BSc (Hons) in Information Technology
Write Up 2

IE1212 – System & Network Programming

Year 2 : Semester I : 2019

Exploiting Vulnerabilities
(Metasploitable)

IT18211160
C.S Wijetunga

BSc (Hons) in Information Technology
Write Up 2

IE1212 – System & Network Programming

Year 2 : Semester I : 2019

Metasploitable is an intentionally vulnerable Linux virtual machine that can be used to conduct security training, test security tools, and practice common penetration testing techniques. The VM will run on any recent VMware products and other visualization technologies such as Virtual Box.

To exploit the vulnerabilities of Metasploitable we must have Kali Linux and Metasploitable operating systems installed in a same VM ware or both machines must be in a same network.

****

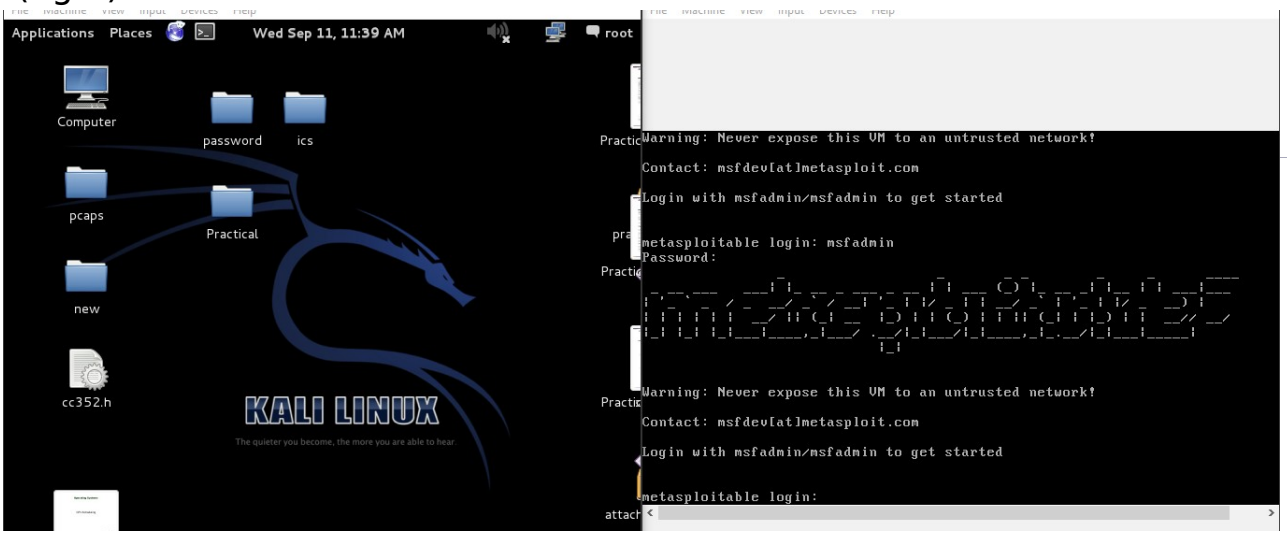
First of all we have to start our Linux OS and Metasploitable. Metasploitable OS will ask us to enter username and password. Both are **msfadmin** (fig 1) and check the IP address to find out if both are on the same network. To do that we have to run those command in both terminals.

*** Kali Linux - Open Terminal and type ipconfig**
*** Metasploitable – type ifconfig** (fig 2)

Also we can ping them and send packets to both of them to check whether they receive each others data. To do that we have to type

***ping [IP address of the other machine]** (fig 3)

(fig 1)

