Analysis of Penetration Testing and Vulnerability in Computer Networks

Abid Khan
Research Scholar
Department of Computer Science & Engineering
Al-Falah University, Faridabad Haryana, India

Ruchi Parashar
Research Scholar
Department of Computer Science & Engineering
Al-Falah University, Faridabad Haryana, India

Neha
Research Scholar
Department of Computer Science & Engineering
Al-Falah University, Faridabad Haryana, India

Abstract

Vulnerability scanners are information security tools able to detect security weaknesses on hosts in a network. Secure hosts in a proactive manner. A proactive approach is considered to be better than reactive approaches followed by, for example, intrusion detection systems, because prevention is better than cure. There are many problems and disadvantages of currently available VSs, such as hampering system resources while conducting scans. This paper introduces a conceptual model for vulnerability forecasting. The model uses intelligent techniques to improve on the efficiency of currently available. The model aims to do vulnerability forecasting specifically by predicting the number of known vulnerabilities that will occur in the near future by using intelligent techniques and vulnerability history data. The model is tested by means of a prototype and an evaluation of the model's results is also provided in the paper.

Keywords- Hacking, Hacker, Ethical Hacking, Penetration Testing, Information Security

I. INTRODUCTION

A. Penetration Testing

It is a process to imitate all ways used by hackers to compromise a system. But with the difference it is purely ethical in deed so as to know in prior how a machine can suffer security breach attack.

B. Vulnerability Scanner

A vulnerability scanner is software application that assesses security vulnerabilities in networks or host systems and produces a set of scan results. Computer security is the process of preventing and detecting unauthorized use of your computer. Prevention measures help you to stop unauthorized users (also known as "intruders") from accessing any part of your computer system. However, because both Administrators and attackers can use the same tool for fixing or exploiting a system, administrators need to conduct a scan and fix problems before an attacker found the vulnerability. It is also important to consider a policy that should be followed by both the tester and the client to reduce financial and confidential disparities, and to bring conformity to the operations between the both parties, so this research suggests a policy that should be followed by penetration testers and clients of the penetration tests. A penetration test is when ethical hackers do their magic. A vulnerability analysis has been conducted against the target host using an automated vulnerability scanner, Nessus, to identify security holes. In this paper is trying to find out the level of belief in a vulnerability scanner's output. In this paper I am using Vulnerability Scanner which are:

C. MBSA (Microsoft Baseline Security Analyzer)

MBSA is a product of Microsoft Company. It is used to determine security state by assessing missing security updates and less-secure security settings within Microsoft Windows, Windows components such as Internet Explorer, IIS web server, and products Microsoft SQL Server. It is a free sources and easy-to- use for IT Persons and also help making security for Small organization. It is a standalone security and vulnerability scanner designed to provide a streamlined method for identifying common security misconfigurations and missing security updates. MBSA is used by many leading third-party security vendors and security auditors and, on average, scans over 3 million computers each week.

D. Nessus

On the homepage of Nessus (http://www.tenable.com/products/nessus) the organization proudly states that their Scanner is used by 75,000 organizations worldwide and that the scanner is the most popular in use today, endorsed by security organizations like the SANS institute. It is not free available but provide trial period. NessusV6 now are available which are latest plug-in which are

useful for searching any vulnerability. NessusV6 uses a script language called NASL (Nessus Attack Script Language), it is described as looking like the programming language C without the pointers and memory management, with some Perl–isms (Perl is a script language). Nessus uses a client –server architecture. Each session is configured and controlled by the client but the test is run on the server side.

E. Nexpose

Nexpose(www.rapid7.in/) is the only vulnerability management solution to analyze vulnerabilities, controls, and configurations to find the who, what, and where of IT security risk. It uses RealContex,RealRisk and the attacker's mindset to prioritize and drive risk reduction. It is developed for Metasploit Framework.

F. Retina

Retina Network security scanner, (www.eeye.com), is developed by "eEye Digital Security", the company state at their website that they are the leading developer of endpoint security and vulnerability management software solutions. It is leight weight software which are highly reliable Scanner. Now on the basis of the Scanner Result we follow the penetration testing. In this paper we try to find that we are not always says that the result coming is always tre. There are two terms which are:

G. False-Positive

A false-positive is when the vulnerability scanner reports an error that is not present.
Sometimes Scanner show that vulnerability which are not present or patch recently or buggy Script. A Buggy Script are that most Scanners are develop own Script there are not always that everything going to planned.

H. False-Negative

A false-negative is when the scanner misses out any legitimate vulnerability. This condition is very critical and dangerous for the network.

