ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 4, April 2018

# A Survey on Assessment of Vulnerability and Network Security by Penetration Testing

Anish Kaushal[1], V.Uma Rani[2]

M.Tech Student, Department of Computer Networks & Information Security, School of Information technology (JNTUH), Village KPHB, MandalKukatpally, Dist Medchal, Telangana, India [1]

Associate Professor, Department of Computer Networks and Information Security, School of Information technology (JNTUH), Village KPHB, MandalKukatpally, Dist Medchal, Telangana, India [2]

**ABSTRACT**:This paper presents the survey of different approaches and analyzing technique of penetration testing by different authors. Penetration test is a process or a method of evaluating computer and network security by simulating an attack on a computer system or network from external or internal threats. The role of this testing method is to identify and fix potential holes in order to stop or prevent attacks that can be harmful to the network or system.This paper describes the different methods for assessing the different types of network i.e., wireless and static networks. In this paper, we discuss the various stages of penetration testing and the literature survey which we had done.

**KEYWORDS**:Penetration testing, Cyber security, Wireshark,Metasploit.

## I. INTRODUCTION

The network security is one of the major concerns of any information system. As the size of the system grows, the possibility of weak configurations increases which in turn create a security loop hole.
The security risks for companies, organizations, and entities that work with sensitive data, from the public sector or not, are more than evident. In many situations, these companies are not able to understand the extension of the actual complex communication structures and have just a little or no control of them. Furthermore, these risks are even bigger when applications that run on their computing infra-structures are taken into consideration. The risks that are not controlled may increase the number of security attacks that can become big financial losses.
However, assessing the security state is a continuous and necessary task to understand the risks there exist. This assessing is usually performed through security tests. So, the use of the right techniques for security testing is an important task to minimize the existing security risks in any corporation. One of the known forms to assess the state of security and reduce security risks is called penetration test (Pentest).
It's the process to identify security vulnerabilities in an application by evaluating the system or network with various malicious techniques. The weak points of a system are exploited in this process through an authorized simulated attack. The purpose of this test is to secure important data from outsiders like hackers who can have unauthorized access to the system. Once the vulnerability is identified it is used to exploit the system in order to gain access to sensitive information. A penetration test is also known as pen test and a penetration tester is also referred as an ethical hacker. We can figure out the vulnerabilities of a computer system, a web application or a network through penetration testing. A penetration test tells whether the existing defensive measures employed on the system are strong enough to prevent any security breaches. Penetration test reports also suggest the countermeasures that can be taken to reduce the risk of the system being hacked.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 4, April 2018

## II. LITERATURE SURVEY

### 1. A STUDY OF NETWORK SECURITY USING PENETRATION TESTING

Author: R. Shanmugapriya

Description: In the network security cybercrime technologies have brought many good things by means of the internet: electronic commerce, easy access to vast stores of reference material, collaborative computing, e-mail, and new avenues for advertising and information distribution, to name a few. As with most technological advances, there is also a other side: criminal hackers. Governments, companies, and private citizens around the world are anxious to be a part of this revolution, but they are afraid that some hacker will break into their Web server and replace their logo with pornography, read their e-mail, steal their credit card number from an online shopping site, or implant software that will secretly transmit their organization's secrets to the open Internet. With these concerns and others, the ethical hacker can help [1].

Hence in this paper author concluded as Hacking is now an issue that does not have any conclusion. The only way we can stop a hacker is by learning hacking. By learning we can read the minds of a hacker which enables us to know the reality. Hacking is not a crime but it is made a crime by misusing the knowledge of programming. Every hacker is a perfect programmer even more than a normal programmer. Everyone should know the ethics of hacking and follow them to be safer.

### 2. PENETRATION TESTING IN WIRELESS NETWORKS

Author: Harshdeep Singh, Dr.Jaswinder Singh

Description: Wireless technology has brought many changes in the way of communication in modern days. With the increased worldwide employment of wireless technology, there is raising concern about the security standards of the technology. Many encryptions and decryption techniques have been implemented today to transmit data over the networks. Despite that, many authentication methods have also been applied. However, such methods must be validated to ensure the security of wireless networks. Penetration testing is the one which can be used to identify the unknown void in the network. This makes pen test crucial to validate the security mechanisms of the system and outcomes of penetration testing could be used to secure the network [2]. In this paper, author has presented an overview of penetration testing and tools. They have done much literature work and explained the different phases of penetration testing as

Phase 1: Reconnaissance,Phase 2: Scanning Phase 3: Gaining Access, Phase 4: Maintaining Access ,Phase 5: Covering Tracks .

The wireless network is an essential part of today's' Information Technology. With this vast implementation of technology, security concerns also increased drastically. Despite the many security measures, new techniques of penetration testing are need to be introduced. Network Penetration testing is a method to detect vulnerabilities in network security before hackers could use them to access it. This paper described the approach used previously for the network penetration test. The aim of this paper was to provide a general overview of the penetration techniques employed earlier in previous studies as well identifying the future research directions in penetration testing and wireless network security.

### 3. ASSESSMENT OF WEBSITE SECURITY BY PENETRATION TESTING USING WIRESHARK

Author: Sandhya S, SohiniPurkayastha, Emil Joshua, Akash Deep

Description: Wireshark is a tool that has proven itself very useful in network sniffing. The packets that it captures from a live network can be analyzed without difficulty within the tool itself. If there is a security lapse in any of the systems, that record data online for big organizations, then access to such systems can be gained by analyzing the packets being transmitted during user authentication. Wireshark aims at understanding, how prone a system is to security breaches [3]. In this paper they created a website and analysed using a pentestingtool:Wireshark for its loopholes and sniffed the user data from the website.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 4, April 2018

Their work showed the usage of Wireshark as a packet sniffer to perform the penetration testing technique of information gathering to indicate whether a website is secure or vulnerable. The result showed that the website that has been assessed has a lapse in its security mechanism.