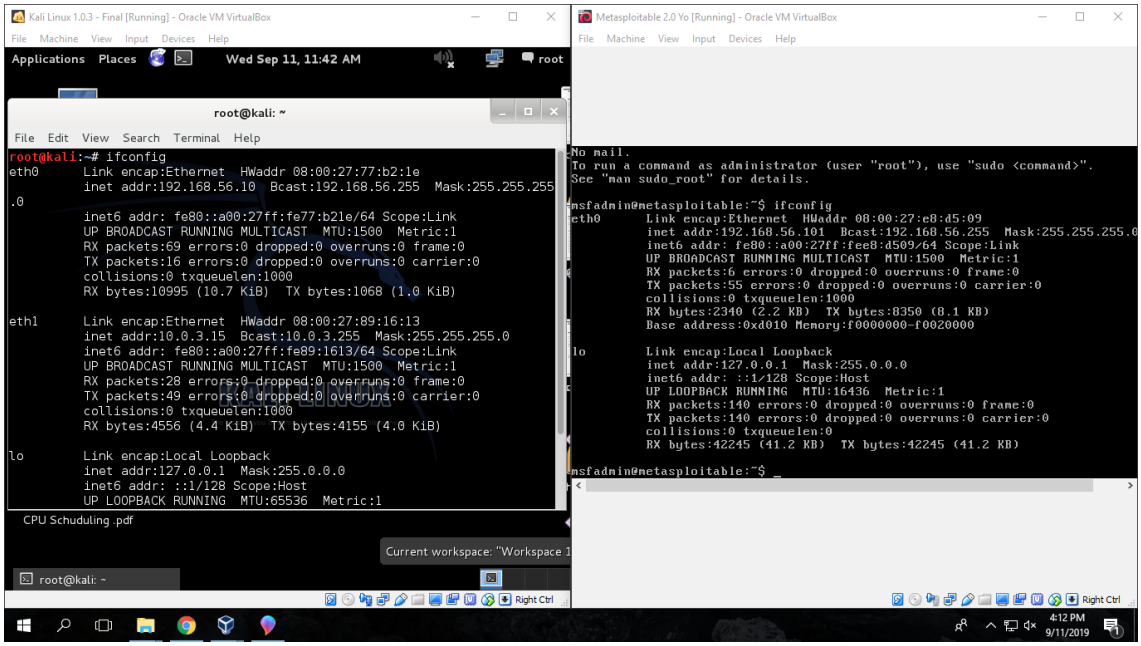


BSc (Hons) in Information Technology
Write Up 2

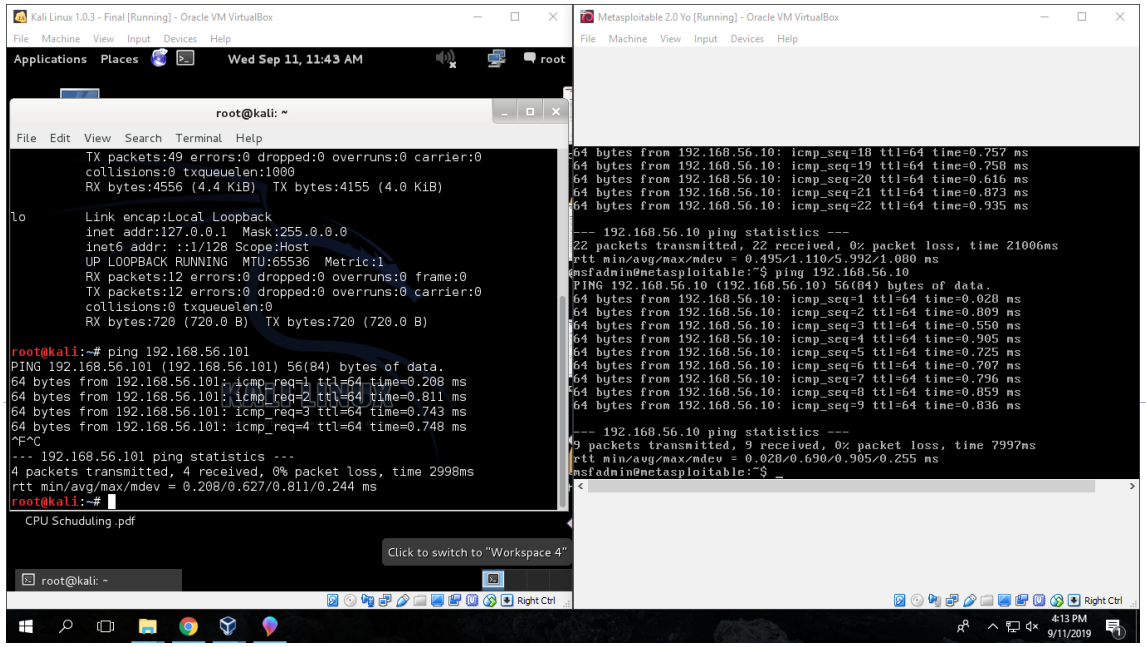
IE1212 – System & Network Programming

Year 2 : Semester I : 2019

(fig 2)

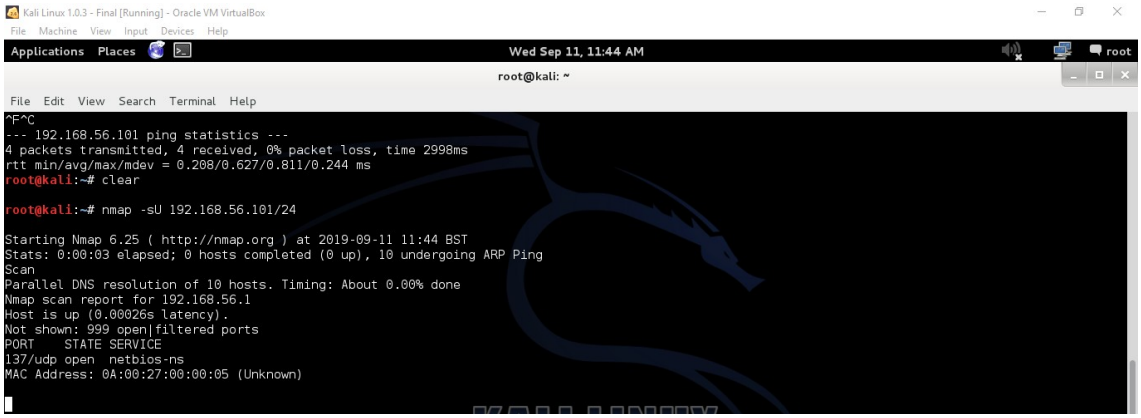


(fig 3)

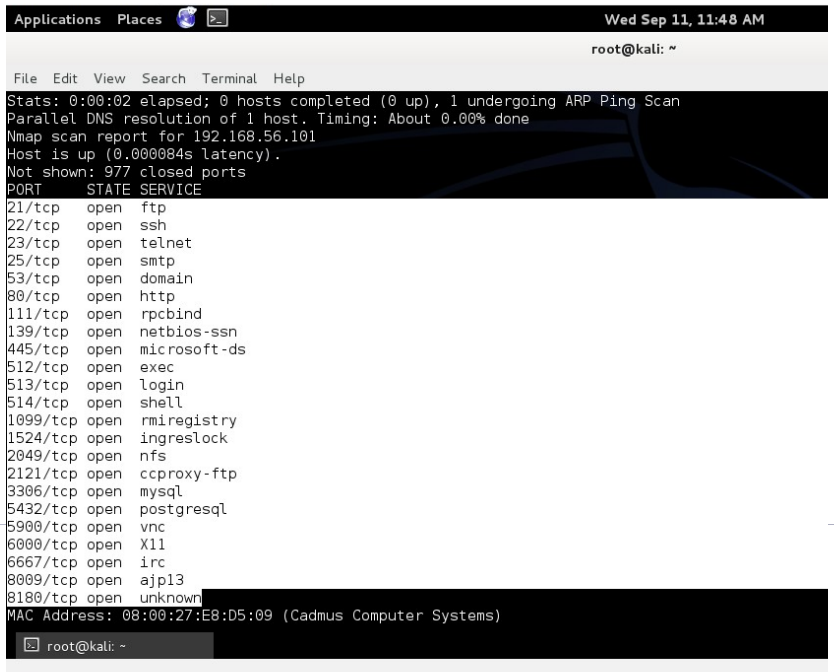


After that we can run a nmap scan on the IP Address of Metasploitable to find out the open ports and other details

*** nmap [Target IP Address]**

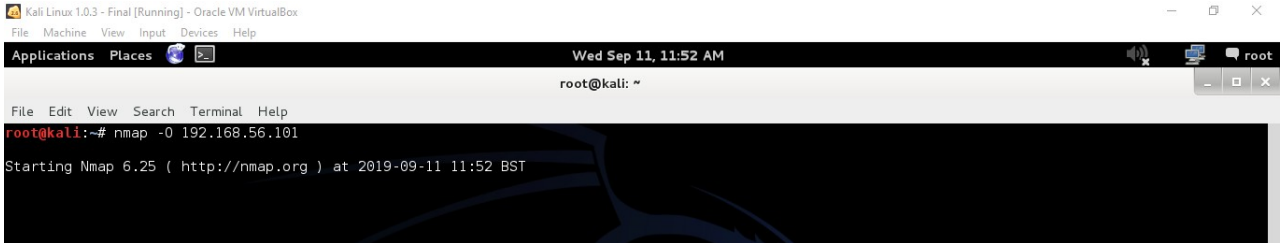


When the scan finished we can see all available open ports in Metasploitable that we can attack