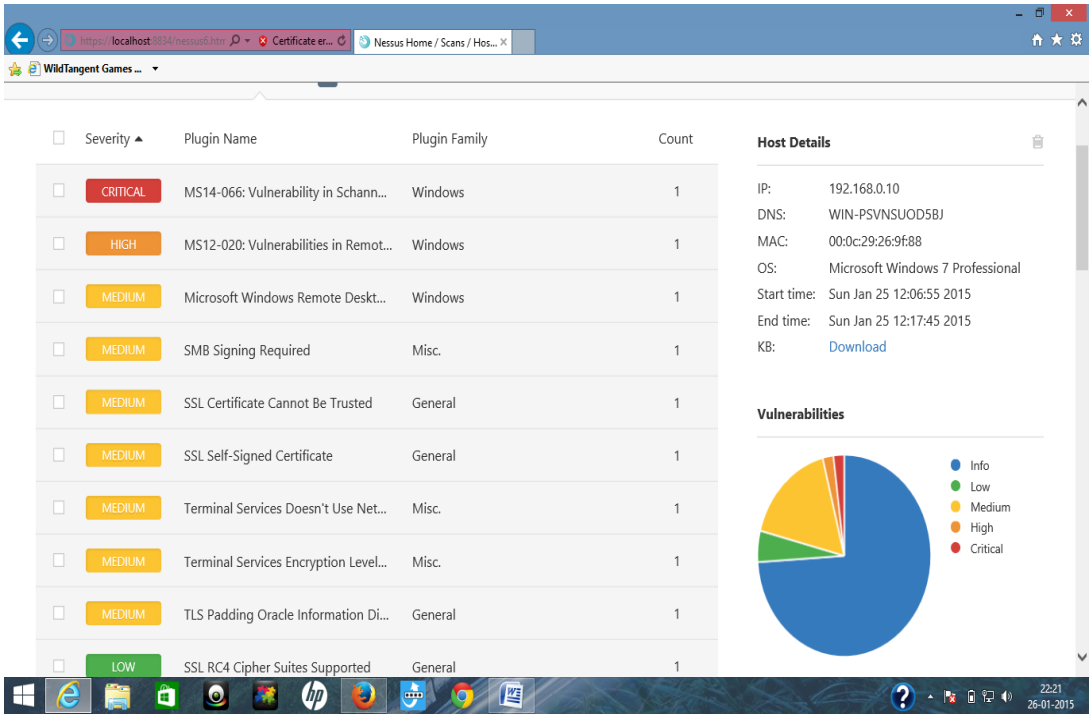

Fig. 1: Nessus Scan Report

I. Proposed Work

For our purpose we have used the tools like Kali Linux, (Attacker machine), several windows OS (Victim machine), VMWare workstation 9.0(Virtual Environment).

J. Information Gathering

Nmap (Network Mapper) is a security scanner originally written by Gordon Lyon (also known by his pseudonym Fyodor Vaskovich) used to discover hosts and services on a computer network, thus creating a "map" of the network. It is used for gathered information against target like what operating system version running, how many ports are open all other information are collected in Nmap.

