ISSN 2348 - 2249
Volume-3, Issue-1, January-March, 2015
International Journal for Multi Disciplinary Engineering and Business Management
(IJMDEBM)

Securing Networks Using Network Penetration Testing

Ramesh
Research Scholar, Department of Computer Engineering
Punjabi University, Patiala
India
rameshnarwal2010@gmail.com

Gaurav Gupta
Department of Computer Engineering
Punjabi University, Patiala
India
gaurav_shakti@yahoo.com

Abstract – In information technology world security is among the most important factors of our life. The evolutions of Computer, Internet and Web have made peoples more dependent upon computer network services than ever. There has been a challenge of providing a secure environment; an effective network security strategy that helps identifying threats and then selecting the most effective sets of tools to mitigate them in such a way that any organization will be able to reduce the likelihood of incidents and resultant data loss. The main objective of penetration testing is to effectively call to low or high potential vulnerabilities existing in the system or network, and then come up with realistic solutions to address such weaknesses; thus, enhancing the security of the system or network as a whole. This paper contains a review of the methodology used in the different phases of network penetration testing. An advanced penetration testing technique has also been discussed that addresses the limitations of current techniques.

Keywords – Information Security, Vulnerability, Vulnerability Assessment, Penetration Testing, Network Security

I. INTRODUCTION

Nothing is fully secure in the world of cyber space. Securing Network is not an easy task due to the different threats, vulnerabilities, exploits and loopholes. Thekey factor for building a secure network is to firstly define what security means to the organization. There has been a challenge of providing a secure environment; an effective network security strategy that helps identifying threats and then selecting the most effective sets of tools to mitigate them in such a way that any organization will be able to reduce the likelihood of incidents and resultant data loss. Penetration Testing is also known as Pentesting and the team which performs penetration testing is known as Red Team.

There are several types of penetration testing like Network Penetration Testing, Application Penetration Testing, Wireless Penetration Testing, Denial of Service (DoS)Testing, SCADA Systems Penetration Testing and Cloud Penetration Testing etc. Here we discuss only Network Penetration Testing. Firstly there is an agreement between pentesting team and the organisation who want to perform pentesting of their network. Then complete planning of pentest is performed. Then network scans of organisation systems and devices are conducted for the purpose of general security and vulnerability assessment. Sometimes peoples are confused about pentesting and vulnerability assessment. They think both of these are same but in reality vulnerability assessment is the part of pentesting. In vulnerability assessemnet, scanning of network, systems and other resources is performed only to find out the loopholes(vulnerability) in the organisation network or systems and then report the organisation about it. Exploitaion is not a part of vulnerability assessment, but it's a part of pentesting. Report generation is the last step of network pentesting.

II. TYPESOF NETWORK PENETRATION TESTING

Generally network pentesting is of two types namely: -

A. External Penetration Testing

External pentesting is the common approach to network pentesting. It checks the ability of a remote attacker to get inside the internal network of organisation. The goal of this pentesting is to access firewall, servers and other network resources within the internal network by exploiting externally.

B. Internal Penetration Testing

Internal pentesting takes a different approach, which tests what an insider attack canaccess. The target is same as external pentesting, but the major difference is that the "attacker" either has some kind of authorized access or is starting from within the internal network. Insider attacks is much more shocking than an external attack because insiders already have the knowledge of internal network and other resources with their location, something that external attackers usually don't know.

III. WHY NETWORK PENETRATION TESTING?

Network Penetration Testing is important because ofmany reasons

a) To identify the threats facing an organisation's resources.
b) To reduce an organisation's expenditure on IT security by identifying and remediating vulnerabilities or loopholes.

ISSN 2348 - 2249
Volume-3, Issue-1, January-March, 2015
International Journal for Multi Disciplinary Engineering and Business Management
(IJMDEBM)

c) For validation and testing the effectiveness of security protections and controls of an organisation.
d) Evaluating the efficiency of network security devices like firewalls, routers, and servers.
e) Provides preventive steps that can prevent upcoming exploitation
f) For changing and upgrading existing infrastructure of software, hardware, and network design

IV. LITERATURE REVIEW

[1] Liwen He and Nikolai Bode; "Network Penetration Testing"; Springer 2006In this paper different types of network penetration tests are classified and the general approach to a test is outlined. Different tools and techniques that are used in each step of the test are introduced. The aim is to give a general overview of the techniques employed in network penetration testing as well as identifying the future trends and further research directions in penetration testing and network security.

