

External Examiner

DECLARATION

I, **KESHIHAA M** (Reg. No. 39120053) hereby declare that the Project report entitled "**DHCP STARVATION USING YERSINIA**" done by me under the guidance of **Dr. S REVATHY, M.E., Ph.D.**, is submitted in partial fulfillment of the requirements for the award of Bachelor of Technology degree in Information Technology.

DATE:

PLACE:

SIGNATURE OF THE CANDIDATE

ACKNOWLEDGEMENT

I am pleased to acknowledge my sincere thanks to Board of Management of **SATHYABAMA INSTITUTE OF SCIENCE AND TECHNOLOGY** for their kind encouragement in doing this project and for completing it successfully. I am grateful to them.

I convey my thanks to **Dr. T SASIKALA, M.E., Ph.D., Dean, School of Computing** and **Dr. R SUBHASHINI, M.E., Ph.D., Head of the Department of Information Technology** for providing me necessary support and details at the right time during the progressive reviews.

I would like to express my sincere and deep sense of gratitude to my Project Guide **Dr. S REVATHY, M.E., Ph.D.,** for her valuable guidance, suggestions and constant encouragement paved way for the successful completion of my project work.

I wish to express my thanks to all Teaching and Non-teaching staff members of the **Department OF INFORMATION TECHNOLOGY** who were helpful in many ways for the completion of the project.

TRAINING CERTIFICATE



ABSTRACT

Cybersecurity encompasses a broad range of practices, tools and concepts related closely to those of information and operational technology (OT) security. Cybersecurity is distinctive in its inclusion of the offensive use of information technology to attack adversaries. Use of the term “cybersecurity” as a key challenge and a synonym for information security or IT security confuses customers and security practitioners, and obscures critical differences between these disciplines. Recommendation for security leaders is that they should use the term “cybersecurity” to designate only security practices related to the defensive actions involving or relying upon information technology and/or OT environments and systems. Within this paper, we are aiming to explain “cybersecurity” and describe the relationships among cybersecurity, information security, OT security, IT security, and other related disciplines and practices, e.g. cyber defence, related to their implementation aligned with the planned or existing cybersecurity strategy at the national level. In the case study given example of The National Cybersecurity Strategy of the Republic of Croatia and Action plan is presented and elaborated. The Strategy's primary objective is to recognize organizational problems in its implementation and broaden the understanding of the importance of this issue in the society. In this we flood DHCP server with DHCP discover packets using yersinia. 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.

TABLE OF CONTENTS

Chapter No.	TITLE	Page No.
	ABSTRACT	i
	LIST OF ABBREVIATIONS	ii
1.	INTRODUCTION	1
	1.1 DHCP	1
	1.2 YERSINIA	1
	1.3 REQUIREMENTS FOR STARVATION	2
2.	DHCP STARVATION USING YERSINIA	
	2.1 AIM	3
	2.3 VIRTUAL BOX	3
	2.4 EXECUTION : STARVATION ATTACK BY YERSINIA	4
3.	SUMMARY AND CONCLUSIONS	8
	REFERENCE	9
	APPENDIX	18
	A. SOURCE CODE	10
	B. SCREENSHOTS	14

LIST OF ABBREVIATIONS

DHCP	-	Dynamic Host Configuration protocol
Yersinia - G	-	Graphical mode
Yersinia - I	-	Interactive mode

CHAPTER 1

INTRODUCTION

1.1 DHCP

The Dynamic Host Configuration Protocol (DHCP) is a network management protocol used on Internet Protocol (IP) networks for automatically assigning IP addresses and other communication parameters to devices connected to the network using a client–server architecture.

The technology eliminates the need for individually configuring network devices manually, and consists of two network components, a centrally installed network DHCP server and client instances of the protocol stack on each computer or device. When connected to the network, and periodically thereafter, a client requests a set of parameters from the DHCP server using the DHCP protocol.

DHCP can be implemented on networks ranging in size from residential networks to large campus networks and regional ISP networks.[2] Many routers and residential gateways have DHCP server capability. Most residential network routers receive a unique IP address within the ISP network. Within a local network, a DHCP server assigns a local IP address to each device.

1.2 YERSINIA

Yersinia is a framework for performing layer 2 attacks. It is 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.

To install yersinia in kali linux use the command:

- Sudo apt install yersinia

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)

1.3 REQUIREMENTS FOR STARVATION:

- Install Kali linux
- Install yersinia in root terminal
- Launch the attack

An effective DHCP starvation attack mitigation is proposed.