4. **EFFECTIVE PENETRATION TESTING WITH METASPLOIT FRAMEWORK AND METHODOLOGIES**

Author: FilipHolik, Josef Horalek, OndrejMarik, SonaNeradova, StanislavZitta

Despription: In this paper they have briefly introduced the basics of penetration testing and showed how to deploy and use Metasploit framework when conducting penetration testing. This paper outlines what tools and aids can be adopted for better and more effective workflow of penetration test procedures. At the end of this paper, a case study, which demonstrates a penetration test conducted against a network in pharmaceutical company where automated lines used for production of medicaments reside, was presented.

Metasploit Framework is also updated on regular basis – new malicious code used for exploiting system vulnerabilities is added when an update is triggered. Despite its initial complexity for newcomers to penetration testing, tools like Metasploit Project offer many valuable tools to conduct penetration testing and simplify some tasks that would have to be solved programmatically without framework [4].

5. **CYBER SECURITY ANALYSIS USING VULNERABILITY ASSESSMENT AND PENETRATION TESTING**

Author :Prashant S. Shinde, Shrikant B. Ardhapurkar

Description: Vulnerability Assessment and Penetration Testing (VAPT) helps to assess the effectiveness and ineffectiveness of the security arrangements of web application to stay protected against the rising Cyber threats. The projected work helps to develop a versatile mechanism which is able to find vulnerabilities from internet applications. So, Identification of Vulnerabilities and remedy of a similar has become one among the prime issues for organizations. With the growing inter-connectivity of systems and advancement in Cyber Services, the extent of Cyber Attacks has conjointly exaggerated. Thus so as to stay immune and for threat minimization, Vulnerability Assessment and Penetration Testing (VAPT) is conducted by the organizations on regular basis [5].

This paper explains the difference between assessment of vulnerability and penetration testing.

The two types of vulnerability testing are Vulnerability Assessment and Penetration Testing (VAPT) which can often be combined for achieving better vulnerability analysis results. So VA and PT are nothing but two different tasks giving different results but within the same workspace.

Here they have explained various types of vulnerabilities and tools to analysis or assess them.

6. **PENETRATION TESTING: A DUET**

Author: Dr. Daniel Geer and John Harthorne

Description: In this paper, author described Penetration testing is the art of finding an open door. It is not a science as science depends on falsifiable hypotheses. And hackers as Artists. This paper explains the characterization and specialisation. Successful penetrations can be characterized as the illegitimate acquisition of legitimate authority. Specialization is, for any field, a consequence of expanding knowledge and the accumulating complexity thereof. Where that knowledge is itself knowledge about complexity, as it is here given the fundamental axiom that complexity is the chief enemy of security, the growth rate in (knowledge) complexity compounds and the rate of needful specialization accelerates [6].

This paper explains briefly the five W's Application of penetration testing as: Why, Who, What, Where and When.

7. **PENETRATION TESTING: ANALYZING THE SECURITY OF THE NETWORK BY HACKER'S MIND**

Author:HarmandeepSingh , Dr. SurenderJangra, Dr. Pankaj Kumar Verma

Description: This paper explained the penetration testing and methodology for performing network security and its assessment. It also discussed the prevalent tools and techniques for information gathering and vulnerability assessment.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 4, April 2018

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.
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 and Clean Up. And finally concluded as 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 [7].

## III. CONCLUSION

The various aspects and theoretical survey on the different network structure and different way of proceeding with penetration testing and vulnerability scanning have been studied, analyzed and presented in this paper.

## IV. ACKNOWLEGMENT

I would like to express my gratitude to Ms. V Uma Rani for her Encouragement and guidance. We are also thankful to the faculty member of School Of Information Technology for their valuable suggestion.

## REFERENCES

[1] R. Shanmugapriya, “A study of network security using penetration testing”, Presented at System, Applications and Technology Conference (LISAT), IEEE Long Island, 2016.
[2] Harshdeep Singh, Dr.Jaswinder Singh, “Penetration testing in wireless networks”, International Journal of Advanced Research in Computer Science, 8 (5), May-June 2017, pp. 2213-2216 .
[3] Sandhya s, SohiniPurkayastha, Emil Joshua, Akash Deep, “Assessment of Website Security by Penetration Testing Using Wireshark”, Presented at 2017 International Conference on Advanced Computing and Communication Systems (*ICACCS* -2017), Jan. 06 – 07, Coimbatore, INDIA, 2017.
[4] FilipHolik, Josef Horalek, OndrejMarik, SonaNeradova, StanislavZitta, “Effective penetration testing with Metasploit framework and methodologies”, CINTI 2014 • 15th IEEE International Symposium on Computational Intelligence and Informatics • 19–21 November, 2014 • Budapest, Hungary, pp. 237-242.
[5] Prashant S. Shinde, Prof. Shrikant B. Ardhapurkar, “Cyber Security Analysis using Vulnerability Assessment and Penetration Testing”, Presented at IEEE Sponsored World Conference on Futuristic Trends in Research and Innovation for Social Welfare (WCFTR’16), 2016.
[6] Dr. Daniel Geer and John Harthorne, “Penetration:A duet”, Presented at Proceedings of the 18th Annual Computer Security Applications Conference (ACSAC.02), 2002.
[7] Harmandeep Singh, Dr. SurenderJangra, Dr. Pankaj Kumar Verma, “Penetration Testing: Analyzing the Security of the Network by Hacker’s Mind”, Volume V, Issue V, May 2016 IJLTEMAS, pp. 56-60.