OPEN ACCESS

International
Journal
Of Modern Engineering Research (IJMER)

Penetration Testing In Virtual and Real Environment

Pooja Rani , Puneet Arora
M.Tech Student, Department of CSE, AIET ,Faridkot, Punjab.
**Corresponding Author: Pooja Rani*

ABSTRACT
Provide internet has opened unlimited avenues of opportunity by enabling organizations to conduct business and share information on a global basis. However , it has also brought new levels of security concerns and cyber threats. It exposes valuable corporate information, mission critical business applications and consumer's private information to more risk than before, but security of IT infrastructure is something that organization cannot afford to compromise. Vulnerability Assessment and penetration testing (VAPT) helps to assess the effectiveness or ineffectiveness of the security infrastructure installed by the organization to remain protected from emerging cyber threats. Hence it enables the organizations to install patches and adopt required security measure to safe guard themselves from possible cyber attacks. VAPT involves compromising the system, and during the process, some of the files may be altered. This process insures that the system is brought back to the original state, before the testing, by cleaning & restoring the data and files used in target machines .vulnerability analysis is the process of identifying vulnerabilities on a network, whereas a penetration testing is focused on actually gaining unauthorized access to the tested systems and using that access to the network or data, as directed by the client.

Date of Submission: 27-04-2018 Date of acceptance: 12-05-2018

I INTRODUCTION

The expansion and evolution of computer , internet and web technologies have made society more dependent upon computer network services than ever .As the domain of these has become large and more sophisticated, security attacks, or even worse security breaches have been ever more critical which may result loss in business and productivity, the time and labour involved in redeploying infected system posses a significant expenses. Penetration test provide a bird eye perspective on current security posture of an organization IT infrastructure .The intent of penetration test is determine the feasibility of an attack and its impact of a successful exploit if discovered. The process involves an active an analysis of the system for any potential vulnerability that may result from poor proper or improper system configuration, known and/or unknown hardware or software flows.

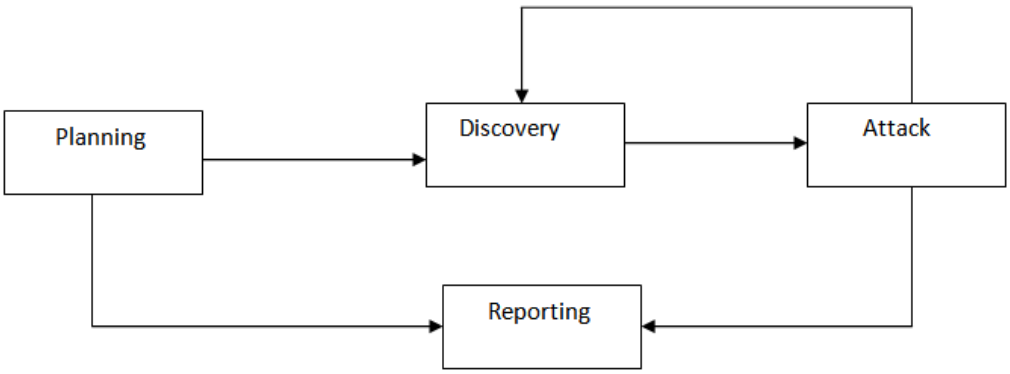

Fig:1 Four phase penetration testing methodology

II METHODOLOGY

1.**Planning Phase**: The planning phase is where the scope for the assignment is defined. Management approvals, documents and agreements like NDA (Non Disclosure Agreement) , etc. are signed. The penetration testing team prepares a definite strategy for the assignment .existing security policies , industry standards, best practices, etc. will be some of the inputs towards defining the scope for the test. There are various factors that need to be consider to execute a properly planned controlled attack. Time in a real world situation , a hacker has ample amount of time to carefully to plot his attack. For a penetration tester, it is a time bound activity. Legal restriction a penetration tester is bound a legal contract , which list the acceptable and non acceptable steps a penetration tester must follow religiously as it could have grave effect on the business of the target organization.

2**. Discovery phase**: the discovery phase is where the actual testing starts ; it can be regarded as an information gathering phase. The phase can be further categorized as follows:

- Foot printing phase
- Scanning and enumeration phase
- Vulnerability analysis phase

Foot printing : The process of foot printing is completely non instrusive activity performed in order to get the maximum possible information available about the target organization and its systems using various means , both technical as well as non technical. This involves searching the internet, querying various public repositories (Data bases, domain registrars, use net groups, mailing lists, etc).

