Rabindra Jaiswal(c7202628)

DIGITAL SECURITY

Explotation MS17\_010

CVE-2017-0147

Table of Contents

[Abstract 2](#_Toc68010873)

[Introduction 3](#_Toc68010874)

[Introduction of vulnerability 3](#_Toc68010875)

[Description of the vulnerability, Exploit and Attack software 4](#_Toc68010876)

[Software used for attacking 4](#_Toc68010877)

[Exploiting Vulnerability 5](#_Toc68010878)

[Anatomy of the attack 6](#_Toc68010879)

[Information Gathering 7](#_Toc68010880)

[Foot printing 7](#_Toc68010881)

[Scanning 7](#_Toc68010882)

[Recommendation for preventing attack 18](#_Toc68010883)

[Related Software 18](#_Toc68010884)

[Conclusion 19](#_Toc68010885)

[References 20](#_Toc68010886)

# 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 |
| * 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 Piece (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 Square one.0 (SMBv1) server, the most severe of the vulnerabilities can allow further code execution. The way the Microsoft Service Message Piece 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 Square 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.

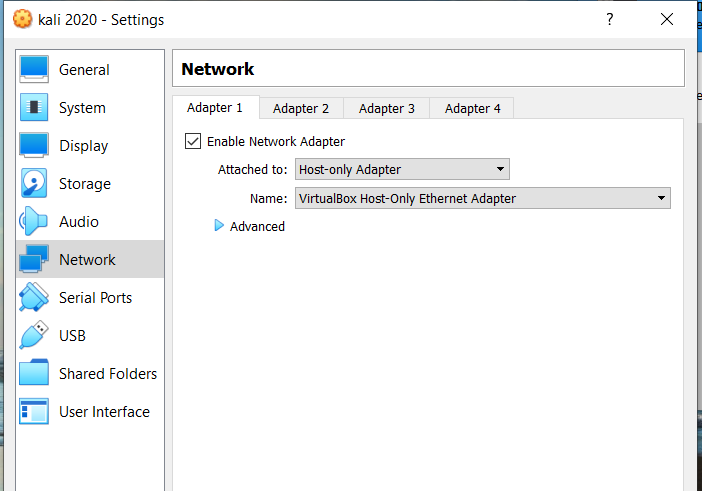
This article makes use of Metasploit for a code execution exploit. It's an open supply consistency that enables an intruder to manipulate weaknesses that have already been detected, checked, confirmed, and recorded. It contains a payload known as meterpreter, which is used to communicate between any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

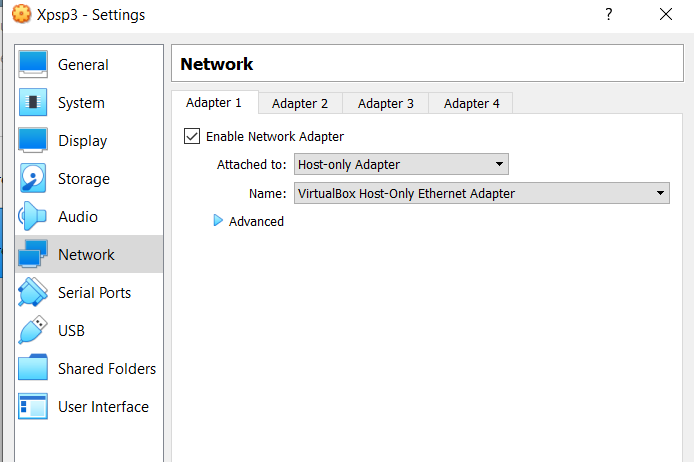
# Exploiting Vulnerability

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

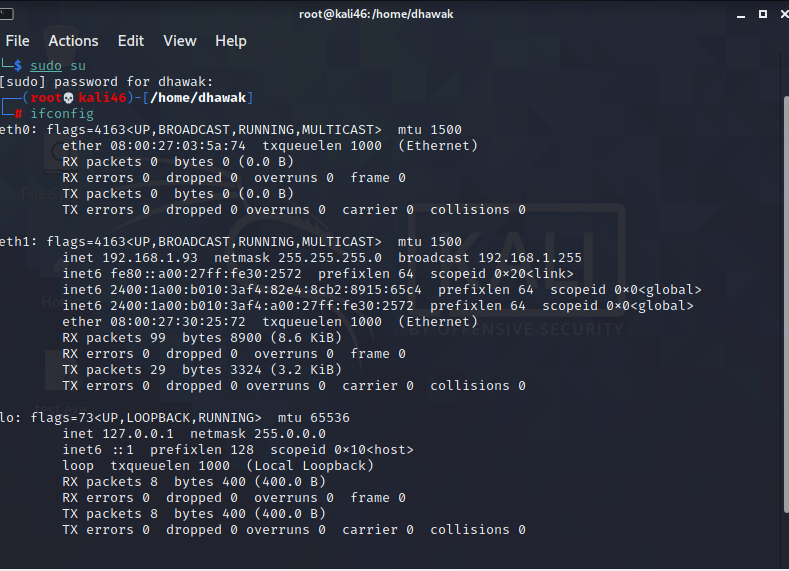
Gathering the data implies gathering diverse information against the gadget which is reaching to be assaulted. Different strategies are utilized to collected the information. A parcel of the focused-on framework information collection procedures are social designing ambushes, hacking, organize ranges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

