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 – Reconnaissance with NMAP Tool

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 testing is performed on a working framework (operating system) with the desire of finding security shortcomings and misusing target OS. The objective of this testing is to discover all security vulnerabilities with no sort of really hurting the PC framework (computer system). In this research paper, we had discussed the scanning of target operating system Windows XP SP0 with using Nmap tool. We will use Nmap for finding the IP address of local host OS and also target remote host OS. We will also use some options of Nmap which will provide us more information about target ports and other useful services. The whole work is on Nmap and the attacks will be performed on Virtual machine (VMware). Kali Linux is the interface of using Nmap tool. In this research paper, we had worked with only Nmap tool for gathering the information of the target operating system. Nmap is used in reconnaissance or information gathering phase, which is the first phase of any penetration test.

***Keywords*:** Penetration testing, Vulnerabilities, Scanning, Nmap, Ports, VMware and Kali Linux.

I. INTRODUCTION

Penetration testing is the way of attempting to access assets without the information of usernames, passwords and other typical methods. The primary concern that isolates a penetration tester from an assailant is consent. The penetration tester will have consent from the proprietor of the processing assets that are being tried and will be dependable to give a report. The objective of a penetration test is to expand the security of the computing assets being tested. Nmap is a well known port examining tool. Port scanning is regularly a piece of the observation period of a penetration test or an assault. Sometime attackers will restrict their testing to a couple of ports while in different circumstances; they will filter every single accessible port. In this research paper Nmap works on finding IP addresses and gaining information about available services and ports on the OS.

II. SYSTEM SPECIFICATIONS

For performing our task we need to explain 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. Tool/Software: Nmap and VMware.

a) VMware

VMware virtualization gives 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 reviewing. It is the world's best port scanner and prominent piece of our host security instruments. With the assistance of Nmap device, we can discover IP address which can be used in our working framework. Nmap will help in finding the available ports and services. It will likewise be utilized for finding and abusing vulnerabilities in a system.

III. LITERATURE SURVEY

In [1] A Network Based Approach to Discover Security Vulnerability on Host System, Sandeep Kumar Yadav, Daya Shankar Pandey and Shrikant Lade discussed that a port scanner is a tool used by both system administrators and attacker(s) to identify vulnerabilities in operating systems. Nmap is a port scanner that takes an IP address of target machine or the host name and then finds the basic information related to it. It also finds the number of ports that are running on that particular host, number of ports that are opened, number of closed ports, services running on those ports, for instance, whether services are TCP-oriented or FTP-oriented. It also predicts the type of operating system being used on that particular host. The network topology of the scanned host is recorded in the graphical format which shows the various gateways through which the local machine accesses that particular remote host.

In [2] Port Scan - A Security Concern, Tariq Ahamad Ahanger explained that port Scanning is the name for the technique used to identify open ports and services available on a network host. It is sometimes utilized by security technicians to audit computers for vulnerabilities; however, it is also used by hackers to target victims. It can be used to send requests to connect to the targeted computers, and then keep track of the ports which appear to be opened, or those that respond to the request.

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] Vulnerability Scanners: A Proactive Approach to Assess Web Application Security, Sheetal Bairwa, Bhawna Mewara and Jyoti Gajrani discussed that Nmap is a port scanner that is used to scan the ports. it takes an IP address or the host name and then finds the basic information related to it. if an IP address is provided, it then finds the host to which it belongs to. it also finds the number of ports that are running on that particular host, number of ports that are opened, number of closed ports, services provided by those ports, for instance, whether services are tcp-oriented or ftp-oriented. It even predicts the type of operating system being used on that particular host. The topology of the scanned host is recorded in the graphical format which shows the various gateways through which the local machine accesses that particular remote host.

In [5] 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.

IV. IMPLEMENTATION DETAILS

In implementation details, we will work on Nmap tool for finding IP addresses of the local host and remote host. It will also scan the ports and services which are present in local and target OS. We will also work on Nmap options which will provide us information about working services and ports. The implementation details of Nmap are following:

A. Nmap:

In the Nmap tool we had worked on the following commands and options:

a. To start with Nmap, first we find IP address of our host machine used ifconfig at the command line:

#ifconfig

We have used ifconfig command to check the assigned IP address of our host machine. It will also display all the active interface details.

