RESEARCH ARTICLE OPEN ACCESS

Study Of Ethical Hacking

Bhawana Sahare[1], Ankit Naik[2], Shashikala Khandey[3]
Research Scholar[1&3], Lecturer[2]
Department of Computer Science and Engineering,
Kirodimal Institute of Technology, Raigarh
Chhattisgarh - India

ABSTRACT

The state of security on the internet is very poor. Hacking is an activity in which, a person exploits the weakness in a system for self-profit or gratification. As public and private organizations migrate more of their critical functions or applications such as electronic commerce, marketing and database access to the Internet, then criminals have more opportunity and incentive to gain access to sensitive information through the Web application. Thus the need of protecting the systems from the hacking generated by the hackers is to promote the persons who will punch back the illegal attacks on our computer systems. Ethical hacking is an identical activity which aims to find and rectify the weakness and vulnerabilities in a system. Ethical hacking describes the process of hacking a network in an ethical way, therefore with good intentions. This paper describes what is ethical hacking, what are the types of ethical hacking, impact of Hacking on Businesses and Governments. This paper studied the different types of hacking with its phases.

***Keywords*:-** Vulnerabilities, Hacker, Cracker, Port and Intrusion.

I. INTRODUCTION

A. What is Hacking

Hacking is the technique in which the persons ,what's in a name? Call them hackers, crackers, intruders, or attackers, they are all interlopers who are trying to break into your networks and systems. Some do it for fun, some do it for profit,or some simply do it to disrupt your operations and perhaps gain some recognition. Though they all have one thing in common; they are trying to uncover a weakness in your system in order to exploit it.[9]

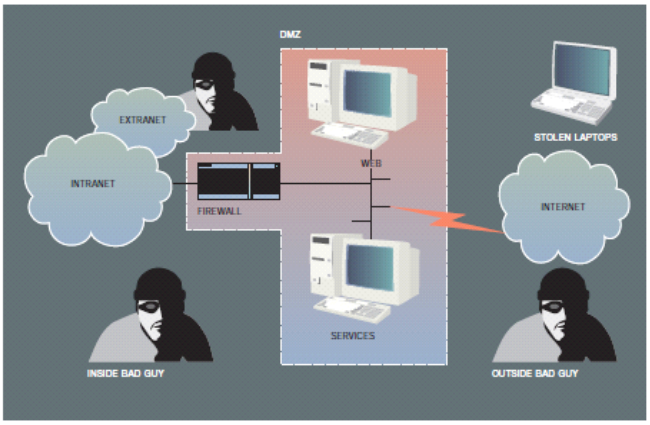

Fig. 1. Different ways to attack computer security

Local network test simulates an employee or other authorized person who has a legal connection to the organization's network. The primary defenses that must be defeated here are intranet firewalls, internalWebservers, server security measures, and e-mail systems.

In **Stolen laptop computer** test, the laptop computer of a key employee, such as an upper-level manager or strategist, is taken by the client without warning and given to the ethical hackers. They examine the computer for passwords stored in dial- up software, corporate information assets, personnel information, and the like. Since many busy users will store their passwords on their machine, it is common for the ethical hackers to be able to use this laptop computer to dial into the corporate intranet with the owner's full privileges.

Social engineering test evaluates the target organization's staff as to whether it would leak information to someone. A typical example of this would be an intruder calling the organization's computer help line and asking for the external telephone numbers of the modem pool. Defending against this kind of attack is the hardest, because people and personalities are involved. Most people are basically helpful, so it seems harmless to tell someone who appears to be lost where the computer room is located, or to let someone into the building who "forgot" his or her badge. The only defence against this is to raise security awareness.

Physical entry This test acts out a physical penetration of the organization's building. Special arrangements must be made for this, since security guards or police could become involved if the ethical hackers fail to avoid detection. Once inside the building, it is important that the tester not be detected. One technique is for the tester to carry a document with the target company's logo on it. Such a document could be found by digging through trash cans before the ethical hack or by casually picking up a document from a trash can or desk once the tester is inside. The primary defenses here are a strong security policy, security guards, access controls and monitoring, and security awareness. Each of these kinds of testing can be performed from three perspectives: as a total outsider, a semi-outsider, or a valid user.

A **total outsider** has very limited knowledge about the target systems. The only information used is available

through public sources on the Internet. This test represents the most commonly perceived threat. A well-defended system should not allow this kind of intruder to do anything.

A **semi-outsider** has limited access to one or more of the organization's computers or networks. This tests scenarios such as a bank allowing its depositors to use special software and a modem to access information about their accounts. A well-defended system should only allow this kind of intruder to access his or her own account information.

A **valid user** has valid access to at least some of the organization's computers and networks. This tests whether or not insiders with some access can extend that access beyond what has been prescribed. A well defined system should allow an insider to access only the areas and resources that the system administrator has assigned to the insider.[8]

B. What is Ethical Hacking?

Fig. 2 Ethical hacking.