## Foot printing

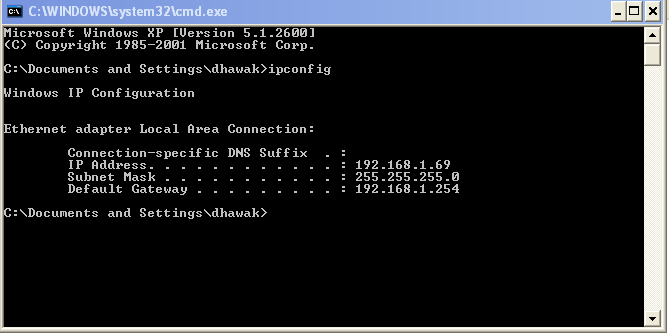
Foot printing (also known as observation) is a technique for collecting information about computing frameworks and the materials they interact with. A programmer might use a variety of devices and technologies to push this info. This knowledge is immensely helpful to a programmer trying to break a whole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

## Scanning

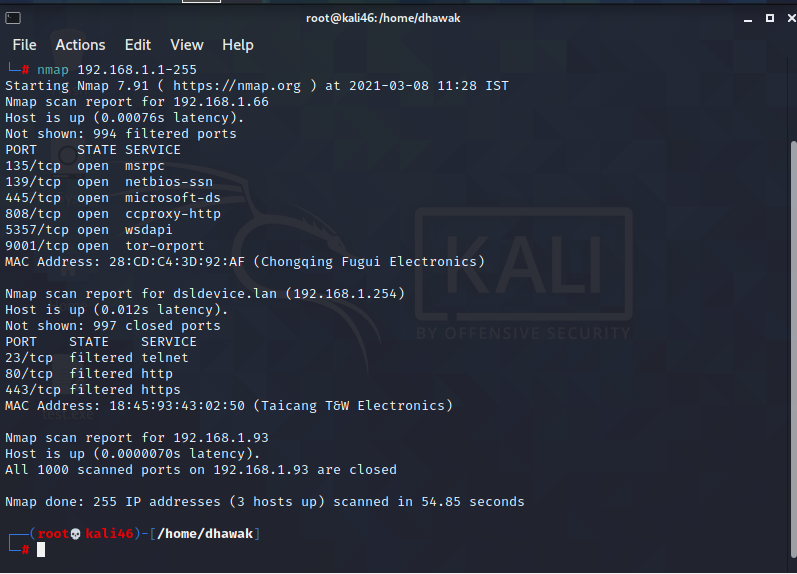
Nmap (Network Adapter) can be used to recognize ports and stable tools used to scan windows in order to find open ports for attack. Nmap is a free and open source scanner that sends packets to a target computer and analyzes the responses.



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

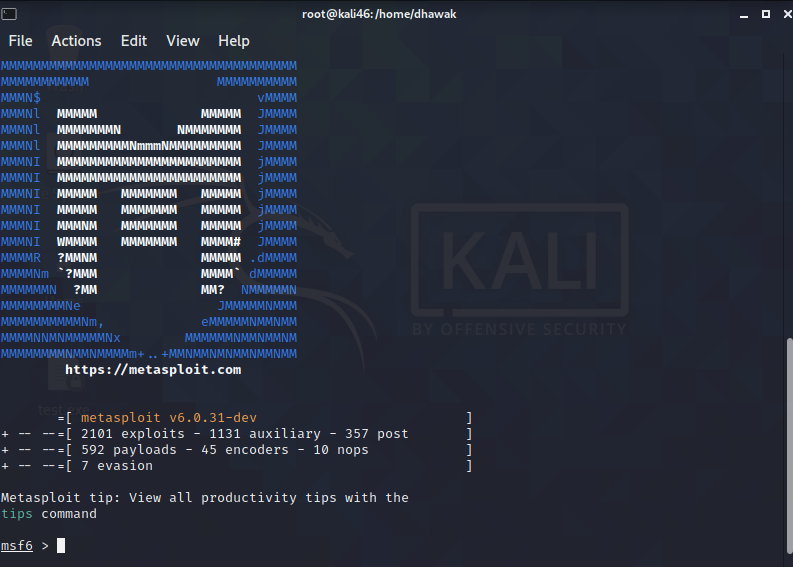


On the target machine after running the command ‘ipconfig’ address of the victim machine is 192.168.1.69.