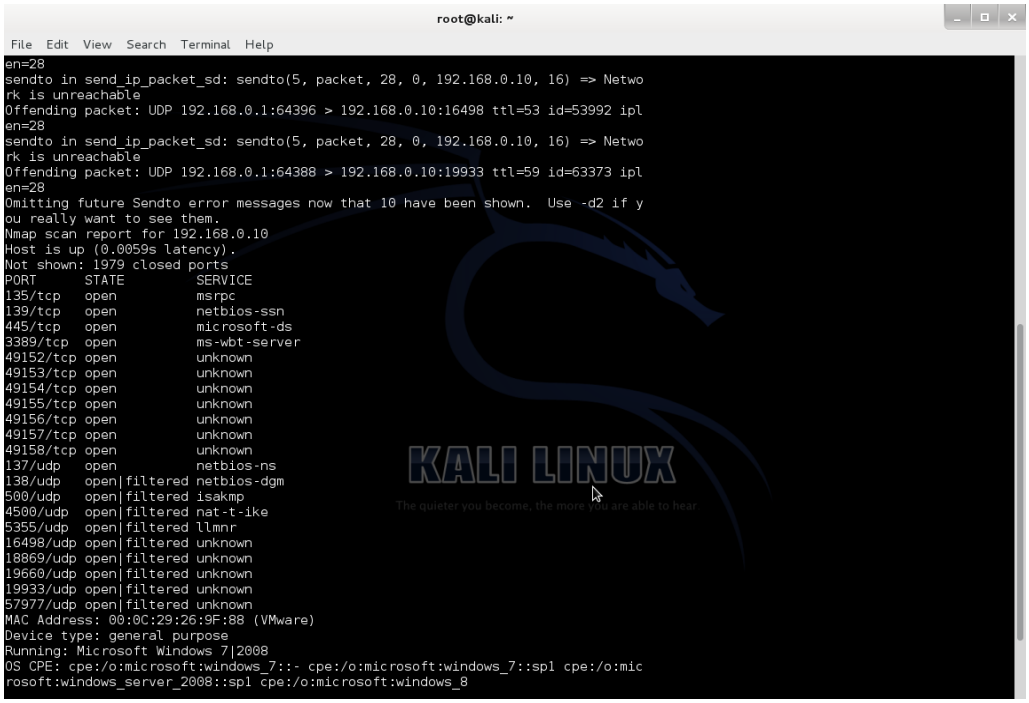

Fig. 2: Information Gathering using Nmap

II. METHODOLOGY OF INFORMATION GATHERING

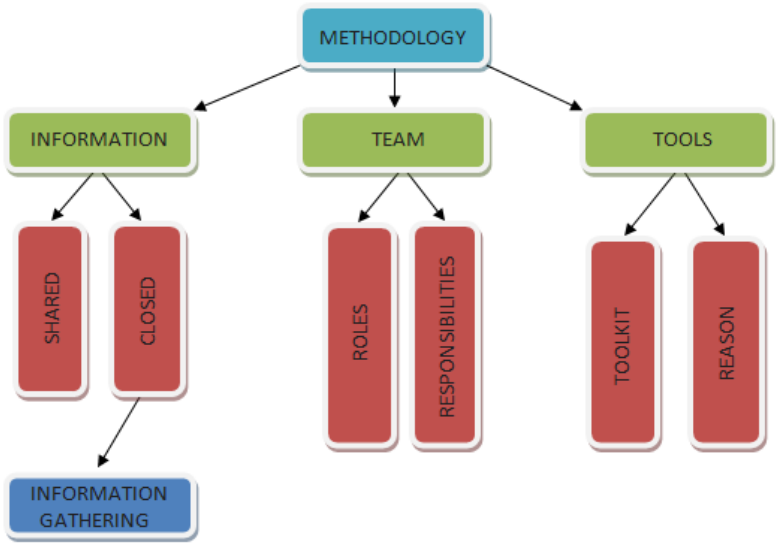

Fig. 3: Methodology of Information Gathering

III. CONCEPT

Fig. 4:

A. What is Payload?

A Payload is a piece of code that is executed when the vulnerability is triggered. The payload is usually written in Assembly Language and it is platform and operating system dependant. The most common payload type used with exploits is shell payloads. These payloads provide the attacker an interactive shell that can be used to completely control the system remotely. The two commonly used shell payloads are:

1) Bind Shell: which have some in-build part of coding
2) Reverse Shell: which have a reply reverse information to the attacker

B. Exploits

An Exploit is a means by which an attacker takes advantage of a vulnerability within a system, an application or a service. Common exploits include buffer overflows, SQL injection and configuration errors. Every vulnerability has its own exploit.

C. Lab Configuration

In my paper i run various machine Windows 8.1 as a host machine Window 7(192.168.0.10) Windows XP(192.168.0.20) and a linux machine (192.168.0.30) and Kali Linux(192.168.0.1) as attacker machine. As we know now 8 April 2014 Microsoft close supports or we can say close making patches. Now if any one uses Xp that means it not assuring for Security.

D. Experiments

In our paper we are using kali linux and windows7 exploit which are internet explorer browser based. An unwanted Script running on the target host and target will allow the programme and then our exploit starts our works. It is also based on windows/meterpreter/reverse_tcp which back control to the attacker.