Ethical hacking is also known as "Penetration Hacking" or "Intrusion Testing" or "Red Teaming".[3] Ethical hacking is defined as the practice of hacking without malicious intent. the Ethical Hackers and Malicious Hackers are different from each other and playing their important roles in security .According to Palmer (2004, as quoted by Pashel, 2006): "Ethical hackers employ the same tools and techniques as the intruders, but they neither damage the target systems nor steal information. Instead, they evaluate the target systems' security and report back to owners with the vulnerabilities they found and instructions for how to remedy them". [10] The vast growth of Internet has brought many good things like electronic commerce, email, easy access to vast stores of reference material etc. As, with most technological advances, there is also other side: criminal hackers who will secretly steal the organization's information and transmit it to the open internet. These types of hackers are called black hat hackers. So, to overcome from these major issues, another category of hackers came into existence and these hackers are termed as ethical hackers or white hat hackers.

Ethical hacking is a way of doing a security assessment. Like all other assessments an ethical hack is a random sample and passing an ethical hack doesn't mean there are no security issues. An ethical hack's results is a detailed report of the findings as well as a testimony that a hacker with a certain amount of time and skills is or isn't able to successfully attack a system or get access to certain information. Ethical hacking can be categorized as a security assessment, a kind of training, a test for the security of an information technology environment. An ethical hack shows the risks an information technology environment is facing and actions can be taken to reduce certain risks or to accept them. We can easily say that Ethical hacking does perfectly fit into the security life cycle shown in the below figure[3]

Fig. 3 Security Life Cycle

II. TYPES OF HACKING/HACKERS

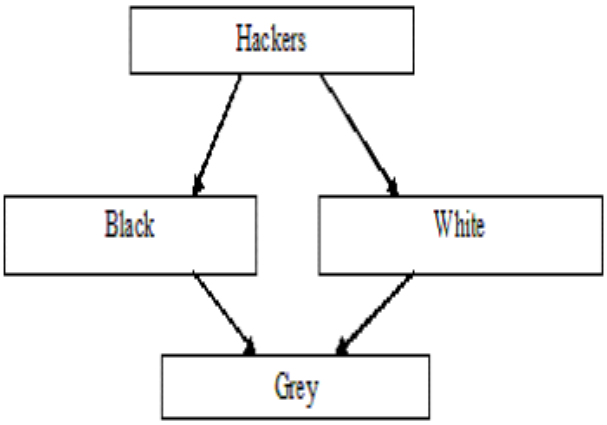

Fig. 4 Hackers Types

The hacking can be classified in three different categories, according to the shades or colours of the "Hat". The word Hat has its origin from old western movies where the colour of Hero's' cap was "White" and the villains' cap was "Black". It may also be said that the lighter the colour, the less is the intension to harm.

A. White Hat Hackers

White Hat Hackers are authorized and paid person by the companies, with good intends and moral standing. They are also known as "IT Technicians". Their job is to safeguard Internet, businesses, computer networks and systems from crackers. Some companies pay IT professionals to attempt to hack their own servers and computers to test their security. They do hacking for the benefit of the company. They break security to test their own security system. The white Hat Hacker is also called as an Ethical Hacker[6]. In contrast to White Hat Hackers.[3]

B. Black Hat Hackers

The intension of Black Hat Hackers is to harm the computer systems and network. They break the security and intrude into the network to harm and destroy data in order to make the network unusable. They deface the websites, steal the data, and breach the security. They crack the programs and passwords to gain entry in the unauthorized network or system. They do such things for their own personal interest like money. They are also known as "Crackers" or Malicious Hackers Other than white hats and black hats.[3]

C. Grey hat hackers

Another form of hacking is a Grey Hat. As like in inheritance, some or all properties of the base class/classes are inherited by the derived class, similarly a grey hat hacker inherits the properties of both Black Hat and White Hat. They are the ones who have ethics. A Grey Hat Hacker gathers information and enters into a computer system to breech the security, for the purpose of notifying the administrator that there are loopholes in the security and the system can be hacked. Then they themselves may offer the remedy. They are well aware of what is right and what is wrong but sometimes act in a negative direction. A Gray Hat may breach the organizations' computer security, and may exploit and deface it. But usually they make changes in the existing programs that can be repaired. After sometime, it is themselves who inform the administrator about the company's security loopholes. They hack or gain unauthorized entry in the network just for fun and not with an intension to harm the Organizations' network. While hacking a system, irrespective of ethical hacking (white hat hacking) or malicious hacking (black hat hacking), the hacker has to follow some steps to enter into a computer system, which can be discussed as follows.[3]

III. 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.

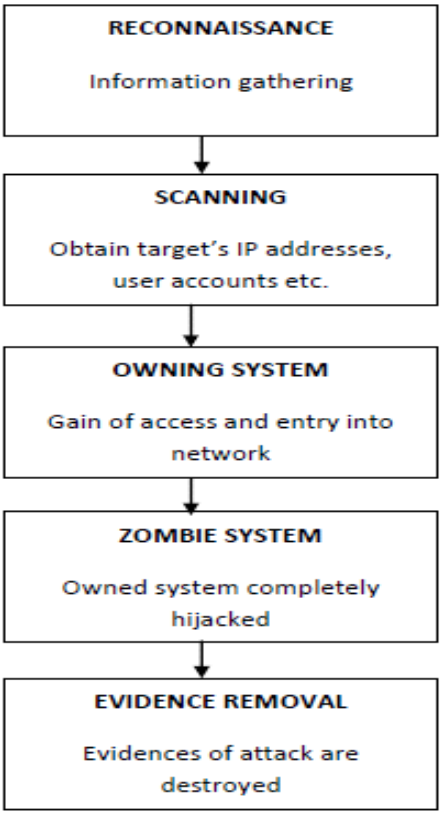

Fig. 5 Hacking Phases

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 Like Dialers', 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".