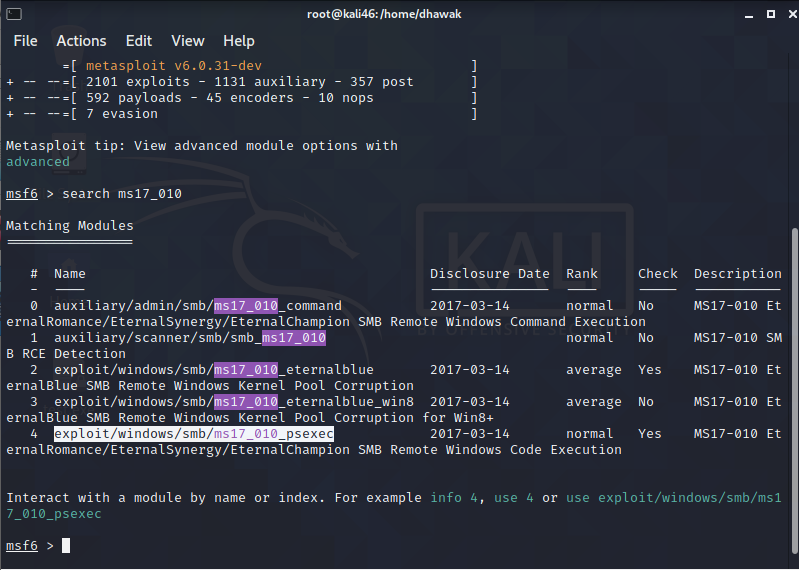
We can see that the most of the port are open in the above diagram. NMAP has a variety of filters, but the search for complex IPs is always done in PC.

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



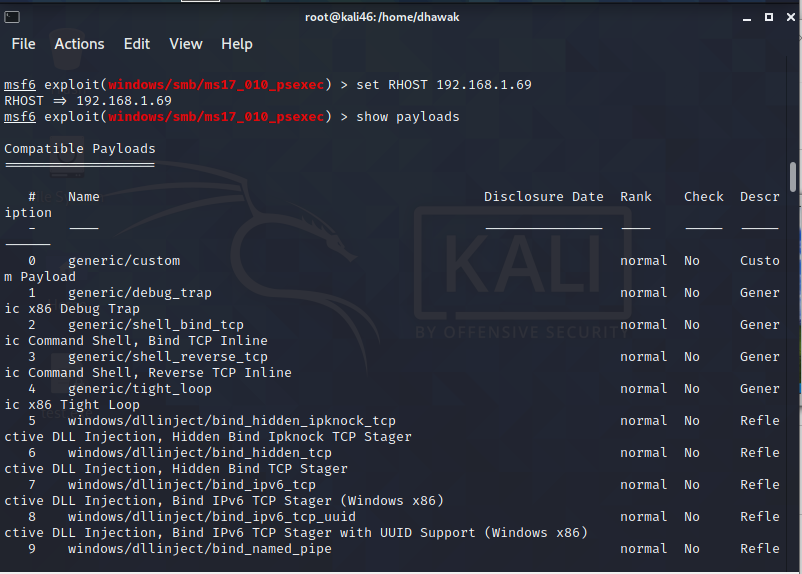
With the help of msfconsole command we are able to work with the metaspolit framework for further exploitation.

Metasploit is a penetration testing application that simplifies the method of hacking. For many attackers and defenders, it's a must-have weapon. Choose an exploit, a payload to drop, and enter Metasploit at your target.



