International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 11 Issue 2 –NOVEMBER 2014.

Ethical Hacking and Penetration Testing Strategies

V.V.N. SURESH KUMAR

Lecturer in mathematics, KBN College, kothapeta, Vijayawada

sureshmathskbn@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 growing era of internet computer security is of utmost concern for the organizations and government. These organizations are using Internet in their wide variety of applications such as electronic commerce, marketing and database access. But at the same time, data and network security is a serious issue that has to be talked about. This paper attempts to discuss the overview of hacking and how ethical hacking disturbs the security. Also the Ethical Hackers and Malicious Hackers are different from each other and playing their important roles in security. This paper studied the different types of hacking with its phases. The hacking can also be categorized majorly in three categories such as white hat, black hat and grey hat hacking. This paper also presents a comparison of the hacking categories with different methods of penetration testing. Key words: Ethical Hacking, Hackers, Hacking Phases.

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

I. INTRODUCTION

With the growth of internet, computer security is of utmost concern for the organizations and government. These organizations are using Internet in their wide variety of applications such as electronic commerce, marketing and database access.. The information such as credit card numbers ,telephone numbers, home addresses, bank account numbers etc. that are available on network may easily be hacked by unsocial elements. They would steal passwords and other information by intruding into the system so as to take control of the entire system.. The system administrator would then have to resume and make repairs to the system., The media instead of calling these intruders as “computer criminal,” began to call them as “hackers” and described them as individuals who intrudes into some others’ computers, may be for fun or revenge, or money. Initially, “hacker” was meant as a compliment, as this person was well verse with computer programming and knowledge, therefore ,term “cracker” or “intruder” for those hackers who used their skills for dark side of hacking. Ethical hackers have clear intensions to break computer security to save the organization from intrusion attacks. They never reveal the facts and information about the organization. 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.

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.

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 internal testing is performed from within the organization's technology environment. This test mimics an attack on the internal network by a disgruntled employee or an authorized visitor having standard access.

Privileges:

The focus is to understand what could happen if the network perimeter were successfully penetrated or what an authorized user could do to penetrate specific information resources within the organization's network.

The techniques employed are similar in both types of testing although the results can vary greatly.

Need of Penetration Testing

The main purpose of penetration 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.

II. TESTING STRATAGIES

External testing strategy: External testing refers to attacks on the organization's network perimeter using procedures performed from outside the organization's systems, that is, from the Internet or Extranet. This test may be performed with non-or full disclosure of the environment in question. The test typically begins with publicly accessible information about the client, followed by network enumeration, targeting the company's externally visible servers or devices, such as the domain name server (DNS), e-mail server, Web server or firewall.

•Internal testing strategy: Internal testing is performed from within the organization's technology environment. This test mimics an attack on the internal network by a disgruntled employee or an authorized visitor having standard access privileges. The focus is to understand what could happen if the network perimeter were successfully penetrated or what an authorized user could do to penetrate specific information resources within the organization's network. The techniques employed are similar in both types of testing although the results can vary greatly.

•Blind testing strategy: A blind testing strategy aims at simulating the actions and procedures of a real hacker. Just like a real hacking attempt, the testing team is provided with only limited or no information concerning the organization, prior to conducting the test. The penetration testing team uses publicly available information (such ascorporate Web site, domain name registry, Internet discussion board, USENET and other places of information) to gather information about the target and conduct its penetration tests. Though blind testing can provide a lot of information about the organization (so called inside information) that may have been otherwise unknown, for example, a blind penetration may uncover such issues as additional Internet access points, directly connected networks, publicly available confidential/proprietary information, etc. But it is more time consuming and expensive because of the effort required by the testing team to research the target.

•Double blind testing strategy: A double-blind test is an extension of the blind testing strategy. In this exercise, the organization's IT and security staff are not notified or informed beforehand and are "blind" to the planned testing activities. Double-blind testing is an important component of testing, as it can test the organization's security monitoring and incident identification, escalation and response procedures. As clear from the objective of this test, only a few people within the organization are made aware of the testing. Normally it's only the project manager who carefully watches the whole exercise to ensure that the testing procedures and the organization's incident response procedures can be terminated when the objectives of the test have been achieved.

