ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Survey on Ethical Hacking Process in Network Security

U. Murugavel[*1], Dr. Shanthi[2]

[*1] Ph.D. Research Scholar (Part-Time), Bharathiar University, Chennai, Tamil Nadu, India

[2] Vice Principal, Alpha Arts and Science College, Chennai, Tamil Nadu, India.

murugavel.research@gmail.com

Abstract

Hacking is a process in which, a person or team exploits the weakness in a system for self-proceeds or indulgence. Ethical Hacking is an activity which focuses on the vulnerability in a system and discovers the weakness and try to rectify the security weakness of a system. In the emergent field of internet, computer security is the ultimate concern for the organizations and governments. Ethical hacker plays a vital role in protecting the valuable and sensitive data in a system. This main objective of this paper is to explore the process behind ethical hacking and penetration testing in network security.

Keywords: Hacking, Ethical Hacking, Vulnerability, Penetration Testing, Network Security.

Introduction

With the rapid growth of the cyber technology world, computer security has become a foremost concern for governments and business peoples where the possibility of being hacked is comparative to the security implemented in their infrastructure. Professional ethical hackers use the same methods and techniques used by hackers to investigate the security flaws and vulnerabilities without affecting the target systems or sensitive data. Once ethical process is complete, the security team will give the details report to the owners with the vulnerabilities they found and instructions on how to eradicate such security flaws.

What is Ethical Hacking?

Ethical hacking is the process of introspect the security weakness and discovers the potential security vulnerabilities for a client which is responsible for the attacked information technology environment. Ethical hackers typically have very strong programming and Networking skills and apply their silks to protect sensitive data they work on client side.

White Hats and Black Hats

Ethical hacker is also known as White hat hacker, or white hat, they use programming skills to determine the vulnerabilities in computer systems. Non-ethical hacker or black hat exploits these vulnerabilities for mischief, personal gain or other purposes. Ethical hacker introspect the weakness in computer security, points them out and may suggest changes to system to secure the information.

Penetration Testing

Penetration testing also known as intrusion testing or red teaming is the method of examining the weakness and vulnerabilities of Computer and network security. Penetration testing helps to measure the effectiveness of system security or ineffectiveness of the system security.

Need of Penetration Testing

The main purpose of penetration testing is to identify the security weakness under controlled circumstances so that the security flaws can be eliminated before hackers exploit the system. Ethical hackers use their skills and apply penetration testing to discover the vulnerability Assessment, give importance to high sensitive data. Penetration testing may be done from business perspective to safeguard the organization against failure through preventing financial loss, as well as operational perspective to identify the risk and vulnerabilities.

Types of Penetration Test

Generally there are two type of penetration testing namely

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

1) Black Box Test 2) White Box Test

The type of penetration testing depends upon the situation of an organization wants to test, whether the scope is to simulate an attack by an insider (employee, network admin/ system admin, etc) or external source. The difference between the two is the amount of information provided to the penetration tester about the system is tested. In black box penetration testing is closely stimulated to that of an external attacker, giving little info or no knowledge about the systems to be tested. The penetration testers gather as much as information about the target system as possible to perform the test. In white box penetration testing the tester generally provided with detailed information about the network to be tested include the IP address.

Merits of Penetration Testing

Penetration testing are effective for many reasons (1) avoid cost of network (2) preserve the corporate image and customer loyalty (3) meet the requirements (4) manage vulnerabilities. Penetration testing provides detailed information about actual, exploitable security threats. By doing penetration test we can easily identify the vulnerabilities are most critical as well as least significant. Penetration test benefits the organization by performing security patches and security resource more precisely to safeguard the information

Literature Review

Title: ETHICAL HACKING: A TECHNIQUE TO ENHANCE INFORMATION SECURITY
Author: GURPREET K. JUNEJA1

In this journal, the author analyzed various Ethical hacking process and phases of hacking involved in Ethical Hacking. Selection of tools plays a vital role in ethical hacking and password cracking tools used in ethical hacking namely ethercao, tcdump, SATAN,
Strobe, firewalk, cybercrop and web password cracking tool such as Brutus, web cracker and obiwan. Finally the author conclude that Ethical hacking is new technique to identify the security attacks and vulnerabilities, Ethical hacker is an educator to enlighten customer and also the security industry.[1]