[2] Brandon F. Murphy; "Network Penetration Testing and Research"; NASA, John F. Kennedy Space Center, Program USRP Summer, 2013This paper focuson the research and testing done on a network penetration testing security purposes. This research paper provide the IT security office new methods of attacks across and against a company's network with new platforms and software that can be used to better assist with protecting against such attacks. In this paper, testing and research has been done on two Linux based operating systems, for attacking and compromising a Windows operating system. Backtrack 5 and BlackBuntu are two different "attacker" computers that will attempt to plant viruses and or exploits on a host Windows 7 operating system, as well as try to gain information from the host.

[3] William G. J. Halfond, Shauvik Roy Choudhary, Alessandro Orso; "Improving penetration testing through static and dynamic analysis", Wiley Online Library, Softw. Test. Verif. Reliab. 2011This paper describe a new approach to penetration testing and addresses the limitations of current techniques. The approach incorporates two recently developed analysis techniques to improve input vector identification and detect when attacks have been successful implemented against a web application. This paper compares the proposed approach against two popular pentesting tools for a suite of web applications with known and unknown vulnerabilities. The results show that the proposed approach performs a more better penetration testing and leads to the discovery of more vulnerabilities and loopholes than both the tools.

[4] Aileen G. Bacudio, Xiaohong Yuan, Bei-Tseng Bill Chu, Monique Jones; "An Overview of Penetration Testing", International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6, November 2011Penetration testing is a sequence of activities used to identify and exploit security vulnerabilities. It checks or verify the effectiveness of the security measures that have been implemented. This paper provides an overview of web applications penetration testing. It describes the benefits, the strategies and the methodology of conducting penetration testing. The methodology of penetration testing mainly includes three phases: test preparation, test and test analysis. The test phase involves following steps: information gathering, vulnerability analysis, and vulnerability exploit. This paper further describes how to apply this methodology to conduct penetration testing on web applications.

[5] Konstantinos Xynos, Iain Sutherland, Huw Read, Emlyn Everitt, Andrew J C Blyth; "Penetration Testing and Vulnerability Assessments: A Professional Approach", 1st International Cyber Resilience Conference, Edith Cowan University, Perth Western Australia, August 2010Organisations always want to ensure security of their systems and adopts appropriate measures to protect their system against potential security breaches. One such measure is to hire the penetration testers (or "pen-tester") to find vulnerabilities that are present in the organisation's network, and provide recommendations as to how best to diminish such risks. This paper discusses the definition and role of the modern penetration testerand summarises current standards. The paper further describes issues arising from pen-testers.

[6] Michele Fiocca, Anna Vapen, "Literature Study of Penetration Testing", Project Report for Information Security Course Linköpings universitet, Sweden, 2009The paper address various aspects regarding how much vulnerable computer systems are and what effort that is needed to break into a system where the access is restricted or the target is remotely located. Penetration testing is the art of using different tools and techniques to get unauthorized access to a victim's computer. The main task of a penetration tester is to find vulnerabilities or security flaws of new and old programs, systems to make the development team aware of required modifications in order to increase the security. This paper also contains a review of the tools used in the different phases of penetration testing.

V. METHODOLOGY

Penetration test is broadly carried out using a four phase methodology as shown in the figure below:

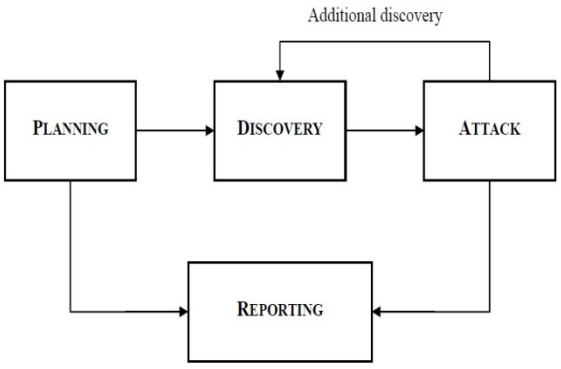

Fig. 1 Network Penetration Testing Methodology

ISSN 2348 - 2249
Volume-3, Issue-1, January-March, 2015
International Journal for Multi Disciplinary Engineering and Business Management
(IJMDEBM)