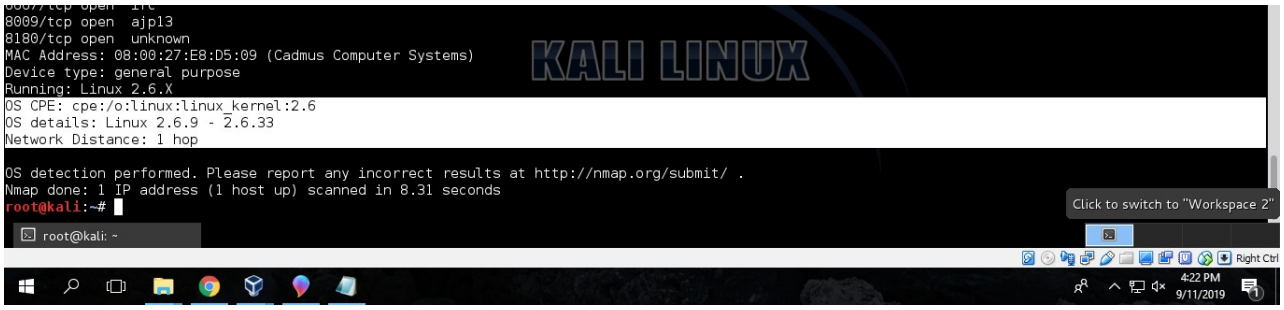


To find out what OS is operating Metasploitable we can run ***nmap -O [Target IP Address]** and it will display the OS as results (fig 6) (fig 7)

(fig 6)



(fig 7)



****

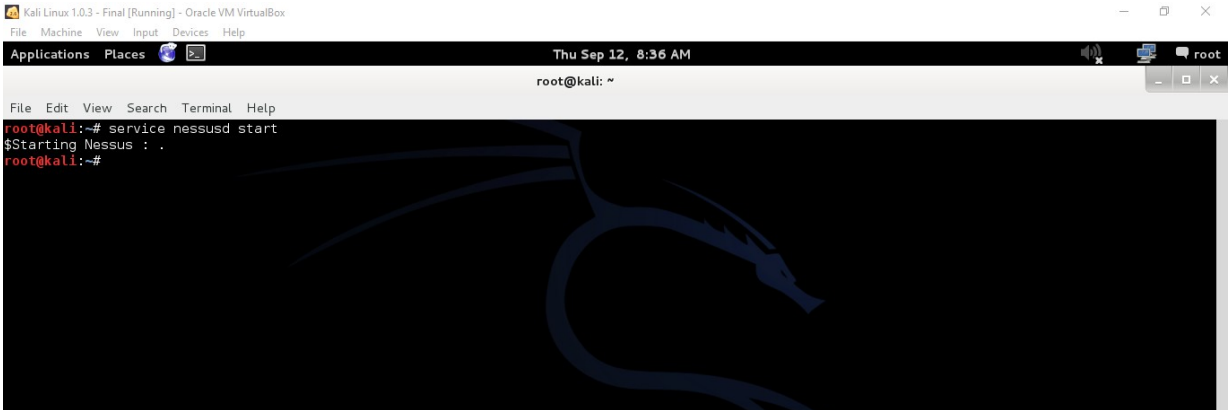
According to the results of the nmap scan we can run out Nessus Vulnerability Scanner on the target IP address. To do that we must start the nessus service in our Kali Linux Local Host first. We can do that running command,

***service nessusd start** (fig 8)

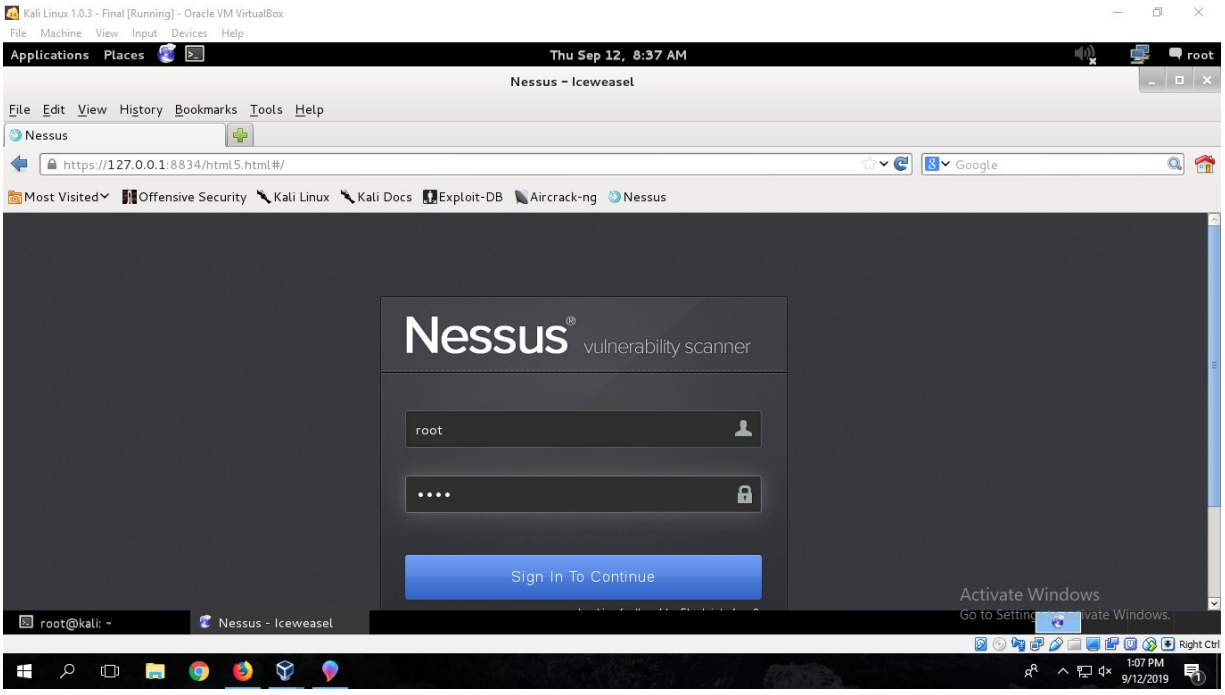
in our Kali terminal.