Phase 5: Evidence Removal: In this phase, the hacker removes and destroys all the evidences and traces of hacking, such as log files or Intrusion Detection System Alarms, so that he could not be caught and traced. This also saves him from entering into any trial or legality. Now, once the system is hacked by hacker, there are several testing methods available called penetration testing to discover the hackers and crackers. [3]

IV. IMPACT OF HACKING ON BUSINESSES AND GOVERNMENTS

Some of the most expensive and prolific victims of hacking have been businesses. Businesses are many times targeted for their customers' personal and financial data and often are targeted by their own employees, whether disgruntled or just opportunistic. Businesses lose billions of dollars yearly as a result of hacking and other computer breaches. Many times, the true cost cannot be evaluated because the effects of a security breach can linger for years after the actual attack. Companies can lose consumer confidence and in many cases are held legally responsible for any loss to their customers. The cost of recovering from an attack can spread quickly: legal fees, investigative fees, stock performance, reputation management, customer support, etc. Companies, and more recently, consumers, are investing more and more money into preventing an attack before it actually happens. Businesses that hold stores of consumer's personal and financial data are especially taking extra steps to insure the data's safety. Microsoft's online group, MSN/Windows Live, requires that no single group store personally identifiable information without explicit consent from an internal security group. Security reviews occur frequently for groups that do store consumers' data and the security group performs its own personal security review by actually attempting to hack into the sites. Sites have actually been with held from releasing to the web due to flaws found through this method. Other businesses that are more limited in technical areas employ outside security experts to assist them with their security. ScanAlert.com boasts of working with over 75,000 secure ecommerce sites, including many famous brands like Foot Locker, Restoration Hardware and Sony. The ecommerce sites host a "Hacker Safe" logo, stating that the site is tested daily and is effectively preventing 99.9% of hacker crime. The Scan Alert disclaimer though appears far less confident: This information is intended as a relative indication of the security efforts of this web site and its operators. While this, or any other, vulnerability testing cannot and does not guarantee security; it does show that [the e-Commerce Site] meets all payment card industry guidelines for remote web server vulnerability testing to help protect your personal information from hackers. HACKER SAFE does not mean hacker proof. HACKER SAFE certification cannot and does not protect any of your data that may be shared with other servers that are not certified HACKER SAFE, such as credit card processing networks or offline data storage, nor does it protect you from other ways your data may be illegally obtained such as non-hacker "insider" access to it. While Scan Alert makes reasonable efforts to assure its certification service is functioning properly, Scan Alert makes no warranty or claim of any kind, whatsoever, about the accuracy or usefulness of any information provided herein. By using this information you agree that Scan Alert shall be held harmless in any event.[7]

A. 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.

- However, information security should not be strictly limited to the mechanics of hardening networks and computer 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. These findings could help promote a need for better communication between system administrators and technical support staff, or identify training needs.

- Quite often, security awareness among senior management is seriously lacking.

traditional diagnostic work primarily deals with the possibility of a threat and this often leads to a casual view of the threat, deferring the need to immediately address the requirements. Through an ethical hacking exercise, especially if the results are negative, senior management will have a greater understanding of the problems and be better able to prioritize the requirements. For improving intrusion detection.[9]

B. 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. The opportunity for discovery may be limited since the testers may only work by applying the information they have been given.

- 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. Consequently, such assessment techniques may seem, at first, to be fundamentally flawed and have limited value, because all vulnerabilities may not be uncovered.[9]

V. CONCLUSION

Hacking has both its benefits and risks. Hackers are very diverse. They may bankrupt a company or may protect the data, increasing the revenues for the company. The battle between the ethical or white hat hackers and the malicious or black hat hackers is a long war, which has no end. While ethical hackers help to understand the companies' their security needs, the malicious hackers intrudes illegally and harm the network for their personal benefits. which may allow a malicious hacker to breach their security system. Ethical Hackers help organizations to understand the present hidden problems in their servers and corporate network.[3] Ethical Hacking is a tool, which if properly utilized, can prove useful for understanding the weaknesses of a network and how they might be exploited.[2]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 [3]

REFERENCES

[1] Wikipedia

[2] Gurpreet K. Juneja,"Ethical hanking :A technique to enhance information security"international journal of computer applications(3297: 2007),vol. 2,Issue 12,december2013

[3] K.Bala Chowdappa et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 3389-3393

[4] Eleventh LACCEI Latin American and Caribbean Conference for Engineering and Technology (LACCEI'2013)

[5] "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"