Penetration Testing Report

TheCyberViking

Module 4

Exercise:

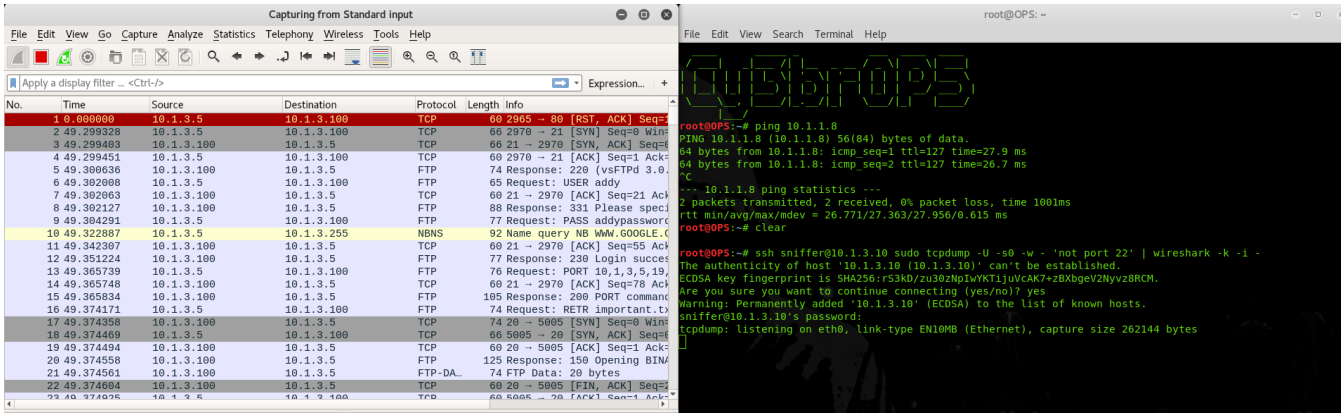
- **Task1 :** Launch wireshark using : ssh sniffer@10.1.3.10 sudo tcpdump -U -s0 -w - 'not port 22' | wireshark -k -i - (password : sniffer) and sniff and report any sensitive information being transmitted between VICTIM host (ip : 10.1.3.5) and SERVER (10.1.3.100).

HOST	**IP Address**
//////////////	10.1.3.10
USER	**PASSWORD**
sniffer	sniffer

Given that the command was already given in the task

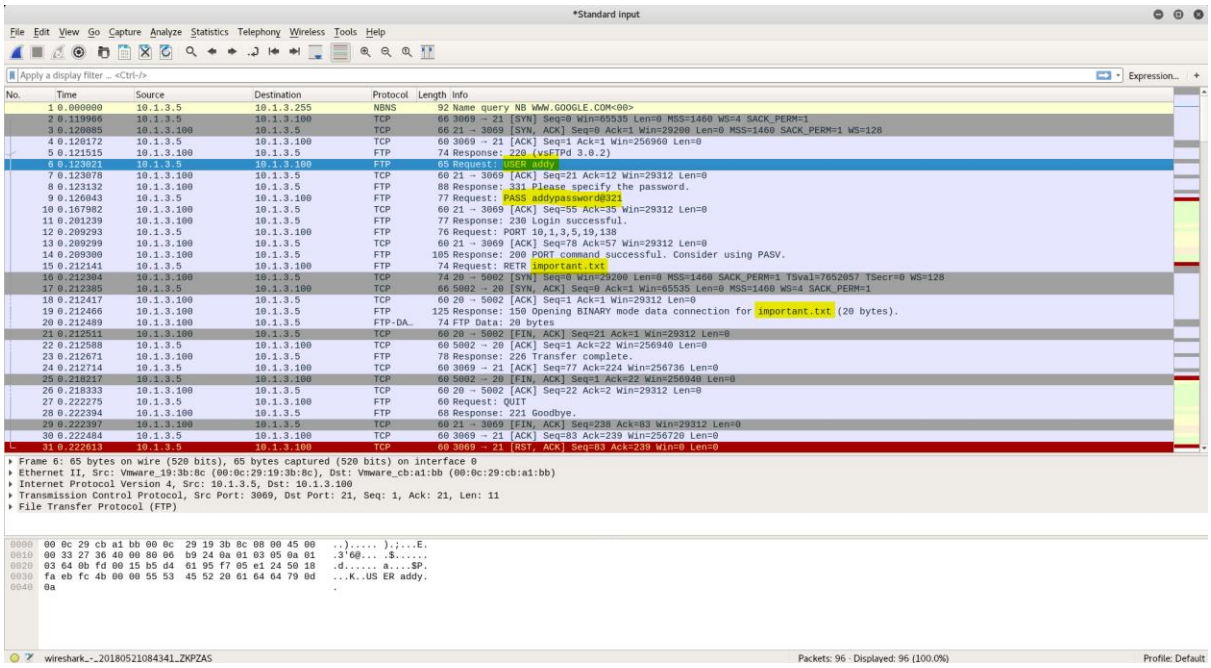
ssh sniffer@10.1.3.10 sudo tcpdump -U -s0 -w - 'not port 22' | wireshark -k -i –

I ran the command and got a certificate to accept, I accepted the certificate then entered the given password of sniffer, the output of the command open a the connection with TCP dump and also opened the Wireshark terminal and start listening for traffic.



Even tho it immediately received traffic, I decided to let it capture packets for 10 minutes before beginning to search.

Going by the specifications I started searching for any sensitive information straight away finding interesting information being transmitted in clear over FTP between 10.1.3.5 and 10.1.3.100



Captured Data over FTP is the Username and Password for the FTP server

SERVER USERNAME	SERVER PASSWORD
addy	addypassword@321

/login.php?username=admin&
password=addy

There is also a file being sent called Important.txt, when pulling that file from log this you get the following text file