After starting Nessus Service we have to fire up our web browser and go to our local host IP address. (https:// 127.0.0.1) Then we can see the login page for nessus vulnerability scanner. We can use our machine logins to access the services. (fig 9)

(fig 8)

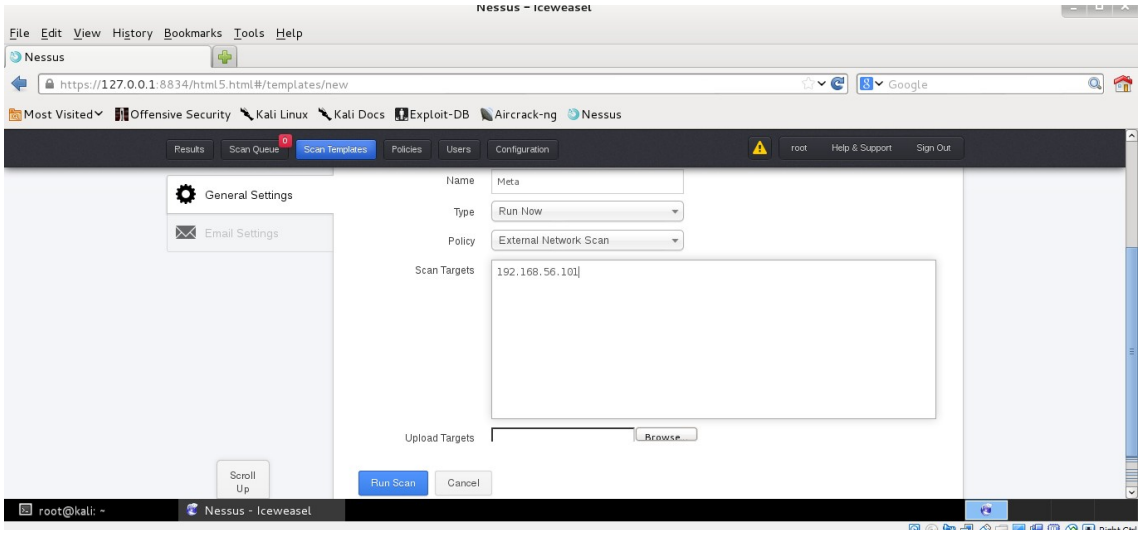


(fig 9)



When the login is successful we will be redirected to the home page of the Nessus and we have to select Scan queue and add a new scan to the system.

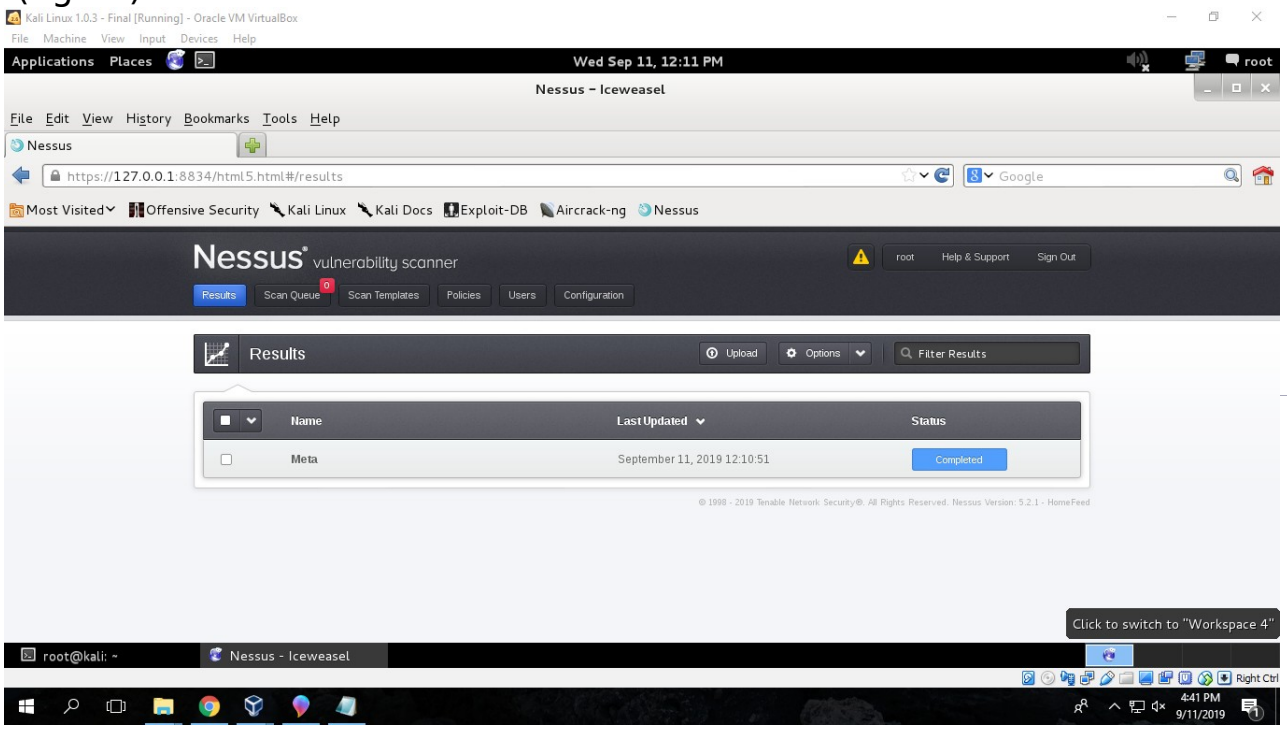
After that we have to fill up the fields and Set up the General Scan with adding the target IP for the scan target field.