Types of Penetration Test

Generally there are two type of penetration testing namely 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.

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.

Automated vs. Manual

Automated and manual penetration testing can be both used as a means to evaluate an organization’s security controls system. Automated testing has been the mainstream approach adopted by organizations because of the rapid technological changes to provide economies of scale compared to manual one, though manual testing may consist of several weeks with an investment of thousands of dollars, whereas an automated can perform the tests within several hours with reduced costs20.

This shows that automated tools can be more cost-effective and efficient if conducted properly. Another benefit of automation is that organizations can perform these tests as frequent as they want compared to ethical hacking practitioners who conduct testing only during working hours. On the other hand, there can be an overreliance and false sense of security on automated tools because they do not guarantee that it will catch 100% of the security gaps in the system and are only as effective as the individuals who programmed and run these tests. In other words, there is a risk that an untrained employee who handles and manages the automated testing can cause more damages to the organization than the expected benefit. Furthermore, an automated testing lacks the flexibility of substituting different scenarios as compared to an extensive manual testing performed by a knowledgeable and experienced ethical hacking practitioner.

External vs. Internal

As identified above, testing should be conducted to address the internal and external threats. Internal testing is performed within the organization's system and simulates what an authorized user or employee could potentially act. On the other hand, external testing attempts to simulate what an external hacker could potentially harm from outside the system. The red team would conduct intrusion attacks on the organization's network system through the use of the Internet or Extranet25. The red team generally targets the organization's servers or devices, such as "Domain Name Server, email server, web server or firewalls". It appears that an internal testing may be more comprehensive because an authorized user can either use the internal or external system to hack into an organization's information system. Blind vs. Double-Blind vs. Targeted Testing

In a blind testing environment, the red team is only provided with publicly available information, such as the organization's website, domain name registry and any other related discussion boards on the Internet. With this limited information, penetration testing attempts to accumulate information to exploit an organization's security weaknesses. It can reveal information about an organization that it would not have known, but can be more time-consuming and expensive due to the extensive effort to conduct research prior to the testing phase.

In a double-blind testing environment, the blind testing process is expanded in which the organization's IT and other staffs are not informed beforehand about the intended testing activities. Hence, they are also considered "blind" to the test. In this type of scenario, very limited people within the organization are aware of the testing, and it requires continuous monitoring by the project sponsor to ensure that the testing procedures can be eliminated once the objective has been attained. Furthermore, this test can reveal the effectiveness of an organization's monitoring, identification and response procedures to incidents.

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.

Limitations of Penetration Testing

According to the Information Technology Association of Canada (ITAC), penetration testing cannot be expected to identify all possible security weaknesses, nor does it guarantee that it is 100% secure. New technology and hacking methods can create new exposures not anticipated during the penetration testing. Thus, it is certainly possible that after a penetration testing, there could be hacking incidents thereafter because it is impossible to have full but rather only good protection for an organization's security system.

III. 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 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.

IV. REFERENCES

[1] Agarwal, Ankit Kumar, Hacking : Research paper, online http://ankitkumaragarwal.com /hacking-a-research-paper/ (visited on may 2012)

[2] Wilhelm, Douglas. "2". Professional Penetration Testing.Syngress Press. p. 503.ISBN 978-1-59749-425-0

[3] Moore, Robert (2006). Cybercrime: Investigating High-Technology Computer Crime (1st ed.). Cincinnati, Ohio: Anderson Publishing. ISBN 978-1-59345-303-9

[4] EC-Council (n.d.). Ethical Hacking and Countermeasures, online http://www.eccouncil.org/ ipdf/EthicalHacker.pdf (visited on may 2012)

[5] Ethical Hacking Basics Class part , online http://www.go4expert.com/forums/ showthread.php?t=11925 (visited on may 2012)

[6] Palmer, C.C.(2001,April 13). Ethical Hacking. IBM Systems Journal Vol. 40 No.3 2001 About Effective Penetration Testing Methodology byByeong-Ho KANG