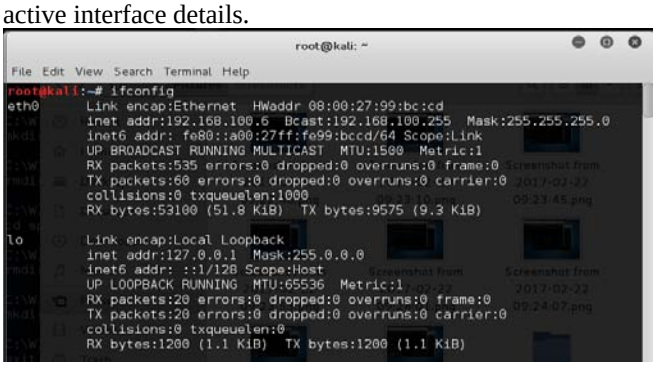

Figure 1: Find local host IP address

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

b. Using netdiscover command for find IP address of target OS

Now we will use netdiscover command for search the IP address of remote operating system with using –r option.

#netdiscover –r 192.168.100.0/24

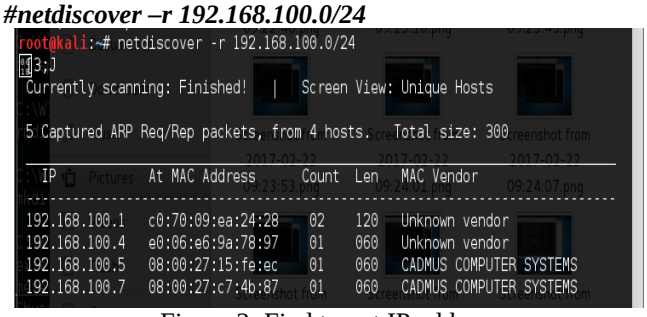

Figure 2: Find target IP address

The output of this command is 192.168.100.5. It has shown the IP address of our target remote OS. In this, we can see that it has shown an IP address, its MAC Address, Count Len and MAC Vendor in a tabular form.

c. Using Nmap command for target specifications, host discovery, scans techniques and etc

We are using Nmap command for details of Nmap options like target specifications, host discovery options, scan technique options etc.

#Nmap

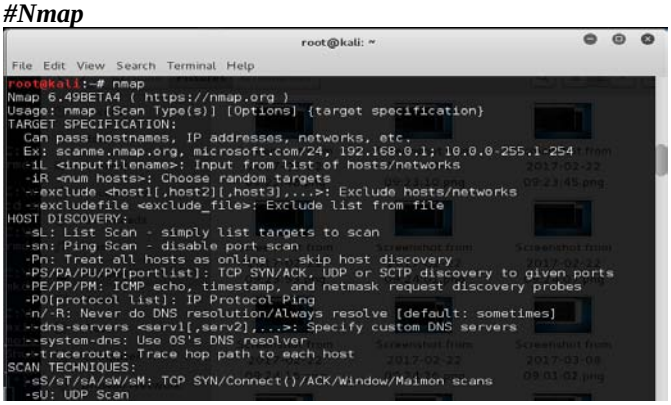

Figure 3: Using Nmap command

The #nmap command has shown all the options of Nmap. We can gather useful information about the target OS using these commands and options. This will help in the reconnaissance phase of penetration testing.

d. Using Nmap –sL [IP of target OS] for list scanning

This command simply generates and will display a list of IP addresses or hostnames without actually pinging or port scanning them with the help of –sL command. –s is used for scanning and L is used for the complete list.

#Nmap –sL 192.168.100.5

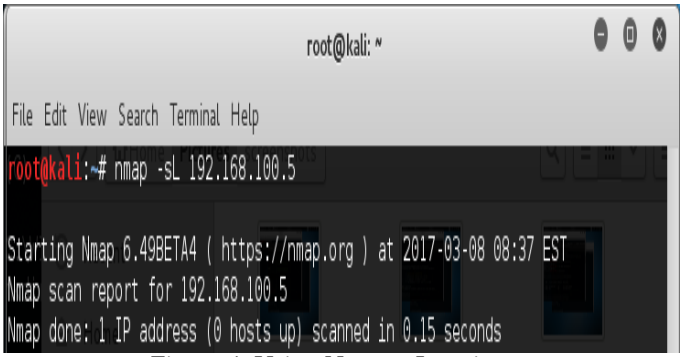

Figure 4: Using Nmap -sL option

e. Using Nmap -sn [IP of target OS] for ping scan

It is used for ping scanning to disable ports. Ping is a computer network administration software utility, which is used to test the reach ability of a host on an Internet Protocol (IP) network. –s is used for scanning and n is used for network, in this case for scanning the network.