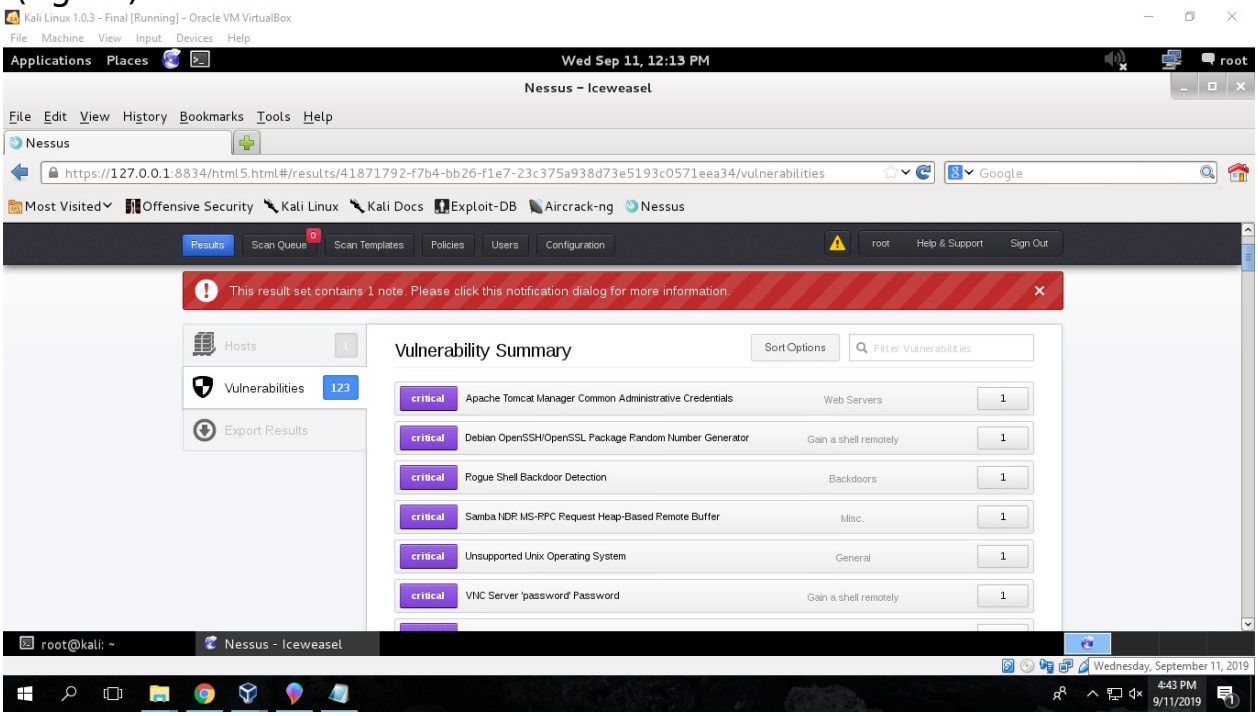
****

It will take some time to scan the vulnerabilities of the given system and after completion results will be displayed as Host Summary (fig 11) and we can view those vulnerabilities by clicking on vulnerabilities (fig 12).

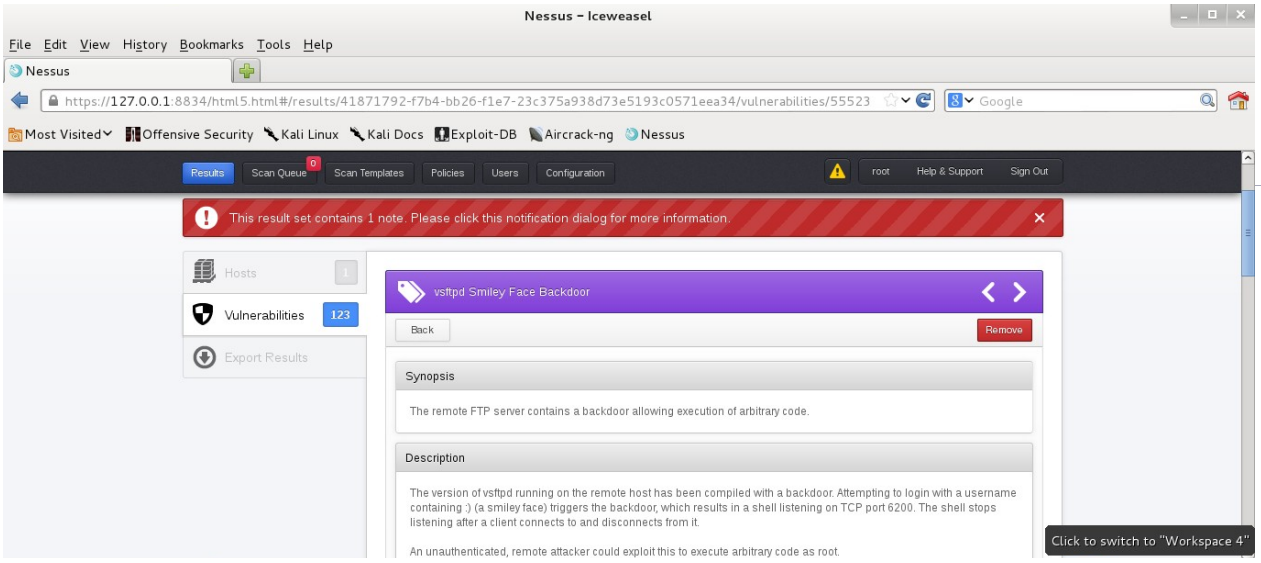
(fig 11)



(fig 12)



We can select vulnerability we want to exploit and if those selected vulnerabilities are critical level, there is a better chance for a successful exploitation. Critical Vulnerabilities are displayed in purple color tags in the summery. First we are going to exploit the **vsfptd Smiley Faced Backdoor** in Metasploitable.



BSc (Hons) in Information Technology
Write Up 2

IE1212 – System & Network Programming

Year 2 : Semester I : 2019

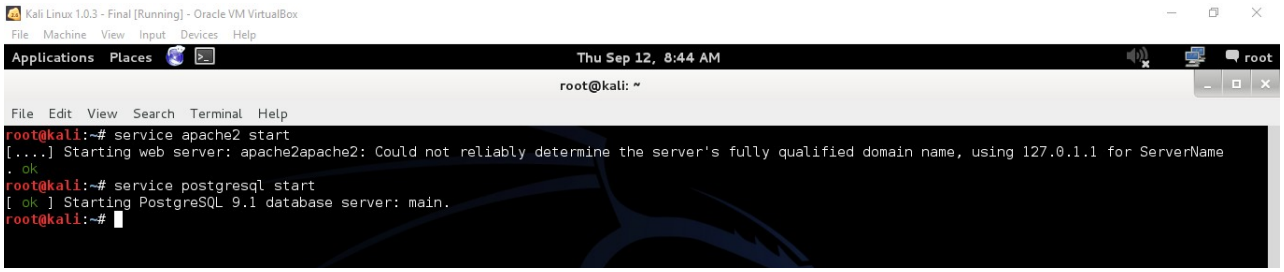
We are using **Metasploit Framework** in Kali Linux for exploit those vulnerabilities. The Metasploit Project is a computer security project that provides information about security vulnerabilities and aids in penetration testing and IDS signature development.

Before start using Metasploit Framework, we have to start the Apache Service and Postgre SQL service in Kali Linux from our terminal.

