THINK INDIA JOURNAL

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

A Novel Approach To Find Vulnerabilities and Exploit Them Using Open Source Penetration Testing Framework

Gurpreet Singh,
Department of Computer Science and Engineering
Cs.thapar.gurpreet@gmail.com

Umeriqbalwani,
Department of Computer Science and Engineering
Umerwani20@gmail.com

Abstract: **Nobody is secure these days. Attackers are looking for loopholes in the networks and try to attack them for their benefits. So, a mechanism named as Penetration Testing is used to find loopholes in the network before the attackers and exploit them. In this paper, it has been desired that the Process of Penetration Testing should be implemented on network before attacker. Zero-Day vulnerability is also found to make Penetration Testing process more effective. Post Exploitation of the vulnerability can add extra enhancement in the process by evaluating the system after compromise.**

Keywords**:** Penetration Testing, Payload, Exploit, Vulnerability, Post exploitation

I. INTRODUCTION

Network security can be achieved by the software as well as hardware. Antivirus, spyware, intrusion detection systems (IDS) and virtual private networks (VPN) are basics of network security[1].

Components of Security

To achieve security in network the CIA i.e. confidentiality, integrity and availability must be maintained. These are also called as basic and important components of security.

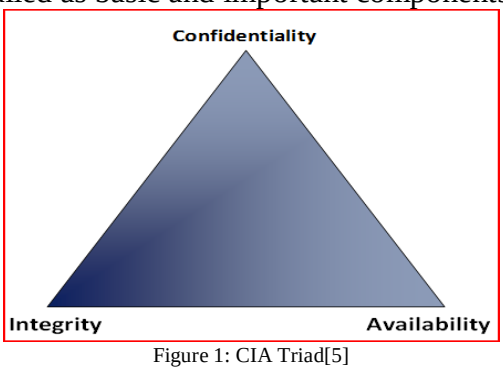

Figure 1: CIA Triad[5]

a) **Confidentiality**: The term confidentiality means that data or information is only available to an authorized user. Here an authorized user means that which have provided with privileges to use the information. Passwords can be used to provide this security component.[5][6].
b) **Integrity**: Integrity defines the trustworthiness of information i.e. data is not modified.

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

Here 'not modified' doesn't mean that data can't be modified. Data can be modified but only by authorized users.

c) **Availability**: An access to the resources and their availability define availability component. This component ensures that system will always remain available when it is needed by authorized users.

Penetration Testing:To find the vulnerabities in our own network by professional pentesters or by internal auditors, and then exploit them to showcase what an attacker can do. Further, how much harmful and how much deep a hacker can go, can be found by Post exploitation.There are certain technical terms used in the Penetration Testing.

A. *Vulnerability*: It is a loophole that can produce a threat to the security of system or network.[9]
B. *Exploit***:** It is defined as to take benefit of our system by entering into it.
C. *Hacker***:** The person which tries to take advantage of IT systems loopholes and weaknesses.
D. *Threat***:** It is kind of intimidation, danger or risk to security.
E. *Payload***:** It is a program which is used after exploitation of vulnerability to take system advantage. It carries exploits and shell code with it.
F. *Shell code***:** Code that use to open command shell on the target system.

Classifications of Penetration Testing: The classifications of penetration testing can be done on the basis of their use. There are different ways to conduct the Penetration Testing[3][10].

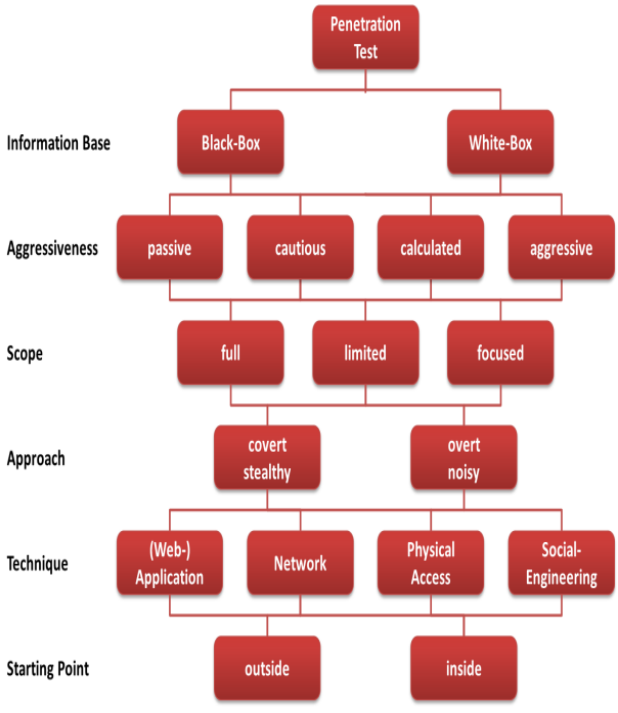

Figure 2: Classification of Penetration Testing

II. LITERATURE REVIEW

Penetration testing has been discussed in brief in previous section. However going through literature, we have described in detail the proper methodology and workflow for Network

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

Penetration Testing.[7][8]

Phases of Penetration Testing: The Penetration Testing process consists of five phases which are discussed below.