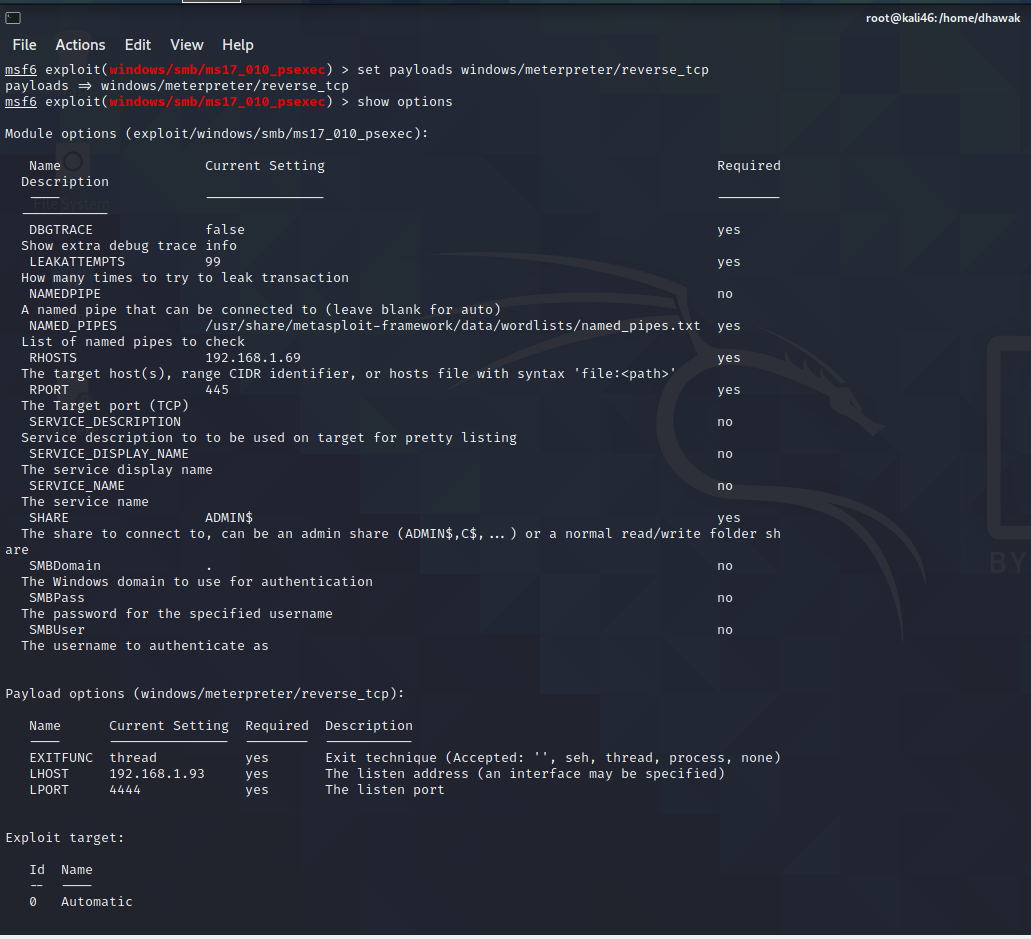
Search MS17\_010 command help us to locate the exploit which is exploit/windows/smb/ms17\_010\_psexec as shown in the above figure which is obtained by searching vulnerability in the windows XP.





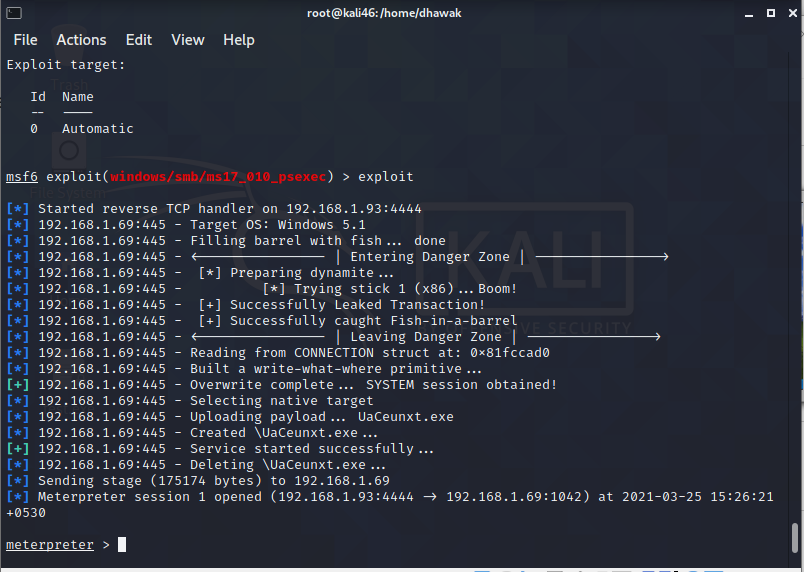
RHOST refers to the IP address of the target host which we are going to attack which is IP address of the XP 192.168.1.69.