Title: AN OVERVIEW OF PENETRATION TESTING
Author: AILEEN G.BACUDIO1,XIAOHONG YUAN1, BEI-TSENG BILL CHU2,MONIQUE JONES1

In this paper the author examines the need of penetration testing and various strategies involved in penetration testing and its types, How to conduct the penetration testing. Author listed out the tools to conduct penetration testing such as Nmap, Hping, Xprobe, Nessus and other toos to conduct the penetration testing. Web penetration testing tools include like Metasploit, Iss scanner, shadow security scanner and etc., web server fingerprinting, application fingerprinting and various Ethical hacking tools to discover the security weakness in web server. the author suggest that penetration testing is useful to identify the vulnerabilities in system and three phase methodology used in penetration testing, the final report needs enough detail and substance to allow to rectify the attack pattern and respect findings.[2]

Title: NEED OF ETHICAL HACKING IN ONLINE WORLD.
Author: MONIKA PANGARIA1, VIVEK SHRIVASTAVA2

In this paper, the authors investigated the need of Ethical hacking in online world and mentioned the survey on cyber Security, type of data stolen in cyber technology world and scope and limitation in ethical hacking, the impact of ethical hacking in cyber security.

The author identifies the security challenges around the online cyber world. Ethical hacker must strive for a strategy to prove fruitful in all case. Whether in distributed environment or other environment where security patch for present system cause vulnerability in future changes.[3]

Title: ETHICAL HACKING
Author: AJINKYA A. FARSOLE1, AMRUTA G.KASHIKAR2, APURVA ZUNZUNWALA3

In this journal author discuss about ethical hacking history, case studies and ethical hacking process to identify the security attacks. Selecting the ethical hacking tools plays a vital role to discover the security vulnerabilities and also mentioned various

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

types of attacks and state the characteristics in tools for ethical hacking, the documentation details needed in computer system. finally the author conclude that through regular auditing ,vigilant intrusion testing, and good system administrating proactive once can avoid security attacks and cyber vandalism.[4]

Title: ETHICAL HACKING TECHNIQUES WITH PENETRATION TESTING
Author: K.BALA CHOWDAPPA, S. SUBBULAKSHMI, P.N.V.S PAVAN KUMAR

This paper deals with security life cycle, hacking strategies , hacking types and phases involved in hacking process , penetration testing strategies in ethical hacking and state the strategies of network in penetration testing include vulnerability identification, network hopping, brute force methods, automated scanners, web page verification. The author concludes that penetration testing and how ethical hacking is important in computer world.[5]

Title: ETHICAL & PENETRATION TESTING: AN OVERVIEW
Author: AKANKSHA BANSAL CHOPRA

In this paper the author describes about Penetration testing is carried out with the intent of finding errors and how penetration is valuable for security attack vectors and identify the risk involved in system, assessing the magnitude of potential business and operational impacts of successful attacks, testing the ability of network defenders, and also it includes the benefits of penetration testing, types, phases of ethical hacking, methodologies of penetration testing, precaution to be followed, risks involved while perform penetration testing and also state the limitation of penetration testing. Author concludes that penetration testing should not be confused with stimulated hacking, not damaging the target and penetration testing focus on legitimate authorization. Penetration testing strengthen the security and to eliminate the weakness of target systems.[6]

Title: ARE COMPUTER HACKER BREAK-INS ETHICAL?
Author: EUGENCE H. SPAFFORD

The concept of ethical hacking is new buzz. The author discussed about various security arguments namely idle system argument, student hacker argument, and social protector argument. Author justifies that hacker break-ins are ethical only in extreme situations like life critical emergency and also discusses why no break–ins is harmless. At last the author conclude that no obvious damage are unethical at the same time endangering the security of other peoples machines or attempting to force them are not ethical. [7]