- The proposed solution addresses both wired and wireless access networks.
- IP allocation on each switch port is proportional to the estimated number of contending users.
- The effectiveness of the mitigation solution has been carried out using simulation.

In addition, we propose a novel mitigation solution. Our solution overcomes the limitations of existing solutions in terms of performance, effectiveness, and flexibility. Our solution is based on dynamic fair allocation of IP addresses and is suitable for unshared and shared (wireless) access networks. We study and analyse the proposed mitigation technique through numerical examples and simulations. Furthermore, simulation results show that our proposed solution is far superior in mitigating DHCP starvation attack when compared to other existing techniques such as fixed allocation and DHCP request rate detection.

The basic functionality of the DHCP protocol is to automatically configure client machines with IP addresses and other network information such as the subnet mask, the default gateway address, and the Domain Name System (DNS) address. DHCP not only eliminates the need for intervention by a network administrator to manually assign IP addresses, but also prevents IP address conflicts among client machines connected to the same network.

CHAPTER 2

AIM AND SCOPE OF THE PRESENT INVESTIGATION

2.1 Aim:

This project aims to do DHCP Starvation using yersinia in kali linux.

2.2 Functional Requirements:

To execute this attack , some major tools are being used. The tools used in this attack are listed below:

❖ Kali linux:

Kali Linux is an open-source, Debian-based Linux distribution geared towards various information security tasks, such as Penetration Testing, Security Research, Computer Forensics and Reverse Engineering.

❖ Wireshark:

Wireshark is a network protocol analyzer, or an application that captures packets from a network connection, such as from your computer to your home office or the internet. Packet is the name given to a discrete unit of data in a typical Ethernet network. Wireshark is the most often-used packet sniffer in the world.

2.3 Virtual box:

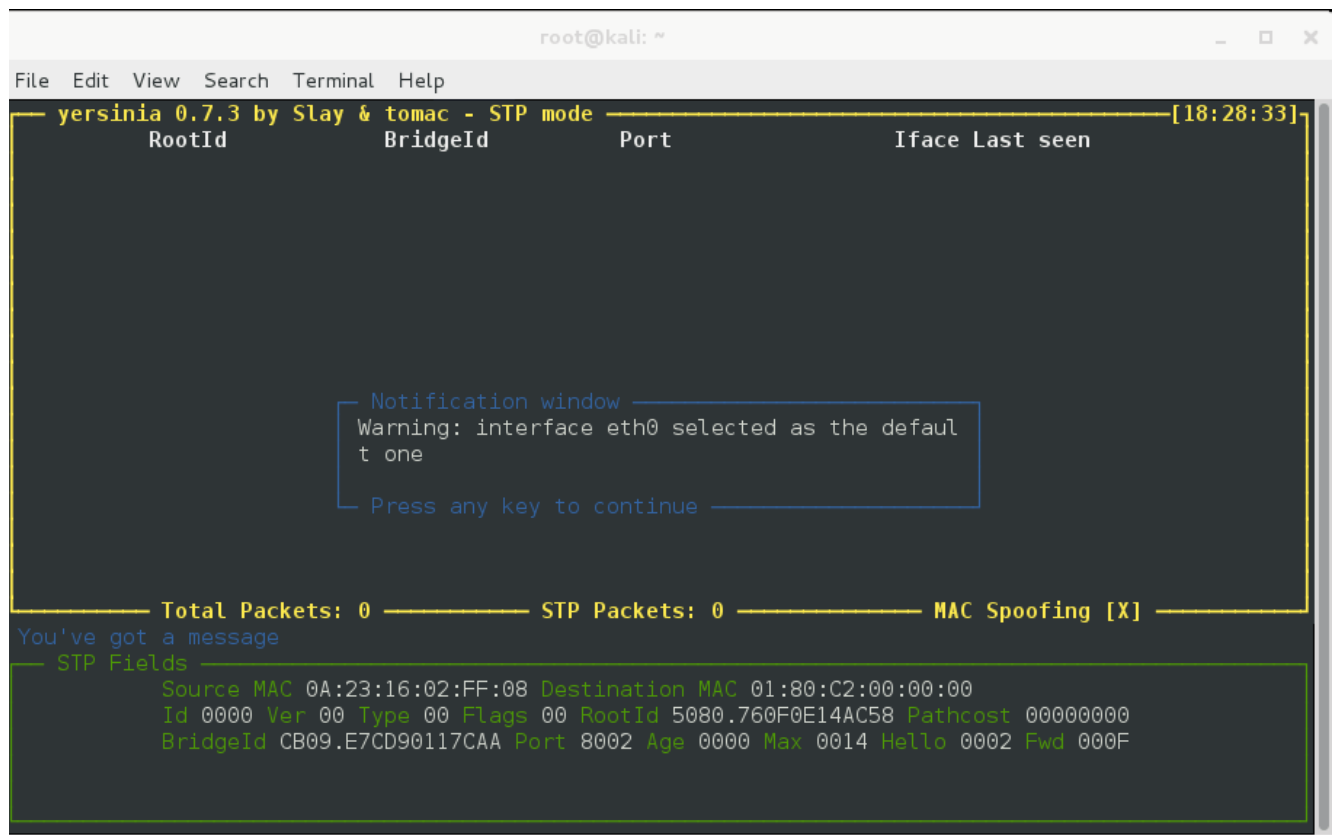
Oracle VM VirtualBox is cross-platform virtualization software. It allows users to extend their existing computer to run multiple operating systems including Microsoft Windows, Mac OS X, Linux, and Oracle Solaris, at the same time.