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



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.

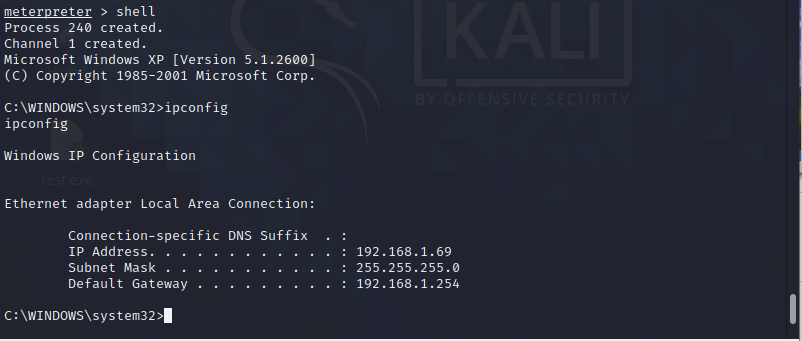


Exploit command is proceeded. (Gizmosphere, 2020) said that “Exploits are software programs that were specifically designed to attack systems with vulnerabilities.”. Meterpreter session is started to perform post exploitation.

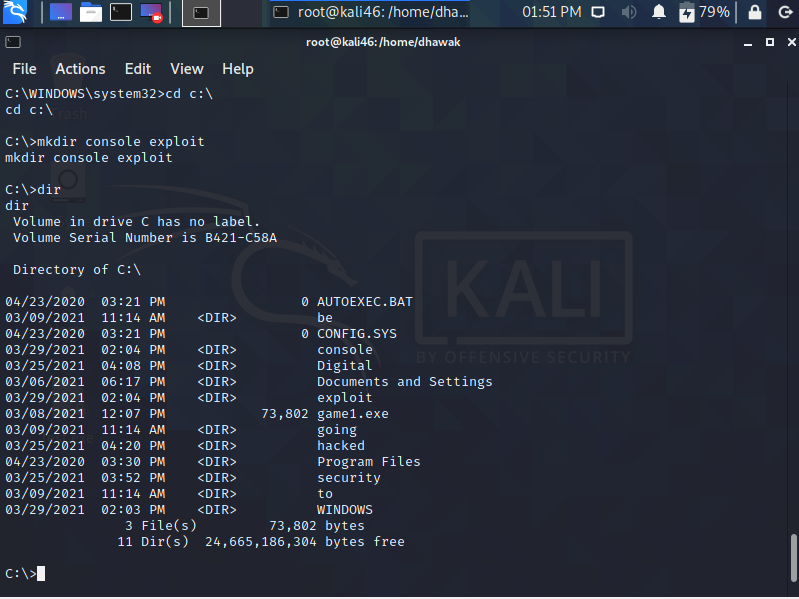
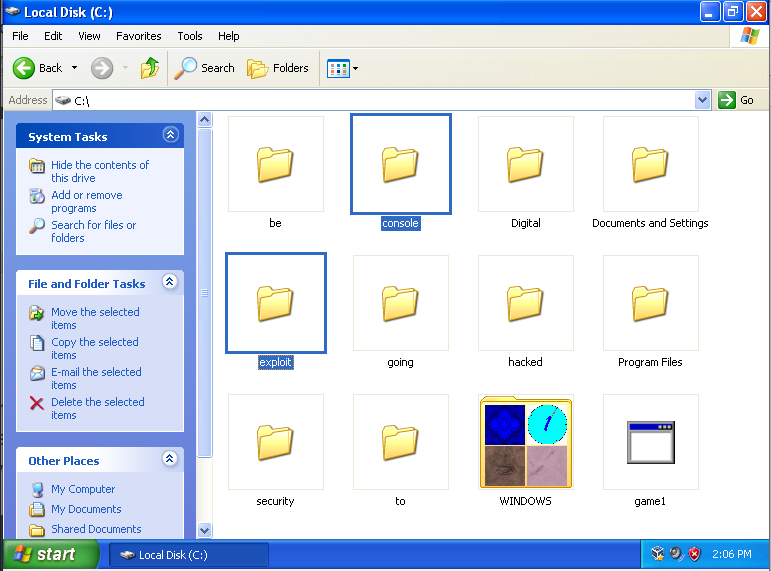
Post exploitation

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.