Scanning and enumeration : the phase will usually comprise of identifying live systems , open/ filtered ports found , services running on these ports , mapping routers / firewalls rules , identifying the operating system details , network path discovery , etc . This phase involves a lot of active probing of the target systems. A penetration tester must be careful and use the tools for these activities sensibly and not overwhelm target systems it excessive traffic . All the tools used for this phase and successive phases must thoroughly tested in a testing environment prior to using in a live scenario.

- Nmap
- Super scan
- Hping

Various services and OS fingerprinting tools are available on the internet. Some of them are:

- Xprobe2
- Queso
- Nmap
- P0f
- Httprint
- Winfingerprint

Vulnerability analysis : after successfully identifying the target systems and gathering the required details from the above phases, a penetration tester should try to any possible vulnerability existing each target system . During this phase a penetration test may use automated tools to scan the target system for known vulnerabilities These tools will usually have their own database consisting of latest vulnerability and their details .

- Nessus
- Shadow security scanner
- Retina
- ISS Scanner
- SARA
- GFI LAN guard

3. **Attack phase** : This is the phase that separates the men from the boys . This is at the heart of any penetration test , the most interesting and challenging phase . This phase can be further categorized into :

- Exploitation phase
- Privilege escalation phase

Exploitation : During this phase a penetration tester will try to find exploits for the various vulnerabilities found in the previous phase . There are many repositories on the internet that provide proof- of-concept exploits for most of the vulnerability. It is recommended that the penetration tester has programming knowledge of C (preferably socket Programming) or scripting language like Perl , Python or Ruby. It helps in understanding and writing exploits and custom tools /scripts . This phase can be dangerous if not execute properly .

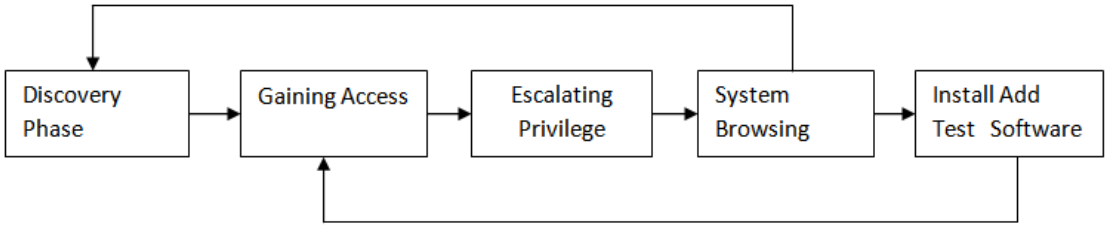

Fig:2 Attack Phase steps with loop back to discovery phase

Privilege Escalation : There are times when a successful exploit does not lead to access . For Example , for particular vulnerability , the penetration tester might acquire user level access . An effort has to be made at such point to carry further analysis on the target system to gain more information that could lead to getting administrative privilege e.g . local vulnerability .

4. Reporting phase : The last stage in the entire activity is the reporting stage . This stage can occur in paraller to be other three stages or at the end of the attack stage. Many penetration testrr do not concentrate on this stage and follow a hurried approach to make all the submissions . The final report must be prepared keeping in mind both management as well as technical aspects , detailing all the finding with proper graphs , figures , etc so as to convey a proper presentation of the vulnerability and its impacts to the business of the target organization . For eg , the necessary things that the report should consist of are :

- Executive summery
- Detailed findings
- Risk level of the vulnerabilities found
- Business impact
- Recommendations
- Conclusion

III RESULTS

Perform penetration testing in virtual environment : Here are few words regarding each respective host with associated operating and software .

- **Kali linux** : also known as the next generation of the in famous free open source penetration testing distribution – the Backtrack 5 , kali linux is rebuild completely adhering to debian development with all tools reviewed and packaged . The primary attacking tools used in the research is the community version of metasploit frame work (available in kali linux) developed by repid7.
- **Metasploitable 2** : This is deliberately vulnerable linux virtual machine especially designed for security tranning, security tools testing , common penetration testing techniques practice . in this research , metasploitable is adopted to demonstrate different attacks on different services such as SSH,FTP,APACHE2,MYSQL

Vulnerability scanning result of metasploitable virtual machine

Host	192.168.181.131 Metasploitable	Total
Most sever Result	Severity: High	
High	16	16
Medium	7	7
Low	3	3
Log	65	65
False positive	0	0

