Volume 8, No. 3, March – April 2017

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Penetration Testing Exploitation of Windows XP SP0

Ms. Gurline Kaur
Assistant Professor
P.G. Dept. of Comp. Sci. & Appls.
Kanya Maha Vidyalaya, Jalandhar , Punjab, India

Navjot Kaur
Student, M.Sc. IANS, Sem IV
P.G. Dept. of Comp. Sci. & Appls.
Kanya Maha Vidyalaya, Jalandhar , Punjab, India

Abstract: A penetration test is performed on an operating system with the expectation of discovering security weaknesses and exploiting target OS. The goal of this testing is to find all security vulnerabilities without any type of actually harming the computer system. In this research paper, we discuss the some phases of penetration testing on operating system. We are using some tools and techniques to penetrate the target system by using Nmap, Metasploit (msfconsole) and Meterpreter. We will make remove folders in host OS and also make and delete folders to the target OS through LINUX commands. And we will shut down the target operating system with using Linux commands. In this, we are using penetration testing tool to attack on particular operating system and to scan and also exploiting target OS. In the previous research paper, we had performed the work on scanning the target operating system with reconnaissance tool Nmap. In this research paper, we will work only on exploitations of our target operating system with Windows XP SP0 "Service Pack".

Keywords: Penetration Testing, VMware, Kali Linux, Nmap, Scanning, Metasploit, Meterpreter, Exploitation, msfconsole.

I. INTRODUCTION

Penetration testing is a sort of security testing that is utilized to test the weakness of an operating system. It is directed to discover the security shortcomings which may be available in the working framework. On the off chance that a working framework is not secured, then assailant can decimate or take approved access to that operating system. In any case, the primary concern is that the penetration tester is entirely unexpected from assailant. The penetration tester will have approval (authorization) from the proprietor of the computing assets that are being trying. In this paper, we penetrate Windows XP SP0. We will discuss how we can exploit and scan the target operating system and create changes in it with different tools and commands. In it, we use Nmap for scan and find the IP addresses of host operating system and the target operating system. We used Metasploit tool to exploit target operating system and Meterpreter tool to make and delete folders to the host OS and also the target OS. We used Meterpreter tool for shut down the target operating system.

II. SYSTEM SPECIFICATIONS

For perform our task we need to explained some system specifications which we used in this paper. In this paper we used two operating system and some tools to scan and exploit target operating system. These specifications are following:

A. ***Operating System:*** Kali Linux 2.6 / 3.x / 4.x (64-bit) and Windows XP SP0 (32-bit).

B. ***Tools/Software:*** VMware, Nmap, Metasploit and Meterpreter.

a. VMware

VMware virtualization gives you a chance to run different virtual machines on a solitary physical machine, with each virtual machine sharing the assets of that one physical PC over various conditions. VMware is a virtual machine programming which giving a virtual PC condition, makes it workable for more than one occurrences of the working frameworks to keep running on a similar server.

b. Nmap

Nmap ("Network Mapper") is a free and open source utility for system security and auditing. It is the world's leading port scanner and popular part of our host security tools. With the help of Nmap tool we can find ip address to host operating system and also our target operating system. It will also used for finding and misusing vulnerabilities in a network.

c. Metasploit

Metasploit is an open source computer security tool. It's a powerful tool used for penetration testing. Metasploit is not a single tool; it is a framework which utilized for creating and executing exploit code against a remote target. Metasploit has many user interfaces but in our paper we used only msfconsole for accessing metasploit.

d. Meterpreter

Meterpreter is a tool which we used to make and delete the folders on target operating system Windows XP SP0. After exploitation we used Meterpreter and perform our actions on target operating system. We will enter in a whole new environment which provide by meterpreter.

III. LITERATURE SURVEY

In [1] an overview of penetration testing, Aileen G. Bacudio, Xiaohong Yuan, Bei-Tseng Bill Chu and Monique Jones provided an overview of penetration testing. They discuss the benefits, the strategies and the methodology of conducting penetration testing. The methodology of penetration testing includes three phases: test preparation, test and test analysis. The test phase involves the following steps: information gathering, vulnerability analysis, and vulnerability exploit. This paper further illustrates how to apply this methodology to conduct penetration testing on two example web applications.