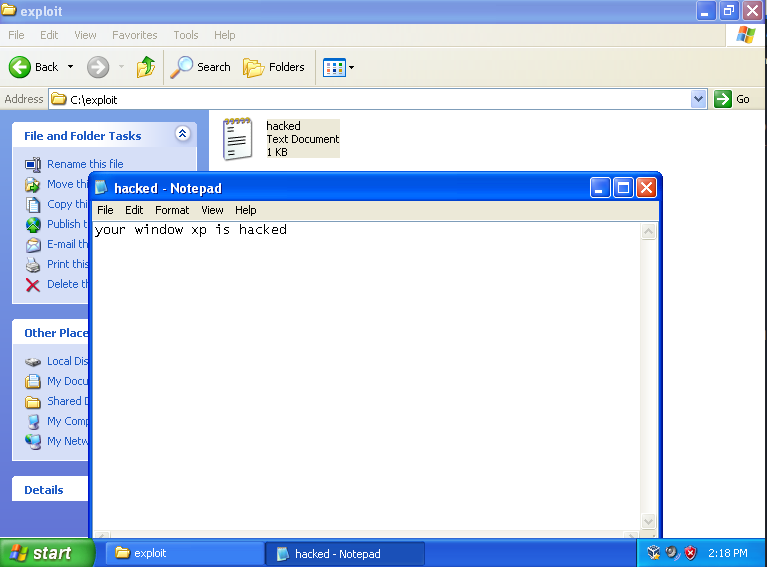
The aggressor must penetrate the casualty shell to perform post misuse. As a result, we end up creating a Meterpreter session for this particular stage where the victim machine has been literally undermined. Meterpreter is a Metasploit attack payload that provides an understandable shell from which an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



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.

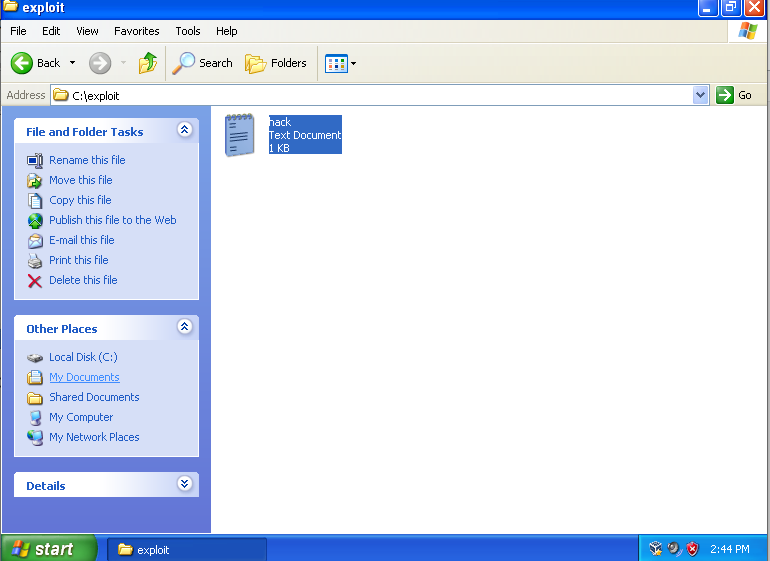
The fig capture shows the C:\ drive of the XP. Where we create directory called console and exploit as shown in the figure.in the window XP also we can see the directory hacked has been crated. Similarly, when we passed the command dir. we can see all the directory of window XP C:\ drive.



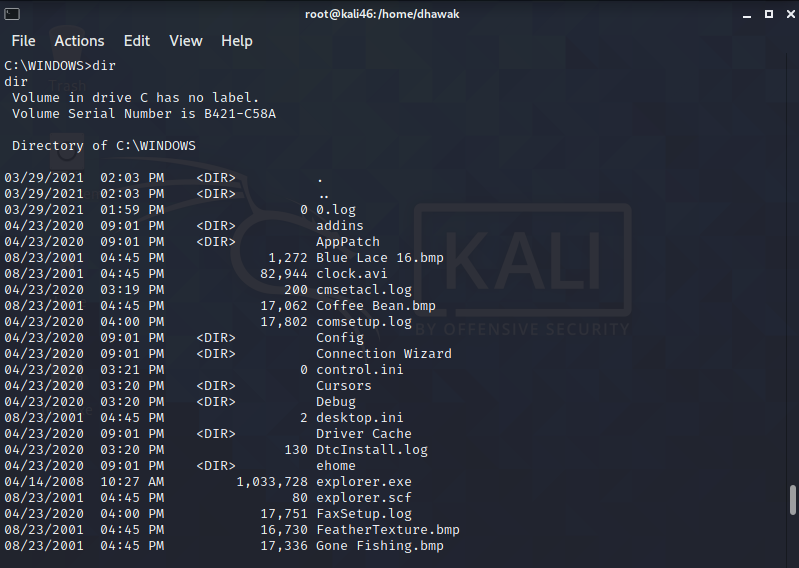
Following content has been written in file we made in the directory.