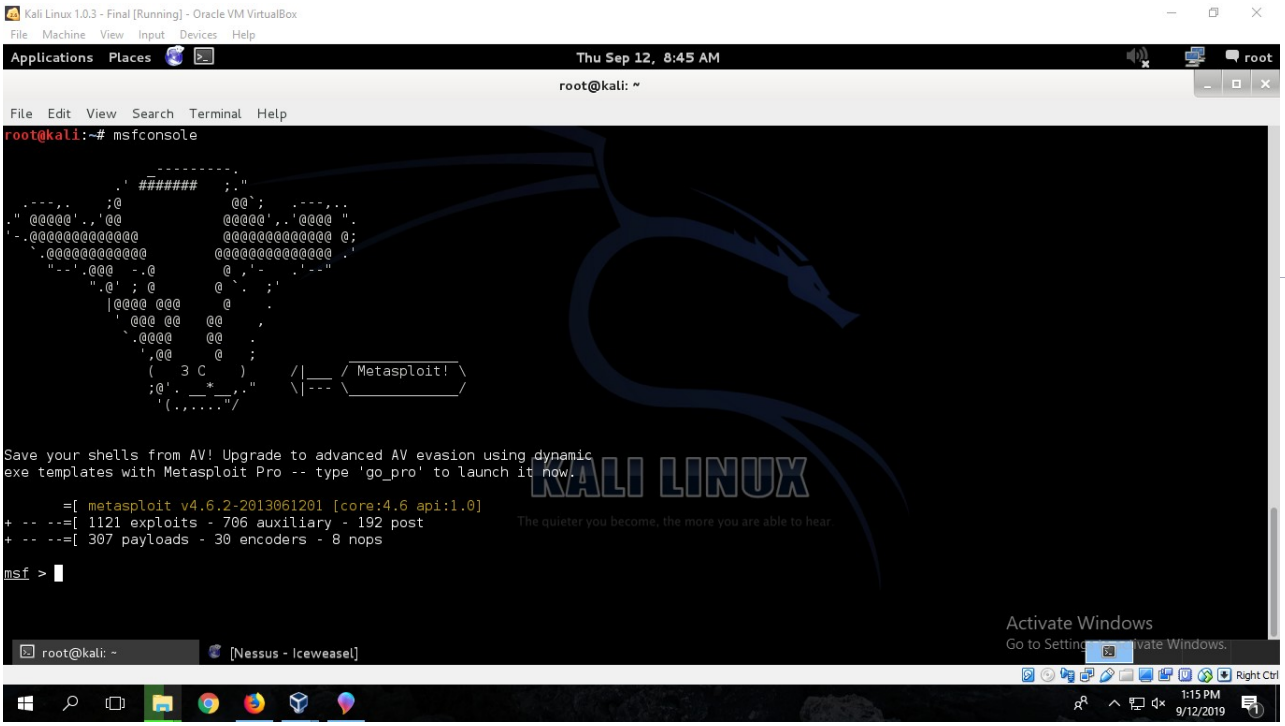
***service apache2 start**
***service postgresql start** (fig 14)

Then we can start Metasploit Framework by typing
***msfconsole** in our terminal. (fig 15)

(fig 14)



(fig 15)



In the msfconsole we have to search for the exploits that available for the selected vulnerability.

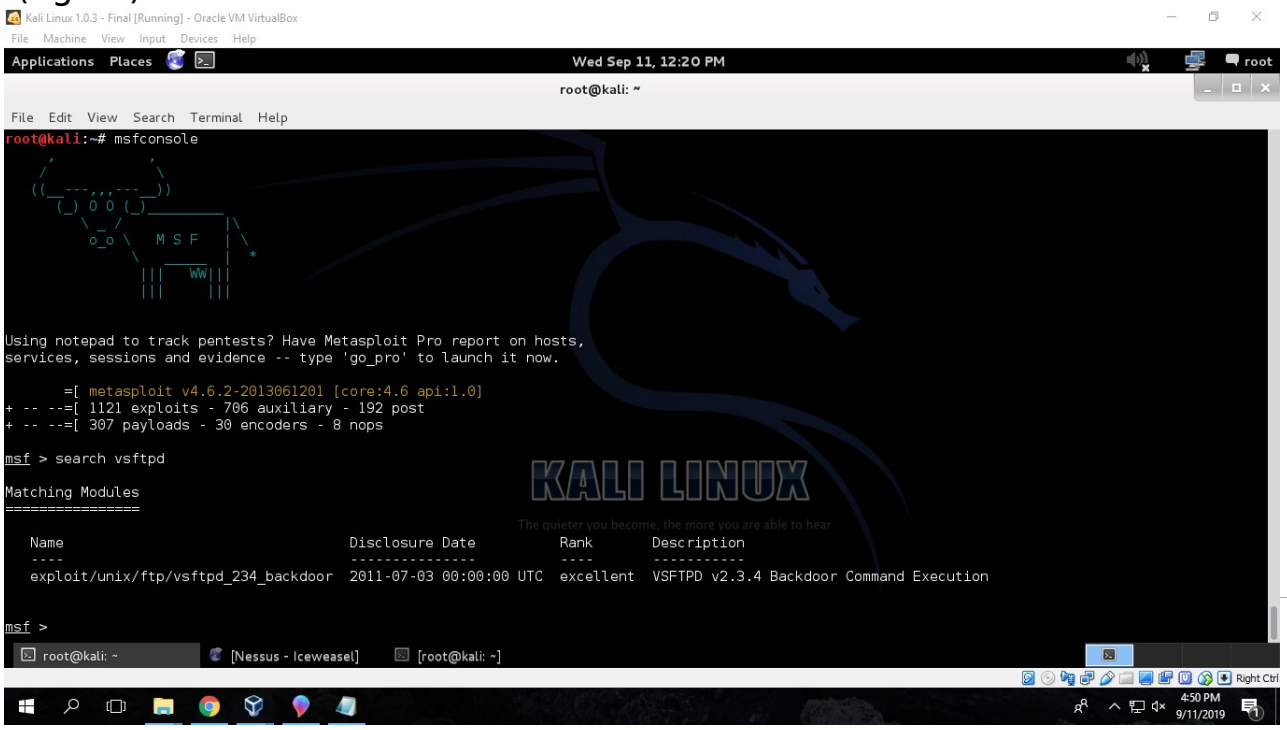
(in msf>) * search [vulnerability ID or Name]

in this case we are searching for the **vsftpd** as the result we can see some matching modules for the selected vulnerability. (fig 16)

We have to use the best ranked exploitation to have best chance in successful attack. In here we are using **VSFTPD v2.3.4 Backdoor Command Execution** exploit to create a shell and have access to the windows machine. We can select the path of the exploitation and use it in msfconsole.

