Penetration Testing: Analyzing the Security of the Network by Hacker's Mind

Harmandeep Singh[1] , Dr. Surender Jangra[2] , Dr. Pankaj Kumar Verma[3]

[1]*Assistant Professor, Department. of Computer Engineering, Punjabi University, Patiala ,Punjab,*

[2]*Assistant Professor, Department. of Computer Applications, GTB College, Sangrur, Punjab,*

[3]*Associate Professor, Department. of Computer Science, NIILM University Kaithal, Haryana.*

***Abstract*- Network security is one of the major concerns of world. We all know that the systems on the internet are increasing day by day and so the vulnerabilities. These vulnerabilities must be found before the attacker. This can be done with the help of penetration testing. Penetration testing is used to check or evaluate the security posture of an organization or network. Its job is to provide the all round investigation for finding the vulnerabilities and security threats in different systems and networks. This paper explains the penetration testing and methodology for performing it. It also discusses the prevalent tools and techniques for information gathering and vunerability assessment. And finally penetration testing frameworks are analyzed so as to find the vulnerabilities so that patches can be made to fill and increase the security of system, network or applications.**

***Keywords* -Vunerability assessment, penetration testing tools, exploits, metasploit, core impact, Immunity Canvas**

I. INTRODUCTION

Today, internet rules our lives. It is only due to internet that we can easily reach out to the huge store of material and data for reference, consultation and for performing computation. Internet is also used for distribution of various types of information with electronic media and electronic mail within the fractions of seconds. In the today internet world, it is very difficult for companies to maintain its internet presence while keeping their confidential information secret. With each passing day the security is becoming more complex and threatening. Now a day's firewalls, cryptography techniques and intrusion detection solutions simply are not enough. Therefore if we want to continue enjoying its benefits then we need a solution that will check our system security by acting as a hacker and identifying vulnerabilities in our system. Today, it is important for individuals or companies to move to penetration testing for vulnerability assessment.

What is Penetration Testing? We can define it as a technique for finding the vulnerabilities or loop holes that exists in our computer systems, software's and networks so that we can protect our assets from attackers. The main aim of the penetration testing is to find the techniques of illegally gaining access to a network or systems by using the ways of hackers. In Penetration testing, the tester thoroughly analyzes all the security features of the network and then tries to illegally enter into the network by breaking the security.

We have two techniques [16] of doing the penetration testing: manual and automated. The manual penetration testing and code review is a slow and complex process. An expert penetration tester is needed to perform this job. But for automated some already built exploitation framework are available to carry out the penetration testing.

Reasons to perform penetration test

One of the major reasons for performing penetration testing is to find out vulnerabilities [5] before an attacker does and to fix them on time. Attackers are using many automated software tools and perform different types of network attacks to enter into the systems. The penetration testing helps the management to get the security view of their network from attacker point of view. The penetration tester aims to finding the ways into the network vulnerabilities and to fix them before some hacker finds and uses the same loop holes. Secondly, sometimes though the administrar and the users of the network are aware of the vulnerabilities, but they need a penetration tester report. With its help, they justify to the management to sanction the budget for fixing the vulnerabilities. Thirdly, penetration testing can be used to check the secure configuration of our networks. The report of the penetration test helps in verifying that the security team of our organization is doing a good job or not. This test does not increase the security of system or network but it finds the gaps between desired and actual implementation. Fourthly, it helps the companies to meet the government legal requirements for doing the business. Finally, penetration testing is used for testing new technology. The new technology should be tested before production. The process of performing a penetration test on new technologies is easy and cheap because no user is relying on it. When it goes to the hand of users, it becomes the costly affair.

II. RELATED WORK

Jason Bau, Elie Bursztein etc[2010] explained the process of automated black box vulnerability testing. They conducted a study with the help of eight leading tools for (a) vulnerabilities tested by existing scanners. (b) Effectiveness

of scanners against vulnerabilities. (c) How much new vulnerabilities found are relevant to existing vulnerabilities. They used a web application that has some known and projected vulnerabilities for performing the test. The results shows the effectiveness and usefulness of the automated tools with some limitations.