Vulnerability scanning result of Window XP virtual machine

Host	192.16.8.181.133 (Red team-D7253BF)	Total
Most Sever Results 15	Severity High	
High	2	2
Medium	8	8
Low	2	2
Log	34	34
False Postives	0	0

IV PERFORM PENETRATION TESTING IN REAL ENVIRONMENT:

a. Information gathering

Identifying live hosts

The hole range of host was determine but that doesn't mean that all hosts will be up or online so the next step will be to determine the live hosts. In order to do that a ping scan is performed by using Nmap. # nmap- sn IP_Address_Range-oN File_name.txt this is the fast scan that gives the number of hosts which are up and there corresponding IP address. The parameters- oN saves the result to a text file called "File-name".

Scanning ports for services

after determine the live hosts we go for identify and audit each device connected to the network. This can be performed by making use of the opened services each computer device is running. Computers devices have over 65000 ports. It is impractical to scan all of them. The solutions to this problem was to scan the most common ports used. To perform the port scan the live host were used as input file must contain pure IP addresses. IP address extractor was developed in Java to produce pure IP addresses to be read directly from the file for the ports scan. The output is a text file containing pure IP addresses.

Ports scan command:

#nmap-T4-A-v-iL pure_20.txt-oX output_file.xml --stylesheet nmap.xsl

where:

-iL is a parameter to specify the path of the input file name containing the pure IP's.

-T4 was chosen to balance between scan speed and depth.

-A parameter used to enumerate the services and platform of scanned devices.

- V is to determine the version of the services and OS.

-ox is the output option to save the ports scan results as an xml file.

Conclusions: 1. The main objectives of the thesis is to design and implement penetration testing and vulnerability assessment mechanism for the virtual and real environment in order to uncover to vulnerabilities and risks that may lead to denying the services, leaking or modification of sensitive data by unauthorized third party.

2. Penetration testing can precisely exmines the effectiveness of the safe guards implemented on the inspected system.

3. Penetration testing process is carried out in proper manner in both virtual and real environment.

4. The availability of tools is restricted by the licensing cost.

5. The assessments is include complete university network, but due to limitation of times the assessments included the some part of university network.

6. It is strongly recommended that systems owners is strictly protect themselves by keeping the systems up-to-date, applying strong password policies, and attempting to raise the employees security awareness, at least at a very basic level.

Future Scope: In future, the present work may be extended on the following lines

1.Performing the penetration testing and vulnerability assessment to the rest of the university network.

2.Performing the penetration testing and vulnerability assessments to the more number of virtual machines.

3. Integration of used tools into one tool to ease the task of penetration testing and vulnerability assessment.

4. Developing new techniques or algorithms to speedup penetration testing and vulnerability assessment tasks.

5. Extending the aspect of penetration testing and vulnerability assessment to include other aspects such as network hardware configuration and traffic analysis.

REFERENCES

[1]. Murphy, B.F, 2013, Network Penetration Testing and Researches John F,Kennedy Space center, NASA.
[2]. William G.J Halfond, S.R.C.A.O,2011. Improving Penetration Testing through statics and analysis. Wiliy online library, Softw. Test. Verify. Reliab.
[3]. Bode , L.H.a.N, 2006 network penetrarion Testing. Springer.
[4]. Aileen G.Bacudio, X.Y.B-T.B.C.M.J, 2011 .An overview of penetration Testing International Journal of Network Security & its applications (IJNSA), Volume 3,P,6.
[5]. Konstantinas Xynos , I.S.H.R.E.E.A.J.C.B, august 2010. Penetration Testing and Vulnerability Assessment: A Professional Approach Perth Western ,Australia, 1st International Cyber Resilience Conference, Edith Cowan University.
[6]. Michele Fiocca, A.V, 2009 Literature Study of Penetration testing, Sweden:Project Report for Information Security Course Linkopings Universitet .
[7]. Michael Hoehl ,R.C.,2014.Web application Penetration Testing for PCI.19 june.
[8]. Stephen Irwin ,S.N.,2014 Creating a threat Profile for your organization .SANS,8 September.
[9]. IMPACT,C., 2013. An Automated Penetartion Testing Framework.
[10]. Sbrusch,R.,2006.Network Covert Channels.SANS.

Pooja Rani." Penetration Testing In Virtual and Real Environment.” International Journal Of Modern Engineering Research (IJMER), vol. 08, no. 05, 2018, pp.71 –75.