Title: ETHICAL HACKING IN LINUX ENVIRONMENT
Author: ANIRUDDH P TEKADE, PRAVIN GURJAR, PANKARJ R. INGLE, DR.B.B MESHRAM

In this paper author discuss about the difference between hacker and cracker, philosophy of hacking , the approach of hackers and reveals the secret of hacking .how hacking is done in Linux environment and open source software, local access control in Linux Environemnt,console access, stealing data using a bootable Linux cd,Rooting directory and privilege escalation. Restrict system calls with systradce interactive policies. The author concludes that penetration testing require proper interpretation, penetration is useful for finding flaws in security weakness. [8]

Methodology

From the above review of Literature, Ethical hacking, penetration testing are use used to identify the security vulnerabilities, different strategies are used in penetration testing, risk involved in preserving the data, ways to enhance the information security. The problems to implementing the penetration testing in online world, various testing techniques are used to identify the vulnerabilities and security flaws. Ethical hacking tools to discover the weakness and password cracks. The ideas of the Literature review, in this article have identified the mentioned problem in implementing the penetration testing in online cyber world. With the help of penetration testing techniques security of computer system can be strengthened and security weaknesses are identified.

Conclusion

Ethical hacking is done with appropriate direction help us to discover the security vulnerabilities. Penetration testing is more valuable to identify the security weakness in a system. It is useful to prevent loss of data, financial loss and proactive

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

elimination of identified risks. Implementing penetration testing through regular auditing, intrusion detection and good system administration once can secure the sensitive data and protect valuable information from hackers. In conclusion ethical hackers use their knowledge and network skills to discover the security vulnerabilities and enlighten the customer, business and secure the system.

Acknowledgment

I convey my honest thanks to Dr. Shanthi[2] Vice Principal, for her valuable suggestions, comments and directing me to publish this international journal and my sincere thanks to my parents for supporting and encouraging me.

References

1. Gurpreet K. Juneja1, A Technique to Enhance Information Security,dec 2013
2. Aileen G. Bacudio, 1Xiaohong Yuan, 2Bei-Tseng Bill Chu, 1Monique Jones, An Overview of Penetration Testing, Volume3.no.6, Nov 2011
3. Monika Pangaria1, Vivek Shrivastava2, Need of Ethical Hacking in Online World, Volume.2. Issue 4.Apr 2013
4. Ajinkya A. Farsole1, Amruta G.Kashikar2, Apurva zunzunwala3, Ethical Hacking, Volume1. No.10, 2010
5. K.Bala Chowdappa,S. Subbulakshmi, P.N.V.S Pavan Kumar, Ethical Hacking Techniques with Penetration Testing, Volume 5(3).2014
6. Akanksha Bansal Chopra, Ethical & Penetration Testing: An overview, Volum1, Issue 1, June 2014
7. Eugene H. Spafford, Are Computer Hacker Break Ins Ethical? April 1997
8. Aniruddha P Tekade, Pravin Gurjar,Pankaj R. Ingle,Dr.B.B Meshram, Ethical Hacking in Linux Environment. Volume 3.jan 2013
9. Danish Jamil, Is Ethical Hacking Ethical?
10. Kumar Utkarsh, System Security and Ethical Hacking Volume 1.Issue 1. 2013
11. Marilyn Leathers, Closer Look at Ethical Hacking and Hackers
12. Dinesh Babu S, Ethical Hacking, Volume.3.Jan-2012.
13. Kenneth Einar Himma ,The Ethics of Tracing Hacker Attacks through the Machines of Innocent Persons, Volume.2, 11/2004
14. Regina D. Hartley, .Rationale for a hacking methodological approach to network security
15. Jeffrey Livermore, Walsh College, Member, IEEE Computer Society, What Are Faculty Attitudes toward Teaching Ethical Hacking and Penetration Testing? June2007.