RESEARCH REVIEW JOURNALS
Volume-03
Issue-09
September-2018

ISSN: 2455-3085 (Online)
RESEARCH REVIEW International Journal of Multidisciplinary
www.rrjournals.com [UGC Listed Journal]

Ethical Hacking

Shaveta

Assistant Professor, Department of Computer Science & Applications, Guru Nanak College, Ferozepur, Punjab (India)

ARTICLE DETAILS

Article History
Published Online: 07 September 2018

Keywords
Hathical hacking, Hacker, IT

ABSTRACT

Traditionally, a hacker is someone who likes to tinker with software or electronic systems. Hackers enjoy exploring and learning how computer systems operate. They love discovering new ways to work electronically. Although ethical is an often overused and misunderstood word, the MerriamWebster dictionary defines ethical perfectly for the context of this book and the professional security testing techniques that I cover — that is, conforming to accepted professional standards of conduct. IT practitioners are obligated to perform all the tests covered in this paper aboveboard and only after permission has been obtained by the owner(s) of the systems.

1. Introduction

Ethical hacking — also known as penetration testing or white-hat hacking — involves the same tools, tricks, and techniques that hackers use, but with one major difference: Ethical hacking is legal. Ethical hacking is performed with the target's permission. The intent of ethical hacking is to discover vulnerabilities from a hacker's viewpoint so systems can be better secured. It's part of an overall information risk management program that allows for ongoing security improvements. The purpose of ethical hacking is to improve the security of the network or systems by fixing the vulnerabilities found during testing. Ethical hackers may use the same methods and tools used by the malicious hackers but with the permission of the authorized person for the purpose of improving the security and defending the systems from attacks by malicious users.Ethical hacking can also ensure that vendors' claims about the security of their products are legitimate. The fact that the design methodologies consist if lots of small refinement steps.

2. History

Since the 1980's, the Internet has vastly grown in popularity and computer security has become a major concern for businesses and governments. Organizations would like to use the Internet to their advantage by utilizing the Internet as a medium for e-commerce, advertising, information distribution and access, as well as other endeavors. However, they remain worried that they may be hacked which could lead to a loss of control of private and personal information regarding the organization, its employees, and its clients..

- In a search for ways to reduce the fear and worry of being hacked, organizations have come to the realization that an effective way to evaluate security threats is to have independent security exerts attempt to hack into their computer systems. In the case of computer security, these tiger teams or ethical hackers would use the same tools and techniques as an attacker, but rather than damage the system or steal information, they would evaluate the system security and report the vulnerabilities they found and provide instructions for how to remedy them [3].C programming language features were derived from earlier language called 'B' (Basic Combined Programing Lange – BCPL)

- From the early days of computers, ethical hacking has been used as an evaluation of system security. Many early ethical hacks were conducted by the United States Military to cary out security evaluations on their operating systems to determine whether they should employ a two-level (secret/top secret) classification system. However, with the growth of computing and networking in the early 1990's, computer and network vulnerability studies began to appear outside of the military organization. In December of 1993, two computer security researchers, Dan Farmer from Elemental Security and WietseVenema from IBM, suggested that the techniques used by hackers can be used to asses the security of an information system. They wrote a report that was shared publicly on the Internet which described how they were able to gather enough information to compromise security and they provided several examples of how this information could be gathered and exploited to gain control of a system, and how such an attack could be prevented.&RC.

- Security Analysis Tool for Auditing Networks, or SATAN, received a great amount of media attention due to its capabilities and implications. The SATAN tool provided auditing capability as well as capabilities to provide advice regarding how the user may be able to correct the problems that were discovered.

3. Attacks to operating sysyem

It's one thing to know that your systems generally are under fire from hackers around the world. It's another to understand specific attacks against your systems that are possible. For example, a default Windows OS configuration, a weak SQL Server administrator password, and a server hosted on a wireless network may not be major security concerns separately. But exploiting all three of these vulnerabilities at the same time can be a serious issue.: -

- **Nontechnical attacks**
  Exploits that involve manipulating people — end users and even yourself — are the greatest vulnerability within any computer or network infrastructure. Humans are trusting by nature, which can lead to social-engineering exploits. Social engineering is defined as the exploitation

- **Network-infrastructure attacks.**
  Hacker attacks against network infrastructures can be easy, because many networks can be reached from anywhere in the world via the Internet

- **Operating-system attacks**
  Hacking operating systems (OSs) is a preferred method of the bad guys. OSs comprise a large portion of hacker attacks simply because every computer has one and so many well-known exploits can be used against them. Occasionally, some operating systems that are more secure out of the box — such as Novell NetWare and the flavors of BSD UNIX — are attacked, and vulnerabilities turn up. But hackers prefer attacking operating systems like Windows and Linux because they are widely used and better known for their vulnerabilities.