William G. J. Halfondet. al[2011] came with a new approach towards penetration testing. The author uses two newly developed techniques for the betterment of input vector identification and detection of attacks on application. The newly developed approach is compared against the existing tools. The results are in the favour of proposed approach as it does a more through penetration test. As compared to existing tools, it discovers more vulnerabilities.

A.Bechtsoudis and N. Sklavos[2012] explain the methodology of Penetration Testing. With the help of framework, the authors finds the exploitable vulnerabilities at the level of network layer. They setup the lab network for performing the penetration test and exposing some common vulnerabilities and security implications for the network as well as users.

Brandon F. Murphy [2013] discusses the various penetration testing frameworks in the paper. In this paper, the author attacks a window 7 system from Linux operating systems. Backtrack 5 and BlackBuntu operating systems are used for performing the attack as well as try to retrieve information from the host.

NunoAntunes and Marco Vieira[2014] discusses the importance of penetration testing in evaluating the web applications security. The author uses the three vulnerabilities scanners and four penetration testing tools. The authors also highlight that it is important to keep improving these tools, using better workload and attack load generation techniques, and also devising new mechanisms to detect vulnerabilities

Sugandh Shah and B. M. Mehtre[2014] discusses the latest trends in vulnerability assessment and penetration testing. They described the entire process of vulnerability assessment and penetration testing with their models and methodologies. Some freeware and open source tools which are useful for performing vulnerability assessment and penetrations testing with required list of precautions are given in this paper.

Jai Narayan Goel et[2015] describes the complete life cycle of vunerability assessment and penetration testing on systems or networks. He also explains some vunerability assessment techniques and open source tools for testing. The author describes the VAPT as compulsory activity for cyber defense. This paper is helpful for future researchers to get complete knowledge of VAPT tools and techniques and for new findings.

Suraj S. Mudalik[2015] in this paper explains that prior to actually deploying the system, best is to check the system by simulating attacks on it. It is helpful in making the system or network flawless. Many professional companies and commercial tools are available for performing penetration testing. The author performed the simulation with the open source tools in Kali Linux and Backtrack. The information gathering, vunerability assessment and attack simulation is particularly done on kali Linux by using various tools.

Munir A. Ghanem[2015] in the paper explain the Linux distribution Backtrack for performing penetration testing. He discusses the various tools which are available in Backtrack like nmap, ettercap for performing man in the middle attack, wireshark tool, Browser exploitation framework and metasploit framework. Many other tools are available in backtrack for network sniffing, file integrity checking, cracking passwords and vunerability scanning. Thus backtrack is complete package for penetration testing.

Deris Stiawan et[2016] in this paper explains the penetration testing in order to find the vulnerabilities in windows server and the process to exploit those vulnerabilities. The author in the experiment performs the information gathering about the target, performs brute force attacks, injecting the malware for entering the network as a backdoor and flooding the machine for denial of service attack. The research is helpful in finding the security loopholes in the Windows Server.

III METHODOLOGY

A methodology is a specific set of inputs, processes, and their outputs. It guides us about the way to reach the output from inputs. The different stages in penetration testing are:

- Setting the target
- Information Gathering about target
- Vulnerability Identification
- Information Analysis and Planning an attack
- Attack and Penetration
- Result Analysis and Reporting
- Clean Up

In the first stage we decide about on which system or network or web application we have to do the penetration test. The Scope of the test is defined in terms of the attacker profile that the tester will use and about the duration of test. The next stage is the information gathering[8]. As the name suggests, it provides the tester with information regarding the various targets. Our focus is to get as much publicly available information as possible about our target network. We also use some network commands like ping , taceroute, ipconfig for that purpose.

The third stage is the Vulnerability Identification [10]. It focuses on identifying the loop holes in our target system or network that can be exploited by the malicious users. It can be performed by two ways that is with automated tools or manual process. In manual vunerability identification, the tester can manually find the common misconfigurations and flaws in

the target network or host. While in the automated process, some freeware and commercial tools known as vunerability scanners are available. They can be used to audit the target network for software vulnerabilities. These scanners will identify the flaws that can be used by hackers to attack our systems or networks. These automated software's are only limited to identification of vulnerabilities, they cannot perform the penetration testing.