VirtualBox is designed to run virtual machines on your physical machine without reinstalling your OS that is running on a physical machine. One more VirtualBox advantage is that this product can be installed for free. A virtual machine (VM) works much like a physical one.

DHCP STARVATION USING YERSINIA

In this 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.

1. Launch yersinia in interactive mode.



```
root@kali: ~  
File Edit View Search Terminal Help  
----- yersinia 0.7.3 by Slay & tomac - STP mode ----- [18:28:33]  
RootId      BridgeId      Port      Iface Last seen  
  
[ Notification window ]  
Warning: interface eth0 selected as the default one  
Press any key to continue  
  
----- Total Packets: 0 ----- STP Packets: 0 ----- MAC Spoofing [X] -----  
You've got a message  
----- 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
```

Press h for help. Then change interface to eth0(or your default interface

```
root@kali: ~
File Edit View Search Terminal Help
----- yersinia 0.7.3 by Slay & tomac - STP mode -----[18:29:51]
RootId      BridgeId      Port      Iface Last seen
-----
Available commands
h      Help screen
x      eXecute attack
i      edit Interfaces
ENTER  information about selected item
v      View hex packet dump
d      load protocol Default values
e      Edit packet fields
f      list capture Files
s      Save packets from protocol
S      Save packets from all protocols
L      Learn packet from network
M      set Mac spoofing on/off
l      List running attacks
K      Kill all running attacks
c      Clear current protocol stats
C      Clear all protocols stats
g      Go to other protocol screen
Ctrl-L redraw screen
w      Write configuration file
a      About this proggie
q      Quit (bring da noise)
-----
Total Packets: 0
This is the help screen.
STP Fields
Source MAC 0A:23:
Id 0000 Ver 00 Ty
BridgeId CB09.E7C
-----
MAC Spoofing [X] -----
:00
thcost 00000000
o 0002 Fwd 000F
```

```
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 (0N)
----- 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
```

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
```

```
File Edit View Search Terminal Help
----- yersinia 0.7.3 by Slay & tomac - DHCP mode -----[18:35:49]
      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

----- Attack Panel -----
No  DoS  Description
0           sending RAW packet
1    X   sending DISCOVER packet
2           creating DHCP rogue server
3    X   sending RELEASE packet

----- Total Packets ----- Spoofing [X] -----
Those strange attacks... Select attack to launch ('q' to quit)

----- 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
```

press 1 key to launch DHCP Discover 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

```

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
108922	14.14466000	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643
108923	14.14490300	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643
108924	14.14496700	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643
108925	14.14505800	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643
108926	14.14519700	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643
108927	14.14544900	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643
108928	14.14551300	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643
108929	14.14567100	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643

+ Frame 108929: 286 bytes on wire (2288 bits), 286 bytes captured (2288 bits) on interface 0
 + Ethernet II, Src: 9f:f2:4e:3a:ca:8f (9f:f2:4e:3a:ca:8f), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 + Internet Protocol Version 4, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
 + User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
 + Bootstrap Protocol

```

0000  ff ff ff ff ff ff 9f f2 4e 3a ca 8f 08 00 45 10  ..... N:....E.
0010  01 10 00 00 00 00 10 11 a9 ce 00 00 00 00 ff ff  .....
0020  ff ff 00 44 00 43 00 fc 9c 25 01 01 06 00 64 3c  ...D.C...%.<
0030  98 69 00 00 80 00 00 00 00 00 00 00 00 00 00 00  .i.....
0040  00 00 00 00 00 00 9f f2 4e 3a ca 8f 35 01 01 ff  ..... N:..5...
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  .....