***use exploit/unix/ftp/vsftpd_234_backdoor** (fig 17)

(fig 16)

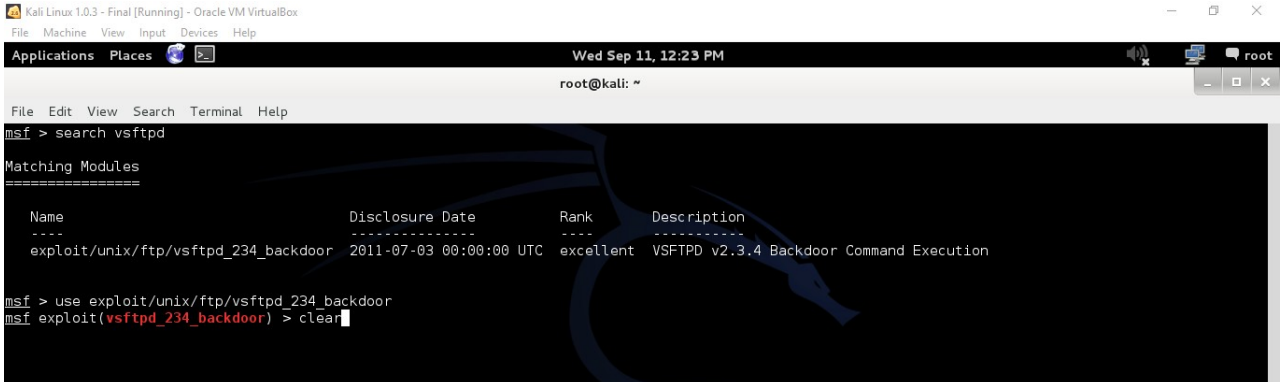


By typing ***show options** we can see the option list that available for the exploit and we have to assign the target IP (Windows 2000) with, ***set RHOST [Target IP Address]**

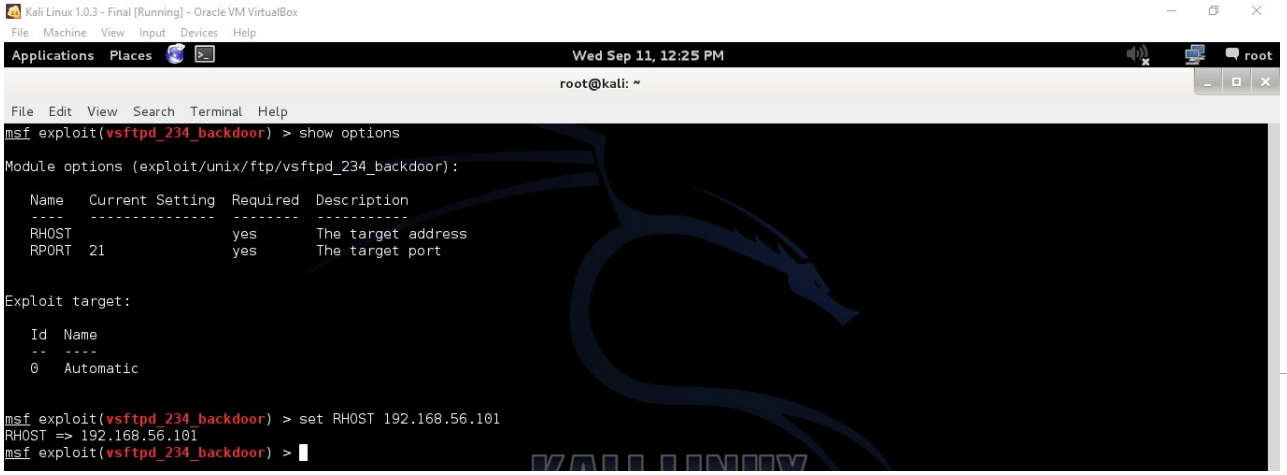
It will be set for the IP address that we ave given and we just have to exploit the whole thing by typing, (fig 18)

***exploit** or ***run** in the msfconsole. Then it will create a shell from an available port for us. We can manipulate the files using that shell. (fig 19)

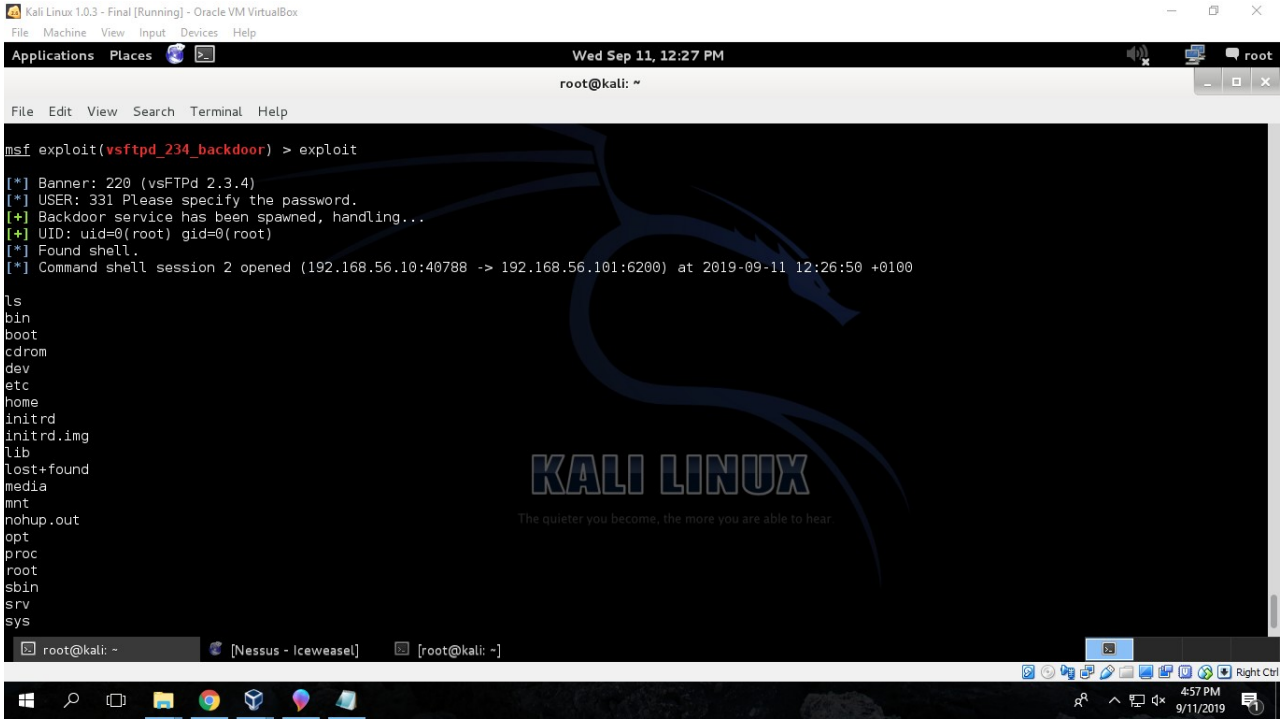
(fig 17)



(fig 18)