In [2] Evaluation and Taxonomy of Penetration Testing, Arpita Tewai and Arun Kumar Misra discussed penetration

testing has been performed mid/large cooperate organization pointing to certain conflicts in the requirements of testing. They also discussed about the processes and methodologies of today's trends that also undergo continuous changes due to rapid technological developments. Some complications in penetration testing have also been highlighted and requirements for adopting the technique in modified way have been discussed.

In [3] Penetration Testing: A Roadmap to Network Security , Mr. Nitin A. Naik, Mr. Gajanan D. Kurundkar, Dr. Santosh D. Khamitkar, Dr. Namdeo V. Kalyankar explained methodology and methods behind penetration testing and illustrate remedies over it, which will provide substantial value for network security Penetration testing should model real world attacks as closely as possible. They have given information about the penetration testing, its methodologies and its application. Highlights how an experienced security consultant is necessary for the good penetration and role of him to give security system to the host machine by expecting the security attacks.

In[4] Daisy Suman, Sarabjit Kaur and Geetika Mannan have suggested , a penetration test generally involves the use of attacking methods conducted by trusted persons that are also used by aggressive intruders or hackers. Pen tests can be automated with software applications. Penetration testing can be performed manually. Penetration tests are an brilliant method for determining the strengths and weaknesses of a network consisting of systems and network devices. However, the process of penetration test is composite, and if it is taken out carelessly then it can have fatal effects.

In [5] Emily Chow has suggested that Ethical hacking and penetration testing is a defensive technique which consists of a chain of legitimate tools that recognize and exploit an organization's security weaknesses. It uses the identical or related mechanism of malicious hackers to attack key vulnerabilities in the company's security system, which then can be mitigated and closed. These tests reveal how simple an organization's security controls can be penetrated, and to obtain contact to its confidential and sensitive information asset by hackers.

In [6] "SWAM: Stuxnet Worm Analysis in Metasploit", Rahat Masood, Um-e-Ghazia, and Dr. Zahid Anwar have showed the real time simulation of first three vulnerabilities of Stuxnet worm using Metasploit Framework 3.2 and analyze their results. A real time scenario is established based on some assumptions. Stuxnet is the first worm that mainly targets ICS using zero day vulnerabilities. It can more fastly propagate in real industrial environment having large number of unpatched systems and cause a lot of damage to heavy machinery. For the current project they had done simulations through dummy malicious Stuxnet exe files.

In [7] "Protection against Penetration Attacks using Metasploit", Himanshu Gupta and Rohit Kumar have proposed a system to counter the attacks by these frameworks, especially Metasploit. They involved proposal of a system that is able to block the metasploit attacks in specific cases otherwise alert the administrator. The proposed system uses a network monitoring application which can able to monitor the connection attempted to the host system and respond according to algorithm used in system.

In [8] "Automated Planning for Remote Penetration Testing", Lloyd Greenwald and Robert Shanley have considered the problem in designing a penetration test plan automatically that can be executed remotely, without no or prior knowledge of the target machine or network. They develop a methodology for generating and executing remote test plans that takes into account the ambiguity of using remote tools both to gain required knowledge of the system and to provide the pen-testing actions.

IV. IMPLEMENTATION DETAILS

In implementation details we will work on Nmap, metasploit (msfconsole) and meterpreter for find IP addresses, for exploitations and control access on the target window. The implementation details of above tools are following:

A. Nmap

Nmap is a security scanner, used to discover hosts and services on the operating system. It can also find ip address of own target operating system. In this tool we use ***#ifconfig*** for details of IP addresses and ***#netdiscover –r 192.168.100.0/24*** and we will see this type of output:

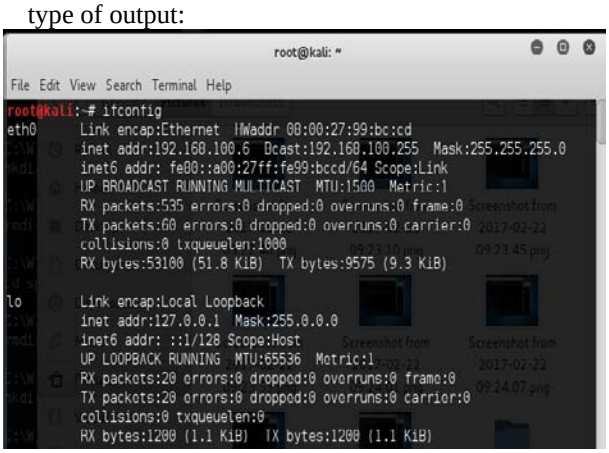

Figure 1: Find local host IP address

The output of this command is 192.168.100.6. It has shown us the IP address of our host operating system.

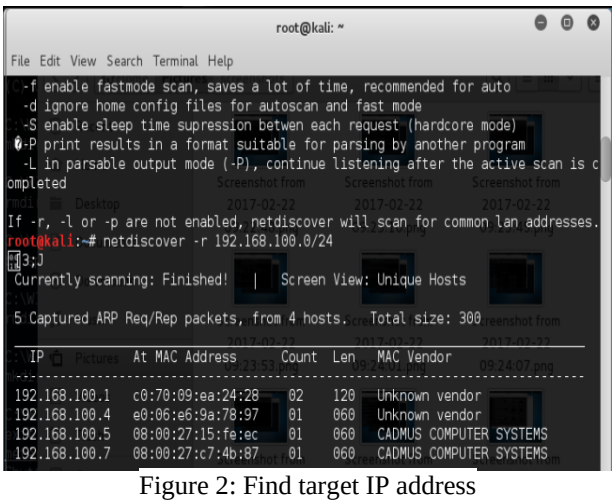

Figure 2: Find target IP address

This command has shown us the IP address of our target operating system which is 192.168.100.5. It is also showing some details as IP address, MAC address, Count, Len and MAC vendor in a tabular form.

B. Metasploit

In Metasploit framework we will use msfconsole interface for access the Metasploit. Using of msfconsole a metasploit window will be launched.

a. Msfconsole: We will simply type ***#msfconsole*** and shown this window:

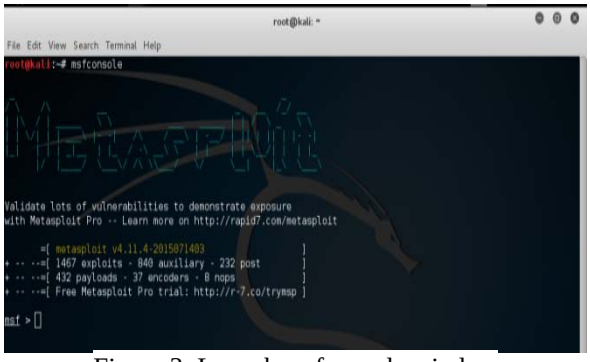

Figure 3: Launch msfconsole window

This output shows the Metasploit window will be launched with the implementation of #msfconsole command.

b. Search dcom*:* After that we give a command #msf > search dcom for find the path of our remote target to hack the Windows XP SP0. After that hack Windows XP SP0 using metasploit.

c. Use exploit and set PAYLOAD: Now once we get the msf prompt, type the below and look for the module ***#exploit/windows/dcerpc/ms03_026_dcom*** and the exploit is loaded, we will set the payload for the above selected exploit. In our scenario will be using reverse TCP payload.

Figure 4: Exploit Window and Set Payload

In this output, target will be exploited and shows the vulnerability named "ms03_026_dcom". And also shows the Payload of target OS.

d. *Set LHOST and RHOST:* Now we have to set local host and remote host to listen. Type the given command:

#msf > set LHOST 192.168.100.6

#msf > set RHOST 192.168.100.5

e. *Exploit:* Now finally start to exploit. Run the command exploit. And our session will be open.

#msf > exploit

Figure 5: Exploit

In this command after exploitation, Meterpreter session will be open.