```

eth0: <live capture in progress> Fil... Packets: 164869 · Displayed: 164869 (100.0%) Profile: Default

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

CHAPTER 3

SUMMARY AND CONCLUSIONS

- **SUMMARY:**

Attacks using DHCP Starvation, which exhausts all IP Pool DHCP server.

The operating principle of this attack is very simple:

Asking yourself IP -address at the DHCP server and a receives it;

Change the MAC addresses and ask for the next one, a different IP -address, masquerading as a new client;

Such action is repeated until the entire pool of IP address on the DHCP server is reached.

- **CONCLUSION:**

Analysation of dhcp discover packets being sent from the attacker system which results the legitimate clients being unable to lease ip addresses

REFERENCES:

1. H. Shahriari et al Vulnerability analysis of networks to detect multiphase attacks using the actor-based language Comput Electr Eng(2010)
.
2. D. Zagar et al Security aspects in IP implementation and testing Comput Electr Eng (2007)
3. A. Wong et al Network infrastructure security (2009)

APPENDIX

A. SOURCE CODE

```
File Actions Edit View Help
RX packets 1 bytes 590 (590.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 12 bytes 1204 (1.1 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 0 bytes 0 (0.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali@kali)-[~]
$ ifconfig --help
Usage:
ifconfig [-a] [-v] [-s] <interface> [[<AF>] <address>]
[add <address>[/<prefixlen>]]
[del <address>[/<prefixlen>]]
[[-]broadcast [<address>]] [[-]pointopoint [<address>]]
[netmask <address>] [dstaddr <address>] [tunnel <address>]
[outfill <NN>] [keepalive <NN>]
[hw <HW> <address>] [mtu <NN>]
[[-]trailers] [[-]jarp] [[-]allmulti]
[multicast] [[-]promisc]
[mem_start <NN>] [io_addr <NN>] [irq <NN>] [media <type>]
[txqueuelen <NN>]
[[-]dynamic]
[updown] ...

<HW> Hardware Type.
List of possible hardware types:
loop (Local Loopback) slip (Serial Line IP) cslip (VJ Serial Line IP)
slip6 (6-bit Serial Line IP) cslip6 (VJ 6-bit Serial Line IP) adaptive (Adaptive Serial Line IP)
ash (Ash) ether (Ethernet) ax25 (AMPR AX.25)
netrom (AMPR NET/ROM) rose (AMPR ROSE) tunnel (IP/IP Tunnel)
ppp (Point-to-Point Protocol) hdlc ((Cisco)-HDLC) lapb (LAPB)
arcnet (ARCnet) dlci (Frame Relay DLCI) frad (Frame Relay Access Device)
sit (IPv6-in-IPv4) fddi (Fiber Distributed Data Interface) hippi (HIPPI)
irda (IrLAP) ec (Econet) x25 (generic X.25)
eui64 (Generic EUI-64)

<AF> Address family. Default: inet
List of possible address families:
unix (UNIX Domain) inet (DARPA Internet) inet6 (IPv6)
ax25 (AMPR AX.25) netrom (AMPR NET/ROM) rose (AMPR ROSE)
ipx (Novell IPX) ddp (Appletalk DDP) ec (Econet)
ash (Ash) x25 (CCITT X.25)
```

```
File Actions Edit View Help
(kali@kali)~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::a00:27ff:fe95:bd54 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:95:bd:54 txqueuelen 1000 (Ethernet)
    RX packets 1 bytes 590 (590.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 12 bytes 1204 (1.1 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali@kali)~$ ifconfig --help
Usage:
ifconfig [-a] [-v] [-s] <interface> [[<AF>] <address>]
[add <address>[/<prefixlen>]]
[del <address>[/<prefixlen>]]
[[-]broadcast [<address>]] [[-]pointopoint [<address>]]
[netmask <address>] [dstaddr <address>] [tunnel <address>]
[outfill <NN>] [keepalive <NN>]
[hw <HW> <address>] [mtu <NN>]
[[-]trailers] [[-]arp] [[-]allmulti]
[multicast] [[-]promisc]
[mem_start <NN>] [io_addr <NN>] [irq <NN>] [media <type>]
[txqueuelen <NN>]
[[-]dynamic]
[up|down] ...

<HW> Hardware Type.
List of possible hardware types:
loop (Local Loopback) slip (Serial Line IP) csllip (VJ Serial Line IP)
slip6 (6-bit Serial Line IP) csllip6 (VJ 6-bit Serial Line IP) adaptive (Adaptive Serial Line IP)
ash (Ash) ether (Ethernet) ax25 (AMPR AX.25)
netrom (AMPR NET/ROM) rose (AMPR ROSE) tunnel (IPIP Tunnel)
ppp (Point-to-Point Protocol) hdlc ((Cisco)-HDLC) lapb (LAPB)
arcnet (ARCnet) dli (Frame Relay DLCI) frad (Frame Relay Access Device)
sit (IPv6-in-IPv4) fddi (Fiber Distributed Data Interface) hippi (HIPPI)
irda (IrLAP) ec (Econet) x25 (generic X.25)
oui64 (Generic EUI-64)
<AF> Address family. Default: inet
List of possible address families:
unix (UNIX Domain) inet (DARPA Internet) inet6 (IPv6)
```