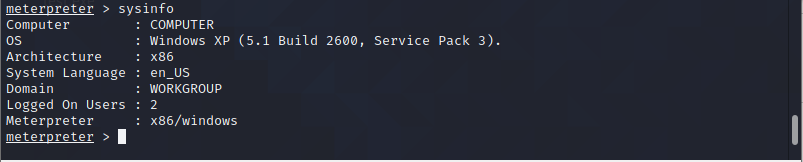
Renaming the file hacked.txt as hack.txt



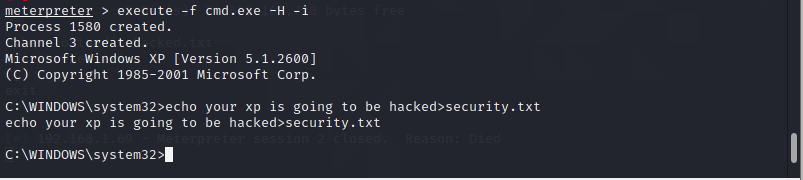
If we stay in the meterpreter session, we can also execute the post-exploit procedures. That is, we do not need to type the shell command to obtain access to the victim's computer. The meterpreter session's casualty can also be dealt with.



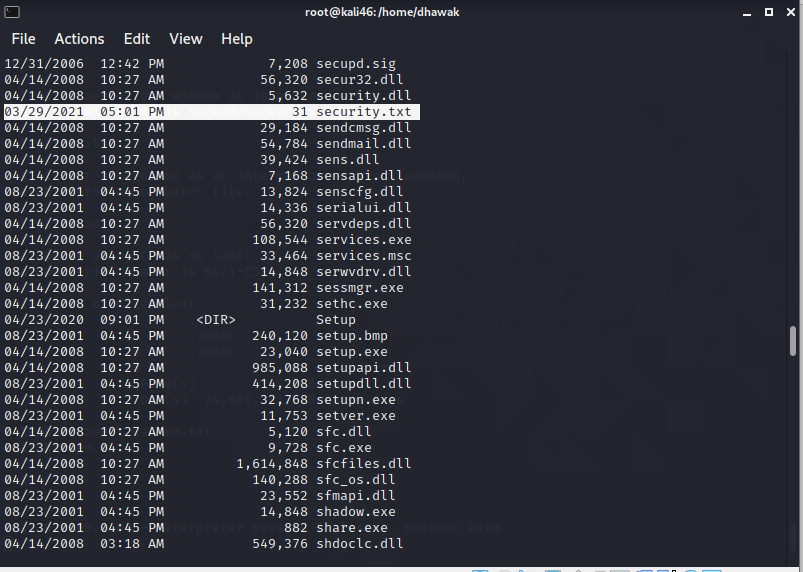
As a result, the Targeted computer can be managed through the command shell by obtaining it. If we stay in the meterpreter session, we can also execute the post-exploit procedures. That is, we do not need to type the shell command to obtain access to the victim's computer. The meterpreter session's casualty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

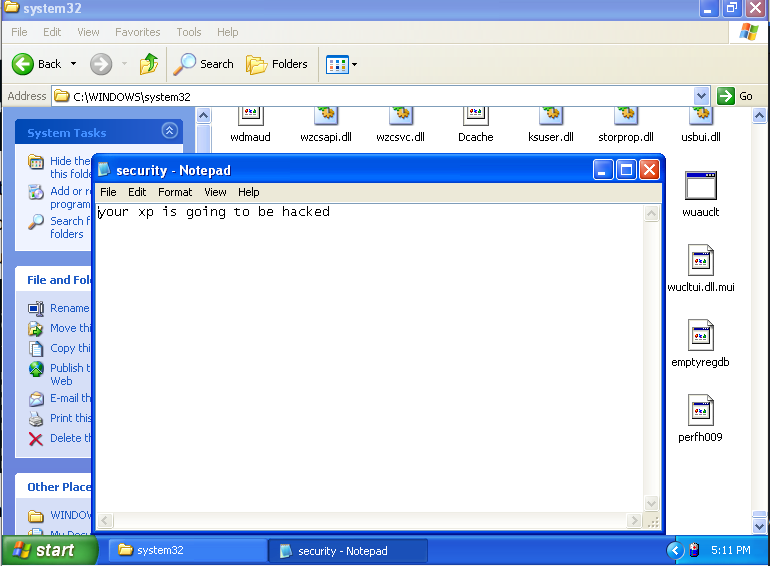


By passing the sysinfo command we can know the victim machine information.