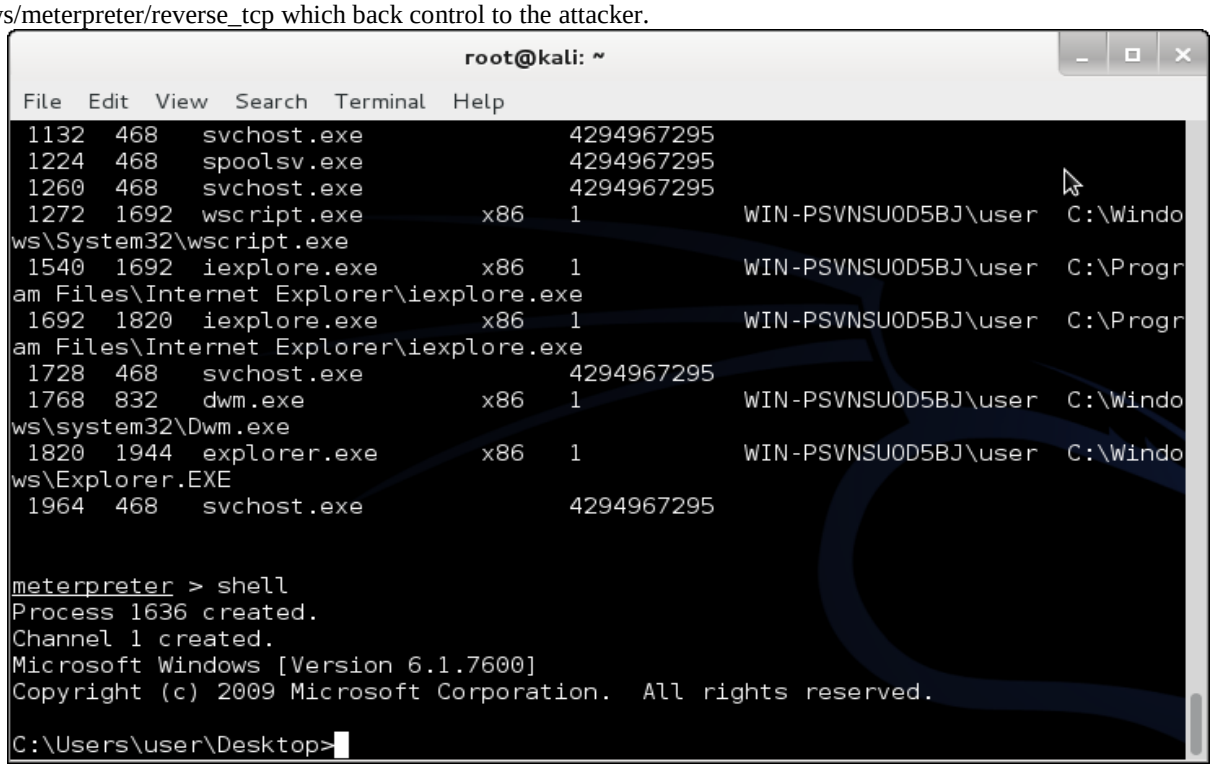

Fig. 5: Command Prompt of the Window7

Now we can see we can access the windows 7 command prompt as well as we also access windowsXp Command Prompt and same as linux file but there is a difference in payload which are change at Vulnerability Based. On the basis of the Scanner this Vulnerability Browser Based which are not shown in Nessus Scanner. On same way we can access all operating system can access from kali linux.

Another vulnerability ms12_020_maxchannelids which are CVE-2012 based which are also known The RDP Vulnerability is a denial-of-service attack which crashes the target system with the above “Blue Screen of Death”.

Fig. 6: Blue Screen of Death

IV. RESULTS

OS	*Payload*	*Result*
Windows7	*Windows/meterpreter/reverse_tcp*	*Breached*
WindowsXp	*Windows/meterpreter/reverse_tcp*	*Breached*
Linux	*Cmd/unix/reverse*	*Breached*

V. CONCLUSION

To provide assurance of appropriate level of confidentiality, integrity and availability of information, vulnerability assessments are important mechanisms through which organizations can identify potential security exposures. Any organization must run Scanner routinely to avoid any circumstances.

A. Future Scope

In this paper there is a limitation is that if we allow firewall the firewall easily Bloch all the exploits and as well as if there are any antivirus programme on the target machine then exploits will not work.

REFERENCES

[1] http://en.wikipedia.org/wiki/Microsoft_Baseline_Security_Analyzer
[2] http://blogs.microsoft.com/cybertrust/2012/10/22/microsoft-free-security-tools-microsoft-baseline-security-analyzer/
[3] http://www.tenable.com/products/nessus
[4] http://www.rapid7.in/products/nexpose/
[5] http://en.wikipedia.org/wiki/Nmap
[6] http://www.offensive-security.com/metasploit-unleashed/Msfpayload
[7] Liu, Bingchang; Shi, Liang; Cai, Zhuhua; Li, Min; "Software vulnerability Discovery Techniques: A Survey" IEEE Conference Publication, DOI: 10.1109/MINES.2012.202, Page(s) 152-156, 2012
[8] Smith, Yurick, Doss "Ethical Hacking" IEEE Conference Publication, DOI: 10.1147/sj.403.0769, Page(s): 769-780
[9] Bradley, Rubin "Computer Security Education and Research: Handle with care" IEEE Conference Publication, DOI: 10.1109/MSP.2006.146, Page(s): 56-59
[10] Nilsson J., 2006, "Vulnerability Scanners", Master of Science in this paper at Department of Computer and System Sciences, Royal Institute of Technology, Kista, Sweden