root@kali: ~

RootId	BridgeId	Port	Iface	Last seen
--------	----------	------	-------	-----------

Available commands

- h Help screen
- x eXecute attack
- i edit Interfaces
- ENTER information about selected item
- v View hex packet dump
- d load protocol Default values
- e Edit packet fields
- f list capture Files
- s Save packets from protocol
- S Save packets from all protocols
- L Learn packet from network
- M set Mac spoofing on/off
- l List running attacks
- K Kill all running attacks
- c Clear current protocol stats
- C Clear all protocols stats
- g Go to other protocol screen
- Ctrl-L redraw screen
- w Write configuration file
- a About this proggie
- q Quit (bring da noize)

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

Total Packets: 0 STP Packets: 0 MAC Spoofing [X]

BridgeId: CB09.E7CD90117CAA Port: 8002 Age: 0000 Max: 0014 Hello: 0002 Fwd: 000F

B . SCREENSHOT

Wireshark interface showing a DHCP transaction. The packet list displays four packets:

No.	Time	Source	Destination	Protocol	Length	Info
13	14.141591	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0xc8f3d505
14	14.200772	192.168.1.1	192.168.1.11	DHCP	590	DHCP Offer - Transaction ID 0xc8f3d505 [Malformed Packet]
15	14.203085	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0xc8f3d505
16	14.311374	192.168.1.1	192.168.1.11	DHCP	590	DHCP ACK - Transaction ID 0xc8f3d505 [Malformed Packet]

The packet details for packet 13 are expanded, showing the following layers:

- Frame 13: 344 bytes on wire (2752 bits), 344 bytes captured (2752 bits) on interface \Device\NPF_{AD6FE506-69E8-463E-8F88-3288E3514D71}, id 0
- Ethernet II, Src: Dell_1f:82:d9 (30:d0:42:1f:82:d9), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
- Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
- User Datagram Protocol, Src Port: 68, Dst Port: 67
- Dynamic Host Configuration Protocol (Discover)

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```

0000 ff ff ff ff ff 30 d0 42 1f 82 d9 00 00 45 00 .....0. B....E
0010 01 4a f0 6a 00 00 80 11 00 00 00 00 00 ff ff -.j.....
0020 ff ff 00 44 00 43 01 36 f3 4e 01 01 06 00 c8 f3 ..D.C.6.N....
0030 d5 05 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0040 00 00 00 00 00 30 d0 42 1f 82 d9 00 00 00 00 .....0. B....
0050 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 .....
0070 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 .....
0090 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 .....
00b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

```

```
root@kali: -

SIP      DIP      MessageType      Iface Last seen
0.0.0.0   255.255.255.255 DISCOVER          eth0  14 Apr 07:19:12
0.0.0.0   255.255.255.255 DISCOVER          eth0  14 Apr 07:19:12
0.0.0.0   255.255.255.255 DISCOVER          eth0  14 Apr 07:19:12
0.0.0.0   255.255.255.255 DISCOVER          eth0  14 Apr 07:19:12
0.0.0.0   255.255.255.255 DISCOVER          eth0  14 Apr 07:19:12
0.0.0.0   255.255.255.255 DISCOVER          eth0  14 Apr 07:19:12
0.0.0.0   255.255.255.255 DISCOVER          eth0  14 Apr 07:19:12
0.0.0.0   255.255.255.255 DISCOVER          eth0  14 Apr 07:19:12
0.0.0.0   255.255.255.255 DISCOVER          eth0  14 Apr 07:19:12
0.0.0.0   255.255.255.255 DISCOVER          eth0  14 Apr 07:19:12