C. Meterpreter

After exploitation we perform our actions on Windows XP SP0.

a. Ps command: Now we use ps command for viewing the processes running on the system. We will entered in Meterpreter which provide us whole new environment.

#meterpreter > ps

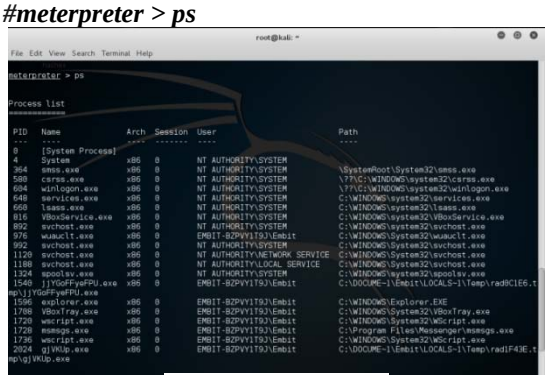

Figure 6: Process list

This output shows us the whole list of running process on the system.

b. *Getpid:* Then we using getpid (get process identification) for returns the process ID of the current process.

#meterpreter > getpid

c. Migrate: After that we will use the 'migrate' command post module, migrate to another process on the target.

#meterpreter > migrate 1324

Figure 7: Migrate process

This output shows the migrate 1324 which we will choose into process list and it will be migrated successfully.

d. Shell: Then we type shell command get started with another channel. It is a user program or it is an environment provided for user interaction.

#meterpreter > shell

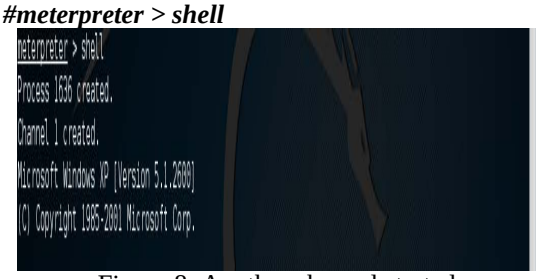

Figure 8: Another channel started

e. *Entered in Windows XP SP0 C:\WINDOWS\system32>:* After created a channel we will entered in Windows XP SP0***'C:\WINDOWS\system32>'*** and perform following work:

i. ***Windows named folder:*** First, we will enter in Windows named folder.

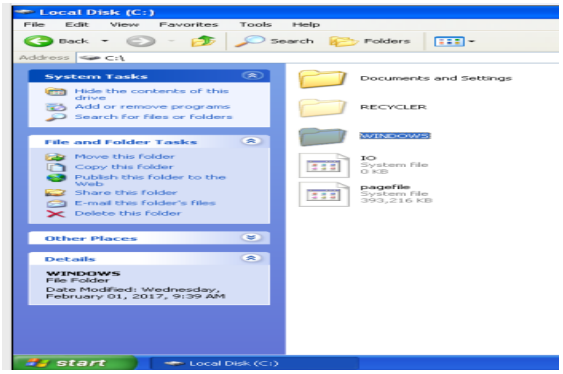

Figure 9: Entered in Windows named folder

ii. ***System 32 named folders:*** Then we will enter in system 32 named folder.

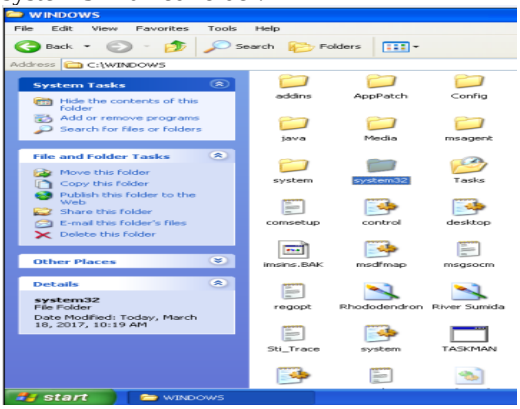

Figure 10: Entered in System 32 named folder

iii. ***Mkdir command:*** In this path we make a 'messages' named directory.
#C:\WINDOWS\system32>mkdir messages

iv. ***Rmdir command:*** Then we using 'rmdir' for remove the directory which we made.
#C:\WINDOWS\system32>rmdir messages