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.

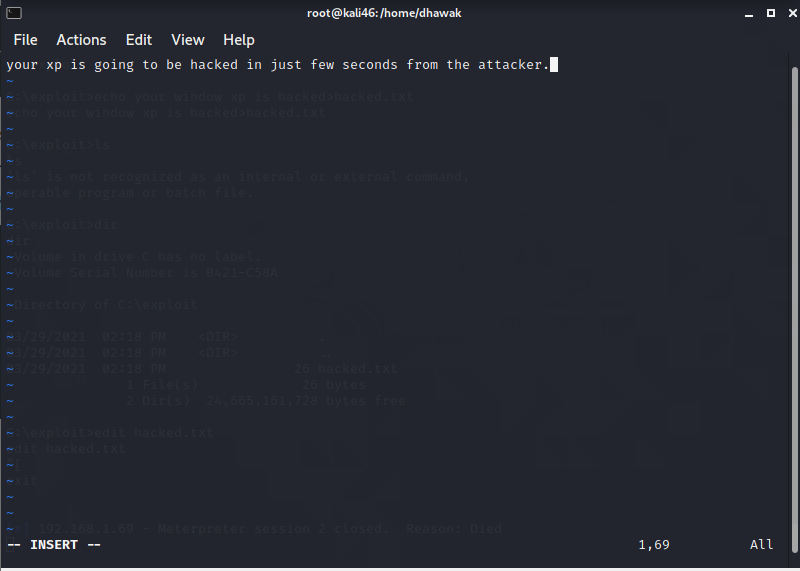




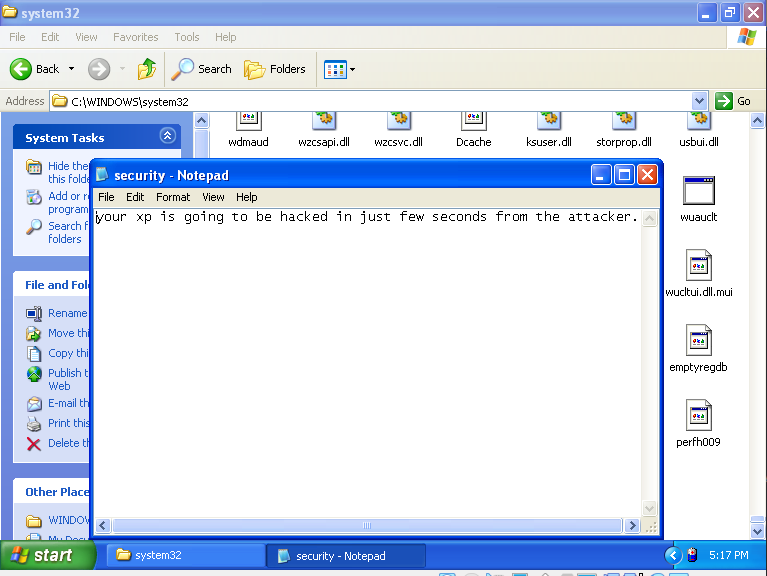
In XP you can see the document we crated and its content which we have written in it.

C:\Users\Dell\OneDrive\Pictures\Saved Pictures\ds sssssss\New folder\edit security.PNG

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



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.



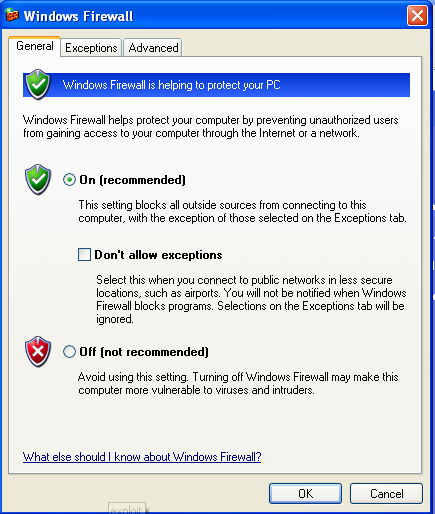
As you can see the content have been already updated in the victim computer as we execute it on our attacker command shell.

C:\Users\Dell\OneDrive\Pictures\Saved Pictures\ds sssssss\New folder\cat.PNG

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 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].Availablefrom: https://www.rapid7.com/db/vulnerabilities/msft-cve-2017-0147 [Accessed 28th March 2021]