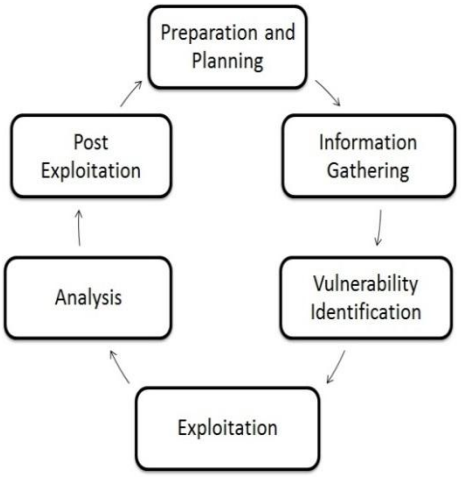

Figure 3: Phases of Penetration Testing

1. *Preparation and Planning*: In this phase, initial preparation is done in the network and planning of various tools for every step is decided according to the network strength and network properties [4].
2. *Information Gathering*: After planning and preparation phase, next phase is to gather all the information about the network using various tools[4].NMAP is a network mapping tool, which is used for port scanning of remote host. This tool has been also used in vulnerability scanning phase. Only the IP address and port range has to specify in NMAP.
3. *Vulnerability Identification*: In this phase, vulnerability is identified in the system or in the network using various tools like NMAP and Nessus. Vulnerabilities will be open ports and services on the target systems. [4].
4. *Exploitation and Launching of Attacks*: In this phase all possible action are taken to exploit the vulnerability found and various tools can be used or an exploit can also be created by writing various scripts. Tester will then check whether the system has been crashed or not. If the system will crash then tester didn't take advantage of that vulnerability.[6]Metasploit has been also used for getting the command prompt of victim's machine by executing shell code. Payloads of Metasploit have been used in Post exploitation phase of the process after target machine has been compromised. Meterpreter is the one of the most emerging payload of this tool.

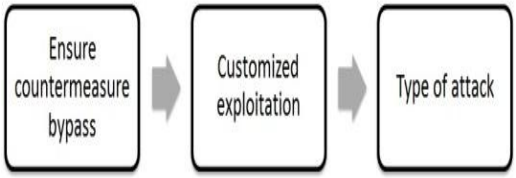

Figure 4: Exploitation Steps

5. *Analysis and Reporting*: In the end, tester will generate the report about all the loopholes found and how those loopholes can be captured by attackers for their further benefits. In

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

the end, report is submitted to authorities

6. *Post Exploitation*: In Penetration Testing framework, loopholes are found and then they are exploited But if the organization wants to know how much deep an attacker can go, then post exploitation comes into picture. Meterpreter is one of the most important payloads of Metasploit. In post exploitation certain important points should be considered.[2][3][14]

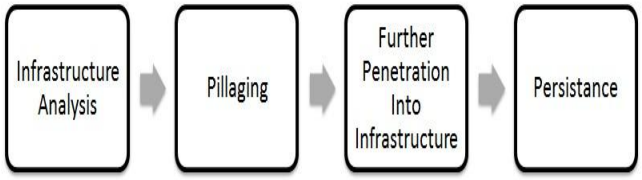

Figure 5: Post Exploitation Process

Steps:

1. Analysis of infrastructure will be done again. As firstly it is done on information gathering phase. Here it means after breaching into target system, check subnets, routers used in network and name servers.
2. Pillaging will be done on the target system to obtain more information. This information includes passwords and secure information.
3. Data exfiltration will be done so that testers can connect to the outside world using a different subnet of the target system. Tester creates its own mapping path of the network.
4. The tester will do the further penetration into target or compromised machine. By performing some actions tester will gain access of targets other systems. This action is called as Pivoting.
5. The tester will also create some more usernames and passwords to again login into the system. Creation of these new accounts called as Persistance.[11][12]

III. PROPOSED METHODOLOGY

Research process has been conducted in different steps. Each phase is having its own importance. Figure 4 shows the research process flow diagram. On the basis of that research process overview has been given below.

1. *Testing of zero-day vulnerability***:** In this phase the testing for zero-day vulnerability has been done on local system. Testing has been done by running the manual scripts on tools.
2. *Penetration Testing Process***:** In this phase automation of Penetration Testing process has been done using zero-day vulnerability. Penetration testing lab has been established using VMware workstation.
3. *Post Exploitation***:** In this phase post exploitation of compromised machine has been done using Meterpreter payload of Metasploit.