v. ***Cd command for entered in spool named directory:*** Then we entered in 'spool' named directory with the help of 'cd' command. This directory exists by default in Windows XP SP0.
#C:\WINDOWS\system32>cd spool

vi. ***Mkdir PRINTERS:*** In 'spool' named directory we will remove a 'PRINTERS' named folder.
#C:\WINDOWS\system32\spool>rmdir PRINTERS

vii. ***Mkdir LAPTOPS:*** Then we make a 'LAPTOPS' named folder in 'spool' named directory.
#C:\WINDOWS\system32\spool>mkdir LAPTOPS

viii. ***Exit:*** After that we will exit into ***#C:\WINDOWS\system32\spool*** named directory with the help of 'exit' command.
C:\WINDOWS\system32\spool>exit

ix. ***Shut down the target OS:*** In the end, we will uses 'shut down -i' command for shutdown our target

x. OS. And then our 'Meterpreter' session will be closed.
#meterpreter > shutdown –i

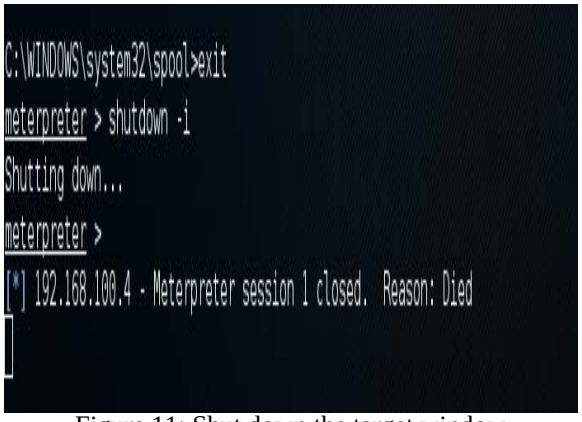

Figure 11: Shut down the target window

In the end, this output shows the target OS will be shutdown and then Meterpreter session will be closed.

V. SYSTEM REQUIREMENTS

We recommend the following computer system requirements:

Manufacturer: Microsoft Corporation

Processor: Intel® Core(TM) i5-2520M CPU @ 2.50GHz

Installed memory: 4.00 GB (3.90 GB usable)

System type: 64-bit Operating system, x64-based processor

VI. CONCLUSION

In this research, we use efficient penetration testing tool like Nmap to find IP addresses of own operating system and also target operating system. We use Metasploit to find vulnerabilities and weaknesses in Windows XP SP0 operating system. We use vulnerability **ms03_026** that send and receive information between clients and servers on target operating system. We also use Meterpreter to delete and make folders on local host operating system and also target operating system. We also perform the work on shut down the target OS.

VII. REFRENCES

[1]. Aileen G. Bacudio, Xiaohong Yuan, Bei-Tseng Bill Chu, Monique Jones "An Overview of Penetration Testing", International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6, November 2011.

[2]. Arpita Tewai and Arun Kumar Misra, "Evaluation and Taxonomy of Penetration Testing", International Journal on Recent and Innovation Trends in Computing and Communication Volume: 3, Issue: 8.

[3]. Mr. Nitin A. Naik, Mr. Gajanan D. Kurundkar, Dr. Santosh D. Khamitkar, Dr. Namdeo V. Kalyankar, "Penetration Testing: A Roadmap to Network Security", Journal Of Computing, Volume 1, Issue 1, December 2009.

[4]. Daisy Suman, Sarabjit Kaur and Geetika Mannan, "Penetration Testing", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 3, Issue 10, October 2014.

[5]. Emily Chow, Ethical Hacking & Penetration Testing, July 1, 2011.

[6]. Rahat Masood, Um-e-Ghazia and Dr. Zahid Anwar, "SWAM: Stuxnet Worm Analysis in Metasploit", IEEE, 2011.

[7]. Himanshu Gupta and Rohit Kumar, "Protection against Penetration Attacks using Metasploit", IEEE, 2015.

[8]. Lloyd Greenwald and Robert Shanley, "Automated Planning for Remote Penetration Testing", IEEE, 2009.