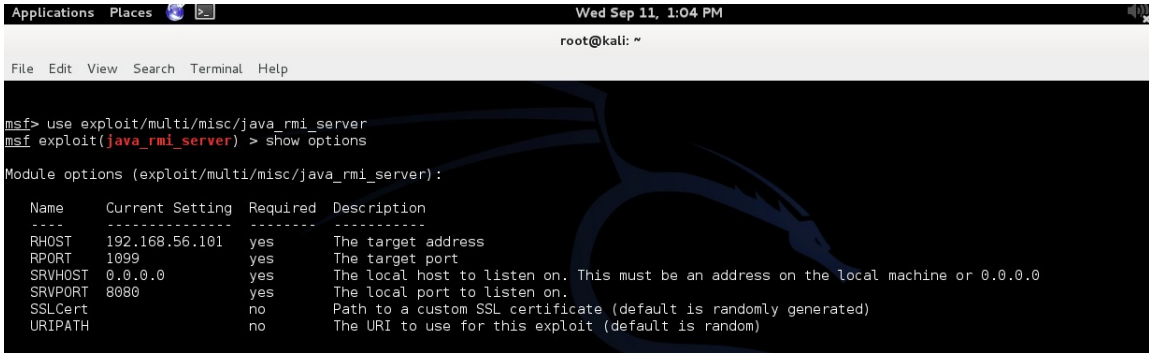
(fig 19)



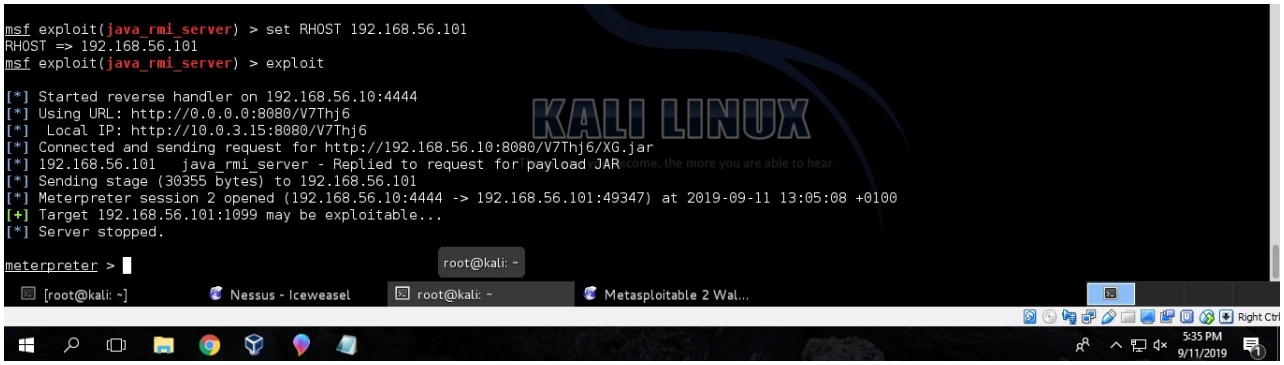
****

There is a vulnerability in Java server in Metasploitable called as **Java RMI Server Insecure Default Configuration Java Code Execution**.
With right exploit we cant create a shell in the Metasploitable.
There is an exploit available in msfconsole to this.
***use exploit/multi/misc/java_rmi_server**

This module takes advantage of the default configuration of the RMI Registry and RMI Activation services, which allow loading classes from any remote (HTTP) URL.



After setting RHOST value to target IP address, we can successfully exploit the vulnerability and access the files in the Metasploitable with a shell.

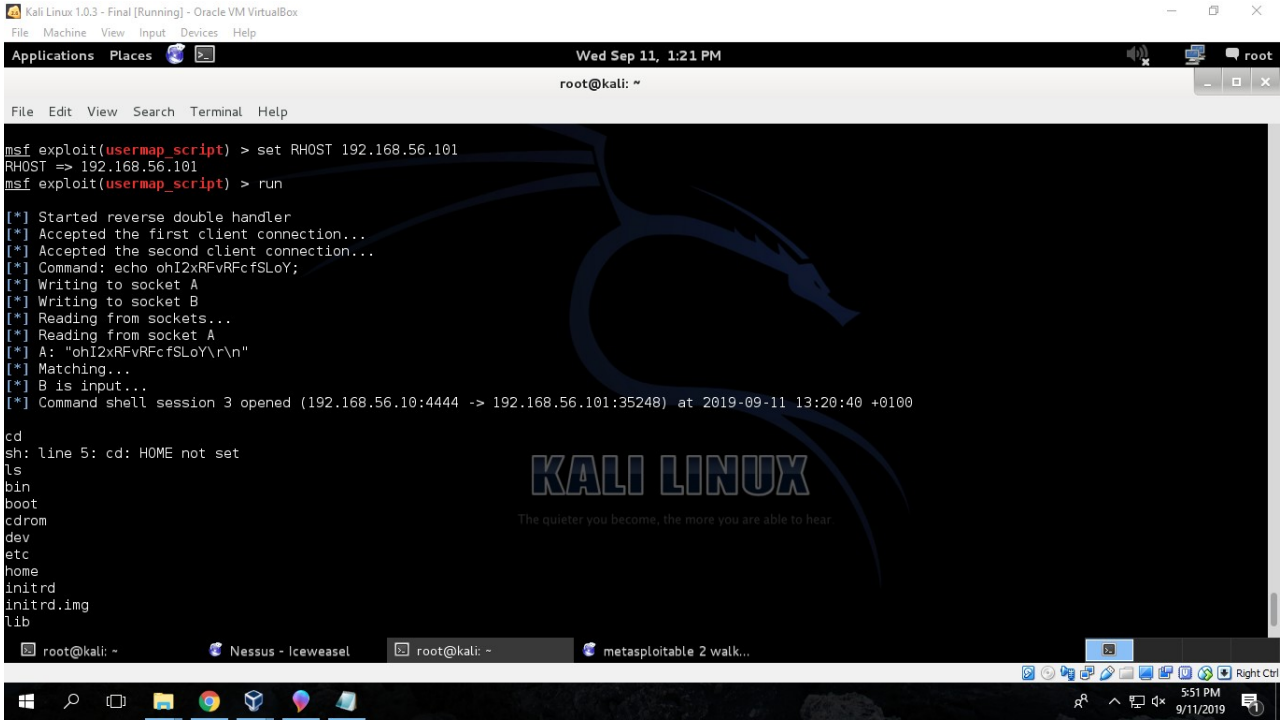


****

Finally there is another critical and attack-able vulnerability in Metasploit called as **Samba "username map script" Command Execution**
This is a vulnerability in Samba versions 3.0.20 through 3.0.25rc3 when using the non-default "username map script" configuration option. By specifying a username containing shell meta characters, attackers can execute arbitrary commands. No authentication is needed to exploit this vulnerability since this option is used to map usernames prior to authentication.

***use exploit/multi/samba/user_map**

After setting the target IP we just have to start our attack by typing exploit or run. It will create a shell in a available port and we can have access to the file system in target machine.



****