The information analysis and planning an attack which is the fourth stage collates the information which is gathered in all the above stages. With the help of this technical and public information, the penetration tester can plan the attack on the target. The tester also finds that which topic requires further research.

The attack and penetration [12] is further divided into two subparts. The first stage is attack and penetration. In this tester, try to exploit the vulnerabilities that are found in the vulnerabilities identification stage. The tester can use the public available exploits that are available in many software frameworks. If they are not suited the tester also writes new exploits. Once the tester is successful in exploiting the network, he can load the payload on that system to control the system or network. With this the tester can get the initial level of access on the target network. The improper execution of vulnerabilities can lead to system downtime or destruction. Second is privilege escalation stage, in which tester try to get the administrator access from the user level access. Only after getting the top privileges, the tester can perform the thorough penetration test.

In result analysis and reporting, the main task the tester faces is to properly organizing the available data and their results sets that it gets from previous stage. The report should be prepared for the management showing the output of the penetration test. Finally, in the last stage of penetration test, cleaning up of all that was done throughout the testing process. The systems or networks should be returned to configurations that they have prior to performing the penetration test.

IV PENETRATION TESTING TOOLS

Penetration testing can be done with the help of exploitation frameworks which can be used to perform attack on the vulnerable target to get unauthorized access on the network. To perform the penetration testing, the first step is to gather information about the target. To achieve this various types of commands like ping, ipconfig, tracert, nslookup are used. We also use the social engineering techniques to gather as much information as possible about the target. A large number of automated tools [5] are also available in the market for information gathering and vunerability assessment. Some of them are given in the table.

Name	Specific Purpose	Portability	Licence
Nmap	Network Scanning Port Scanning OS Detection	Linux, Windows	Free
SuperScan	• detect open TCP/ UDP ports determine which services are running on those ports • run queries like whois, ping, and hostname lookups	Linux, Windows	Free
Hping	Port Scanning Remote OS fingerprinting	Windows	Free
AngryIP	TCP Scan Host Discovery	Windows	Free
Unicornscan	TCP, UDP port scanner, PCAP file logging.	Unix/Linux	Free
Advanced Port Scanner	TCP Scan. Multithreading tool	Windows	Free
Nessus	Detect Network vulnerabilities. Find open file shares. Detect misconfigurations, passwords	Linux/ Windows	Free personal edition , Enterprize edition (Nessus ProfessionalFeed)Paid
Shadow Security Scanner	Detect network vulnerabilities, LDAP servers and audit Proxy.	Windows	Free Trial Version.
OpenVas	Perform Network Vulnerabilities Tests	Linux	Free
Retina CS Community	XSS, SQL Preauthentication.	Linux, Windows	Free for 256 IPs
Nexpose	Vunerability scanning	Linux, Special Edition for Windows	Free for 32 IPs
GFI LandGuard	TCP Scan, Host Discovering. Patch Management and Network Auditing.	Linux, Windows	Paid
ISS	Detect network vulnerabilities. RPC Bind, XSS	windows	Free Trial Version
MBSA	SQL Preauthentication.	Windows	Free

Different scanners use different ways of assessing if an address corresponds to an online host but the most common is the use of ICMP echo request (ping). Nessus as well as other scanners also has the ability to use both TCP and UDP packets to find out if the host is active.

Exploitation tools[19] are used to verify that an actual vulnerability exists by exploiting it. Many open source and paid tools are available in the market. Some of the tools are used by both attackers and penetration testers. There are many more exploitation tools than the ones listed here. Many tools in this category are single-purpose tools that are designed to

exploit one vulnerability on a particular hardware platform running a particular version of an exploitable system. The tools that are highlighted here are unique in the fact that they have the ability to exploit multiple vulnerabilities on a variety of hardware and software platforms.