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

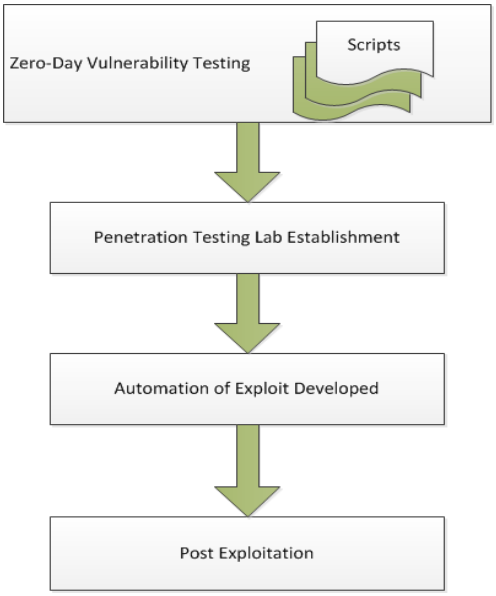

Figure 6: Research Process Flow

Zero-day vulnerability testing: Buffer overflow is the vulnerability of the decade. Most of the servers, especially the FTP servers have this vulnerability in common. A script can be written with Perl which generates the 1000 times of 'A' character as data in hexadecimal format. After that this script can be tested locally on Windows XP with some random FTP servers to crash them. The Baby FTP Server can be one of them. And the script can be successfully worked on that. The server can get crashed with a segmentation violation error when 1000 bytes of random data is send as input to its secure service port 200. So there exists a buffer overflow in Baby FTP Server on secure port.

Penetration Testing Process: In this phase the automation of exploit script on Baby FTP server can be done by conducting the whole penetration testing process by integrating the exploit with Metasploit tool. Payload and RHOST has been set to exploit the vulnerability. On successful exploitation of vulnerability the Meterpreter has been opened up.

Post Exploitation: In this phase the post exploitation of the compromised system can be done. As in previous phase on successful exploitation of remote host the Meterpreter can be opened up.

a) pwd command can be run to check the present working directory. It shows the parent directory of remote system.
b) ps command can be run to check process list on remote host. Then process migration to explorer.exe can be done so that remote host would not through us out of the system.
c) getsystem command can be run and kernel level privileges have been got of remote system.

So Meterpreter has hundreds of commands to run. Some of them have been run on the compromised machine. These all commands provide the different services and control of compromised system.

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

IV. CONCLUSION

In today's era, Organizations are using many countermeasures to improve network security. Penetration Testing is the best process to identify the vulnerabilities in organizational network as shown in this research. This process improves the network security of organization to a great extent by finding zero –day vulnerability. Baby FTP server has the zero-day vulnerability of the type stack based buffer overflow. Metasploit tool provides the user level exploit integration service. It has been concluded that this tool provides better results for the Penetration Testing process because Metasploit have its integrated payloads like Meterpreter, which makes the post exploitation process easy and effective. It has been also concluded that Post exploitation adds extra enhancement in the process for taking more control over the remote target.

V. FUTURE SCOPE

The scope of Penetration testing process never limited to any vulnerability and organization. The results of this research process can be further improved in following manner.
The whole process of Penetration Testing can be automated so that even a user with less knowledge about the tools and process can conduct this process in the organization on one click.
Organizations can use database to store the results of Penetration Testing process which will be analysed before conducting the next Penetration Testing process.

VI. REFERENCES

[1] M. Christiansen. "Stack Based Overflows: Detect & Exploit". SANS Institute, 2007
[2] P. Shi, F. Qin, R. Cheng and K. zhu,"The Penetration Testing Framework for Large-scale Network Based on Network Fingerprint", International Conference on Communications, Information System and Computer Engineering (CISCE), IEEE, 2019.
[3] J. Goel, B. Mehtre," Vulnerability Assessment and Penetration Testing as a cyber defence technology", Elsevier,Volume 57, Pages 710-715 ICRTC 2015
[4] E. Agichtein, E. Gabrilovich and H. Zha, "The Social Future of Web Search: Modeling, Exploiting, and searching collaboratively generated content". IEEE, 2009.
[5] C. T Wai,. "Conducting a Penetration Test on an Organization". *SANS Institute Infosec*, 2002
[6] W. Halfond, S. Chaudhary and A. Orso. "Penetration Testing with Improved Input Vector Identification". *IEEE*, 2009.
[7] H Guppta, R. Kumar, "Protection against Penetration Attacks using Metasploit", ICRITO, IEEE 2015
[8] I. Mukhopadhyay, S Goswami andE. Mandal," Web Penetration Testing using Nessus and Metasploit Tool", IOSR Journal of Computer Engineering (IOSR-JCE) 7Volume 16, Issue 3, Ver. IV (May-Jun. 2014), PP 126-129
[9] F. Loo,. "Comparison of penetration testing tools for web" Semantic Scholar, 2011.
[10] C. J. Marquez. "An Analysis of the IDS Penetration Tool: Metasploit" 2009.
[11] M. Pangaria, V. S. "Compromising windows 8 with metasploit's exploit". *IOSR Journal of Computer Engineering (IOSRJCE), 2012*.
[12] N. Kumar, M. E. "*Penetration Testing of Android-based Smartphones"*. Sweden, 2011.
[13] N. Y. Hamisi, Student MIEEE, N. H. Mvungi, MIEEE, D. A. Mfinanga, B. M.

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

M. Mwinyiwiwa, Member, MIEEE. "Intrusion detection by penetration test in anorganization network". 978-1-4244-3523-4/09, 2009 IEEE

[14] J Kaur, T Singh, K Lakhwani - 2019 International Conference …, 2019 - ieeexplore.ieee.org