#nmap -sn 192.168.100.5

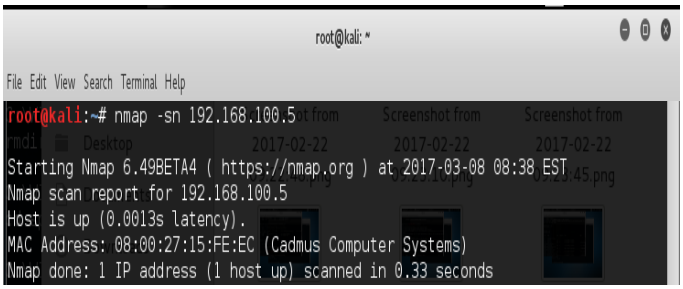

Figure 5: Using Nmap –sn option

This output shows the scanning of network. It will be used for ping scanning.

f. Using Nmap –PE [IP of target OS] for true ping (ICMP echo request) packet

This option uses a true ping (ICMP echo request) packet. It finds hosts that are up and also looks for subnet-directed broadcast addresses on your network.

#nmap -PE 192.168.100.5

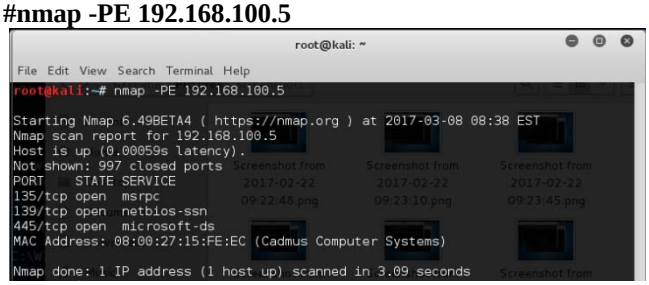

Figure 6: Using Nmap –PE option

The output shows the ICMP echo request and all the ports, State Services and the MAC address of target OS.

g. Using Nmap –Pn [IP of target OS] for scan selected ports

This option uses for scan selected ports - ignore discovery.

#nmap –Pn 192.168.100.5

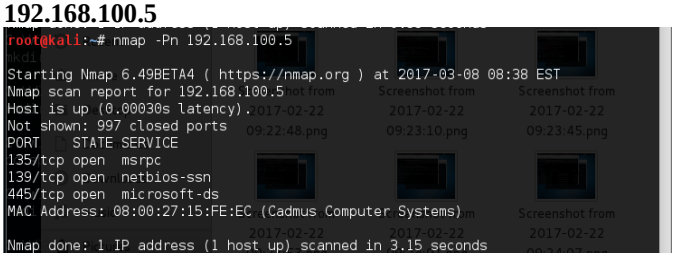

Figure 7: Using Nmap –Pn option

The output shows scan the selected network ports.

V. CONCLUSION

Penetration testing is very valuable technique to audit the security and defects in a particular operating system. A penetration testing is a method implied on a computer system with the intention of finding security flaws, potentially gaining access to it, its functionality and data. In this research paper, we had used an efficient penetration testing tool Nmap to scanning ports and finding the IP addresses of own operating system and also of the target operating system. It also works on searching the available open, close ports and available services.

VI. REFERENCES

[1]. Sandeep Kumar Yadav* Daya Shankar Pandey Shrikant Lade, "A Network Based Approach to Discover Security Vulnerability on Host System", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 12, December 2014.

[2]. Tariq Ahamad Ahanger, "Port Scan - A Security Concern", International Journal of Engineering and Innovative Technology (IJEIT) Volume 3, Issue 10, April 2014.

[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]. Sheetal Bairwa, Bhawna Mewara and Jyoti Gajrani, "Vulnerability Scanners: A Proactive Approach to Assess Web Application Security", International Journal on Computational Sciences & Applications (IJCSA) Vol.4, No.1, February 2014.

[5]. 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.