Metasploit Framework

The Metasploit Framework [18] is an open-source framework created by HD Moore in 2003.It can be used for doing vulnerability research and development, IDS signature development, and exploit research and penetration testing. The user first selects the payload and then uses the exploit. He can exploit the targeted remote service. When combined with a Meterpreter script, it can be used to control the backdoor running applications. The Metasploit Framework is skilled in performing both penetration test as well as in developing platform in order to create security tools and exploits.The metasploit framework is written in the Ruby programming language.

Metasploit framework is free ware software. It is acquired by Rapid7 Company in 2009. The Company launches its commercial versions. Metasploit Express and full Featured Metasploit pro fissional are paid. The metasploit community edition is free for one year. The Metasploit Framework comes in command base and GUI. Its GUI version is called armitage.

Core Impact

Core Impact [17] is a commercial framework by core security technologies. It is first fully developed automated penetration testing tool. Core Impact Pro allows us to evaluate your security posture using the same techniques employed by cyber-criminals. It supports multi vector testing capabilities across network, web, mobile and wireless. The core impact pro 2015 edition include new capabilities:

- New commercial grade exploits.
- Record login for web application authentication
- Flexible and customizable reporting
- Kerberos support
- Agent persistency using Windows Management Instrumentation (WMI)
- Rapid7 Nexpose support

Core Impact is expensive framework. It costs around $25000 per system. But it is most powerful and widely used penetration testing tool. Its supports come with regularly updated database of tested exploits and documentation. Its reporting features are worth mentioning.

Canvas

Canvas is a commercial vulnerability exploitation tool from ImmunitySec. The latest version is Immunity Canvas 6.45. It is designed mostly as exploit development and defense testing tool rather than penetration testing tool. It has completely open design that allows it to adapt to the environment and user's needs. Canvas provides the MOSDEF environment for the rapid creation of exploits. Immunity CANVAS helps an organization to check the concrete picture of their security posture.

Security Forest Exploitation Framework

It also has an open source tools which can be used by penetration testers. This framework uses the collection of exploit code known as Exploit Tree. Its front end GUI allows the tester to launch the exploit code through the web browser.

It supports come with full source code, and sometimes even includes zero-day exploits. The Comparison of these is:

Features	Metasploit	Core Impact	Immunity Canvas	Security Forest
Number of Exploits	More than 1467 exploits	More than 155 exploits(update)	Over 800 exploits	Massive amount of exploits.
Interface	GUI and CLI	GUI	GUI & CLI	GUI with limited features.
Platform and Installations	Independent	Windows	Independent	Windows
Cost	Free limited version.	$25000 per seat	$ 3101 for 10 seat	Free
Programming Language	Ruby , C	Python	Python	Perl for framework. C, python, Perl for exploits
Updates	Announced on public website.	Regular updates are available.	Monthly updates	Occasionally updates
Initial host discovery	Supported	Supported	Not supported	Not Supported
Reporting Features	Lack in Reporting.	Excellent Reporting features	Lack in Reporting.	Limited
Conclusions	Free availability and customizable.	Fully automatic, most exploits available, Most Professional and Most expensive	Less exploits, Less Cost than core impact.	Pre compiled exploits, indexed exploits.

Many more frameworks other than those listed above are available for the penetration testing. One of them is w3af. It is basically a Web Application Attack and Audit Framework. We can use it for finding and exploiting the vulnerabilities in the web applications.

Nowadays most organization and users are working on Microsoft products which are vulnerable to well written exploits for those applications. So keeping data and information secure is most difficult task now a day. Criminal organizations are organized in their efforts for trying to break into the system. In the last few years, it has been crystal clear that there is real money being made from criminal hacking.

V. CONCLUSION

A network security or vulnerability assessment may be useful to a certain degree, but do not always reflect the extent to which hackers will go to exploit a vulnerability. Penetration tester's put honest efforts to simulate a real world attack to a certain extent but the penetration testers will generally compromise a system with vulnerabilities that are successfully exploited. Hackers and intruders are mostly successful in their intentions because all they have to find only one hole to exploit whereas penetration testers need to possibly identify all the holes that exist in network. This is a daunting task as penetration tests are usually done in a certain time frame. The existing penetration testing frameworks lacks the adaptability when applied to different types of systems or networks and the manual tests which are prevailing in those platforms are usually long and complex process. All the information leads us to conclude that a penetration test alone provides no improvement in the security of a computer or network. Thus there is need for some action to be taken to address the vulnerabilities that are found as a result of conducting the penetration test. Thus we can conclude that penetration testing can be effectively and successfully used for the cyber defense technology.