A. PLANNING

The planning phase is where the scope for the network penetration test is defined. Management approvals, documents and agreements like NDA (Non-Disclosure Agreement), etc., are signed. The penetration testing team prepares a strategy for the pentest. Existing security policies, industry standards, best practices, etc. will be some of the inputs towards defining the scope for the test. This phase usually consists of all the activities that are needed to be performed prior to commencement of the actual penetration test.

B. DISCOVERY

The discovery phase is where the actual testing starts, it can be regarded as an information gathering phase. This phase can be further categorized as follows:
• Footprinting phase
• Scanning and Enumeration phase
• Vulnerability Analysis phase

C. ATTACK

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

D. REPORTING

The last stage in the entire activity is the reporting stage. This stage can occur in parallel to the other three stages or at the end of the Attack stage. This stage is probably the most important of all the phases, after all the organization is paying you for this final document. The final report must be prepared keeping in mind both Management as well as Technical aspects, detailing all the findings with proper graphs, figures, etc. so as to convey a proper presentation of the vulnerabilities and its impact to the business of the target organization. Based on these findings the cost of implementation of the recommendations will eventually be made.
The report must be precise and to the point. Nothing should be left to the client's imagination. Clear and precise documentation always shows the ability of a successful penetration tester.
For example the necessary things that the report should consist of are:
• Executive Summary
• Detailed Findings
• Risk level of the Vulnerabilities found
• Business Impact
• Recommendations
• Conclusion

VI. CONCLUSION

A large number of security problems can be solved by penetration test tools which try to exploit possible vulnerabilities and show us false alarms or vulnerabilities that exist but assessment tools cannot find them. Network Penetration testing evaluates an organization's ability to protect its networks, network devices (like firewalls, router etc), applications, endpoints and users from external or internal attacks which attempts to circumvent its security controls to gain unauthorized or privileged access to protected assets.

REFRENCES

[1] Liwen He and Nikolai Bode; "Network Penetration Testing"; Springer 2006
[2] Brandon F. Murphy; "Network Penetration Testing and Research"; NASA. John F. Kennedy Space Center, Program USRP Summer, 2013
[3] William G. J. Halfond, Shauvik Roy Choudhary, Alessandro Orso; "Improving penetration testing through static and dynamic analysis", Wiley Online Library, Softw. Test. Verif. Reliab. 2011
[4] Aileen G. Bacudio, Xiaohong Yuan, Bei-Tseng Bill Chu, Monique Jones; "An Overview of Penetration Testing", International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6, November 2011
[5] Konstantinos Xynos, Iain Sutherland, Huw Read, Emlyn Everitt, Andrew J C Blyth; "Penetration Testing and Vulnerability Assessments: A Professional Approach", 1st International Cyber Resilience Conference, Edith Cowan University, Perth Western Australia, August 2010
[6] Michele Fiocca, Anna Vapen, "Literature Study of Penetration Testing", Project Report for Information Security Course Linköpings universitet, Sweden, 2009
[7] Metasploit, Nov, 2014
URL: http://www.metasploit.com/
[8] Virtual Box, Nov, 2014
URL: https://www.vitrualbox.org/
[9] Zenmap, Nov, 2014
URL: http://nmap.org/zenmap/
[10] D. Maynor, K.K. Mookhey; Metasploit Toolkit: For Penetration Testing, Exploit Development, and Vulnerability Research, Syngress Publishing, Inc., Burlington, MA, 2007
[11] D. Kennedy, J. O'Gorman, D. Kearns, and M. Aharoni, Metasploit: The Penetration Testers Guide, No Starch Press, Inc., San Francisco, CA, 2011
[12] Nessus, Nov, 2014
URL:http://www.tenable.com/products/nessus
[13] BlackBuntu, Nov, 2014
URL: http://www.blackbuntu.com
[14] Armitage, Nov, 2014
URL: http://www.fastandeasyhacking.com