4. Hacking Phases

Hacking Can Be Done By Following These Five Phases:

Phase 1: Reconnaissance: can be active or passive: in passive reconnaissance the information is gathered regarding the target without knowledge of targeted company (or individual). It could be done simply by searching information of the target on internet or bribing an employee of targeted company who would reveal and provide useful information to the hacker.

This process is also called as “information gathering”. In this approach, hacker does not attack the system or network of the company to gather information. Whereas in active reconnaissance, the hacker enters into the network to discover individual hosts, ip addresses and network services. This process is also called as “rattling the doorknobs”. In this method, there is a high risk of being caught as compared to passive reconnaissance.

Phase 2: Scanning: In Scanning Phase, The Information Gathered In Phase 1 Is Used To Examine The Network. Tools LikeDialers’, Port Scanners Etc. are being Used by the Hacker to Examine the Network So As To Gain Entry in the Company’s System And Network.

Phase 3: Owning the System: This Is The Real And Actual Hacking Phase. The Hacker Uses The Information Discovered In Earlier Two Phases To Attack And Enter Into The Local Area Network (LAN, Either Wired Or Wireless), Local Pc Access, Internet Or Offline. This Phase Is Also Called As “Owning The System”.

Phase 4: Zombie System: Once the hacker has gained the access in the system or network, he maintains that access for future attacks (or additional attacks), by making changes in the system in such a way that other hackers or security personals cannot then enter and access the attacked system. In such a situation, the owned system (mentioned in Phase 3) is then referred to as “Zombie System

5. Benefits of ethical hacking

- This type of “test” can provide convincing evidence of real system or network level threat exposures through proof of access. Even though these findings may be somewhat negative, by identifying any exposure you can be proactive in improving the overall security of your systems.

- A mature security information program is a combination of policies, procedures, technical system and network standards, configuration settings, monitoring, and auditing practices. Business systems, which have resisted simple, direct attacks at the operating system or network level, may succumb to attacks that exploit a series of procedural, policy, or people weak points.

- An ethical hack, which tests beyond operating system and network vulnerabilities, provides a example, should your ethical hack prove that your firewalls could withstand an attack because there was no breach, but no one noticed the attacks, you may be better prepared to make a case for improving intrusion detection broader view of an organization’s security. The results should provide a clear picture of how well your detection processes works as well as the response mechanisms that should be in place. “Tests” of this sort could also identify weakness such as the fact that many systems security administrators may not be as aware of hacking techniques as are the hackers they are trying to protect against.

6. Limitations of ethical hacking

- Ethical hacking is based on the simple principle of finding the security vulnerabilities in systems and networks before the hackers do, by using so-called “hacker” techniques to gain this knowledge. Unfortunately, the common definitions of such testing usually stops at the operating systems, security settings, and “bugs” level. Limiting the exercise to the technical level by performing a series of purely technical tests, an ethical hacking exercise is no better than a limited “diagnostic” of a system’s security.

- Time is also a critical factor in this type of testing. Hackers have vast amounts of time and patience when finding system vulnerabilities. Most likely you will be engaging a “trusted third party” to perform these test for you, so to you time is money. Another consideration in this is that in using a “third party” to conduct you tests, you will be providing “inside information” in order to speed the process and save time.

- A further limitation of this type of test is that it usually focuses on external rather than internal areas, therefore, you may only get to see half of the equation. If it is not possible to examine a system internally, how can it be established that a system is “safe from attack”, based purely upon external tests? Fundamentally this type of testing alone can never provide absolute assurances of security.

7. Key points to remember c language

1. Hacking has both its benefits and risks. Hackers are very diverse.
2. The battle between the ethical or white hat hackers and the malicious or black hat hackers is a long war, which has no end.

8. Conclusion

This also concludes that hacking is an important aspect of computer world. It deals with both sides of being good and bad. Ethical hacking plays a vital role in maintaining and saving a lot of secret information, whereas malicious hacking can destroy everything. What all depends is the intension of the hacker. It is almost impossible to fill a gap between ethical and malicious hacking as human mind cannot be conquered, but security measures can be tighten.

References

1. Gurpreet K. Juneja,”Ethical hanking :A technique to enhance information security”international journal of computer applications(3297: 2007),vol. 2,Issue 12,december2013
2. K.BalaChowdappa et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 3389-3393
3. Eleventh LACCEI Latin American and Caribbean Conference for Engineering and Technology (LACCEI’2013)
4. ”Innovation in Engineering, Technology and Education for Competitiveness and Prosperity” August 14 - 16, 2013 Cancun, Mexico. “Faculty Attitudes Toward Teaching Ethical Hacking to Computer and Information Systems “Undergraduates Students Aury M. Curbelo, Ph.D,Alfredo Cruz, Ph.D. [6] Kumar Utkarsh” SYSTEM SECURITY AND ETHICAL HACKING”