REFERENCES

[1]. Deris Stiawan1, Mohd Yazid etc," Penetration Testing and Mitigation of Vulnerabilities Windows Server", International Journal of Network Security, Vol.18, No.3, PP.501-513, 2016.

[2]. Suraj S. Mudalik," Penetration testing: An Art of Securing the System (using Kali Linux)", International Journal of advanced research in Computer Science and Software Engineering, ISSN: 2277 128X ,Volume 5, Issue 10, October-2015.

[3]. Munir A. Ghanem,"BackTrack System: Security against Hacking", International Journal of Scientific and Research Publications, ISSN 2250-3153, Volume 5, Issue 2, February 2015.

[4]. Jai Narayan Goel, BM Mehtre," Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology", 3rd International Conference on Recent Trends in Computing 2015 (Elsevier), Procedia Computer Science 57,pp 710-715, 2015.

[5]. B. M. Mehtre, Sugandh Shah,"An overview of vulnerability assessment and penetration testing techniques", Springer Journal of Computer, pp 27-49, 2014.

[6]. E. Martins, M.I.P. Salas," Security Testing Methodology for Vulnerabilities Detection of XSS in Web Services and WS-Security", Elsevier, pp.133–154, 2014.

[7]. NunoAntunes and Marco Vieira," Penetration Testing for Web Services",IEEE,ISSN: 0018-9162/14, 2014.

[8]. Brandon F. Murphy," Network Penetration Testing and Research", NASA. John F. Kennedy Space Center, USRP Summer ,July 30 2013

[9]. N. Sklavos, A. Bechtsoudis," Aiming at Higher Network Security through Extensive Penetration Tests", Revista IEEE , Vol. 10, Issue 3, 2012.

[10]. Shauvik Roy Choudhary, William G. J. Halfond, etc ," Improving penetration testing through static and dynamic analysis", Wiley Online Library, DOI: 10.1002/stvr.450, 2011.

[11]. ElieBursztein, Jason Bau etc," State of the Art: Automated Black-Box Web Application Vulnerability Testing", IEEE Symposium on Security and Privacy (SP), 2010

[12]. Lloyd Greenwald and Robert Shanley,"Automated Planning for Remote penetration testing", IEEE,ISSN: 978-1-4244-5239-2, PID: 901436, 2009.

[13]. Shauvik Roy Choudhary, William G.J. Halfond etc," Penetration Testing with Improved Input Vector Identification", IEEE, ISSN: 978-0-7695-3601-9, 2009.

[14]. Nitin A. Naik,Gajanan D. Kurundkar, Santosh D. Khamitkar, Namdeo V. Kalyankar, "Penetration Testing: A Roadmap to Network Security", Journal of computing,vol1, Issue1, ISSN: 2151-9617, Dec 2009.

[15]. Bing Duan, Yinqian Zhang, DawuGu,"An Easy-to-deploy Penetration Testing Platform" ,IEEE The 9th International Conference for Young Computer Scientists, ISSN: 978-0-7695-3398-8, 2008.

[16]. Danny Allan, "Web application security: Automated scanning versus Manual penetration testing",IBM web application security, 2008.

[17]. Charles J. Kolodgy Gerry Pintal,"Automated Penetration Testing: Can IT Afford Not To? ", IDC, PID: 20516, jan-2007.

[18]. K.K Mookhey, David Maynor etc., "Metasploit toolkit for penetration testing, exploit development and vulnerability research" Syngress press, ISBN 13: 978-1-59749-074-0, 2007.

[19]. James S. Tiller," The Ethical Hack, A Framework for business value Penetration Testing", Auerbach publications, ISBN: 0-8493-1609-X, 2005.

[20]. Matt Bishop and Deborah A. Frincke," About Penetration testing", IEEE SECURITY &PRIVACY, pno.1540-7993, pp. 84-87.