Total Packets: 669804  DHCP Packets: 669804  MAC Spoofing [X]

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
```

No.	Time	Source	Destination	Protocol	Length	Info
6390.	13.141134710	0.0.0.0	255.255.255.255	DHCP	206	DHCP Discover - Transaction ID 0x643c9069
6390.	13.141159044	0.0.0.0	255.255.255.255	DHCP	206	DHCP Discover - Transaction ID 0x643c9069
6390.	13.141166298	0.0.0.0	255.255.255.255	DHCP	206	DHCP Discover - Transaction ID 0x643c9069
6390.	13.141189938	0.0.0.0	255.255.255.255	DHCP	206	DHCP Discover - Transaction ID 0x643c9069
6390.	13.141214819	0.0.0.0	255.255.255.255	DHCP	206	DHCP Discover - Transaction ID 0x643c9069
6390.	13.141236868	0.0.0.0	255.255.255.255	DHCP	206	DHCP Discover - Transaction ID 0x643c9069
6390.	13.141243827	0.0.0.0	255.255.255.255	DHCP	206	DHCP Discover - Transaction ID 0x643c9069
6390.	13.141266457	0.0.0.0	255.255.255.255	DHCP	206	DHCP Discover - Transaction ID 0x643c9069
6390.	13.141273496	0.0.0.0	255.255.255.255	DHCP	206	DHCP Discover - Transaction ID 0x643c9069
6390.	13.141295963	0.0.0.0	255.255.255.255	DHCP	206	DHCP Discover - Transaction ID 0x643c9069
6390.	13.141302905	0.0.0.0	255.255.255.255	DHCP	206	DHCP Discover - Transaction ID 0x643c9069
6390.	13.141334301	0.0.0.0	255.255.255.255	DHCP	206	DHCP Discover - Transaction ID 0x643c9069
6390.	13.141342636	0.0.0.0	255.255.255.255	DHCP	206	DHCP Discover - Transaction ID 0x643c9069
6390.	13.141364611	0.0.0.0	255.255.255.255	DHCP	206	DHCP Discover - Transaction ID 0x643c9069
6390.	13.141371597	0.0.0.0	255.255.255.255	DHCP	206	DHCP Discover - Transaction ID 0x643c9069
6390.	13.141394356	0.0.0.0	255.255.255.255	DHCP	206	DHCP Discover - Transaction ID 0x643c9069

Frame 1: 286 bytes on wire (2288 bits), 286 bytes captured (2288 bits) on interface eth0, id 0

Ethernet II, Src: 44:37:96:79:18:5c (44:37:96:79:18:5c), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255

User Datagram Protocol, Src Port: 68, Dst Port: 67

Dynamic Host Configuration Protocol (Discover)

```
0000 ff ff ff ff ff ff 44 37 96 79 18 5c 00 00 45 10 .....D7 y \ E
0010 01 10 00 00 00 10 11 a9 ce 00 00 00 00 ff ff .....
0020 ff ff 00 44 00 43 00 fc 96 d5 01 01 06 00 64 3c ...D C...d<
0030 98 69 00 00 00 00 00 00 00 00 00 00 00 00 00 ...i.....
0040 00 00 00 00 00 00 44 37 96 79 18 5c 00 00 00 00 .....D7 y \...
```

Command Prompt

Microsoft Windows [Version 10.0.22000.556]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Dell>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

```
Connection-specific DNS Suffix . :  
Link-local IPv6 Address . . . . . : fe80::994e:e45b:6a03:d114%8  
IPv4 Address. . . . . : 192.168.1.11  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . : fe80::1%8  
                             192.168.1.1
```

C:\Users\Dell>ipconfig /release

Windows IP Configuration

Ethernet adapter Ethernet:

```
Connection-specific DNS Suffix . :  
Link-local IPv6 Address . . . . . : fe80::994e:e45b:6a03:d114%8  
Default Gateway . . . . . : fe80::1%8
```

C:\Users\Dell>ping google.com

Ping request could not find host google.com. Please check the name and try again.

C:\Users\Dell>ipconfig /renew

Windows IP Configuration

Ethernet adapter Ethernet:

```
Connection-specific DNS Suffix . :  
Link-local IPv6 Address . . . . . : fe80::994e:e45b:6a03:d114%8  
IPv4 Address. . . . . : 192.168.1.11  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . : fe80::1%8  
                             192.168.1.1
```

C:\Users\Dell>

S