ISSN: 2455 - 1597

ijergs
Open Access

International Journal of Engineering Research and Generic Science (IJERGS)
Available Online at www.ijergs.in

Volume - 4, Issue - 6, November - December - 2018, Page No. 88 - 83

An Overview of Ethical Hacking Technique to Enhance Information Security

[1]Vivek Kumar Jethani, Dept. of Computer Science, Arya College of Engineering and Research Center, Jaipur, Rajasthan

[2]Shalini Joshi, Dept. of Computer Science, Arya College of Engineering and Research Center, Jaipur, Rajasthan

[3]Aman Soni, Dept. of Computer Science, Arya College of Engineering and Research Center, Jaipur, Rajasthan

[4]Anuj Raj, Dept. of Civil Engineering, Arya College of Engineering and Research Center, Jaipur, Rajasthan

E-mail: [1]vivekkrjethani@gmail.com, [2]shalini.joshi2710@gmail.com, [3]amansonirj0203@gmail.com

[4]anujraj1309@gmail.com

Abstract

The explosive growth of the Internet has led to many good things like e-commerce, online banks, e-mail and cloud computers, but there is also a dark side like hacking and backing down. Etc. Piracy is the first major problem facing governments, businesses and ordinary citizens around the world. A moral hacker can help people who are suffering from this hacking. This document describes ethnic hackers, their skills, their attitude and how they find their customers and find security advances. Test the piracy problems that the company deals with in this article.

Keywords: Ethical Hacking, Vulnerabilities, Hacker, Cracker, Information Security.

Introduction

The explosive growth of the Internet has brought many positive things: e-business, easy access to the main references, collaboration, e-mail, new forms of advertisement and distribution, just to name a few. If in most technical developments, hackers have a dark side. Rego, companies and citizens around the world are trying to participate in this revolution, but they fear that the servers of your web server will pirate, replace your pornographic logo, read your email and your credit card. Obtain online programs or transplant programs that are transmitted in secret from your organization to the Internet. With these and other types, hackers can help moralists. This document describes ethnic hackers: their skills and attitudes and how they can find their clients and close security spaces. With the growth of the Internet, IT security has become a major concern for businesses and governments. They want to benefit from the Internet for e-commerce, advertising, distribution, access to information and other activities, but they are afraid to attack. At the same time, potential customers are interested in these services when managing their personal information, credit cards to social security numbers and private homes. In seeking a way to solve the problem, companies have realized that the best way to assess the risk of unnecessary interest is for independent security experts to attempt to access their computer systems. This program can be compared to the independent hearing program that invites the organization to view its books. In In the case of IT security, these teams use the same tools and techniques used by hackers, without damaging target systems or stealing information. Instead, it will assess the vulnerability of target systems and inform those at risk, as well as tips for resolving them.

Hacking

Piracy is a technique that hackers, hackers. Hackers or attackers are hackers trying to penetrate their Networks and systems. Some do it for fun, others do it for violence, or just to block their work and recognize something. Although everyone has one thing in common, they try to detect weaknesses in their system to exploit them.

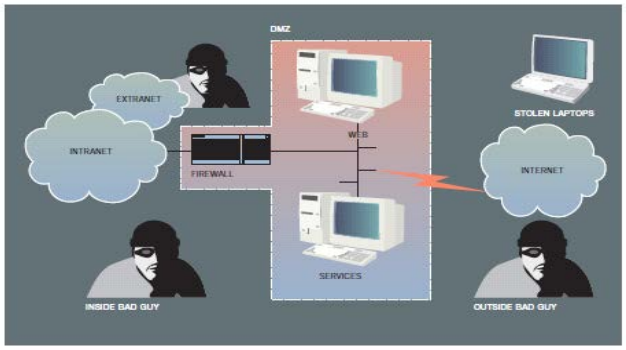

Figure 1 : Different Ways to Attack Computer Security

Social engineering is about getting people to give confidential information. The type of information that may indicate this may be different, but when people try, they just get their password or bank information as they get access to their secretary computer. This will give you access to your passwords and information and allow you to control your computer.

Criminals use social technology techniques because it is usually easier to trust their natural inclination or explore ways to push their program. For example, an e-phishing attack is a computer-based social structure that uses an attack, a social e-mail.

Physical access is a computer term that refers to the ability of people to access physical access to the computer system. It is often said that in the event of physical access to a bureau, a prosecute of invalid information can quickly find the information needed to access the computer system and the business network.

Physical access also provides installation of hardware key loggers. The parasite can boot from a CD or other external medium and read as scanned data from the hard drive. They can also use the absence of access control in the boot manager.

Figure 2 : Physical Access Control

The valid user has valid access to at least some computers and networks in your organization. This proves that launching any access can extend this access further than expected In the definition of the system, the average water system, the label and the help for all means of communication in the middle of the fan system and the customer service system or the operating system.

Ethical Hacking

Moral piracy is also known as piracy. Ethnic piracy is defined as a practice of piracy without sulphurous intentions. Hackers and hackers distinguish each other and play an important role in security. According to Palmer (2004, in Pashel,

2006): "Hackers use the same tools and techniques as hackers, but they do not play any specific systems, or information, or process." Good things, such as e-commerce, e-mail, access to extensive repositories of reference equipment, etc. In the Internet, these types of Hackers have called the black dog pirates and have overcome these major problems. The name of these pirates is moral pirates or white pirates. Ethnic piracy is a way of doing a safety evaluation. Just like all other evaluations, it is a random problem for the Ethics and it does not seem to be a hazardous problem. The results of moral progress are an extensive report of the results and a witness that a hacker with a certain time and ability has the ability to influence a system or access to certain information. Ethnic piracy can be classified as security evaluation, a kind of training and a test of the security of a computer environment. The ethical trunk illustrates the risks of an IT environment and measures can be made to lower or accept certain risks. It is easy to say that Ethiopian piracy is well suited to the safety bug in the picture below.

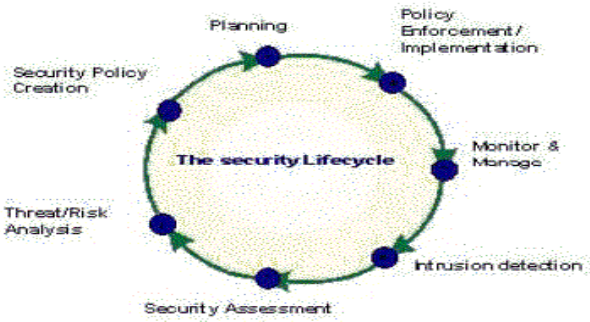

Figure 3 : Security of Life Cycle

Types of Hackers

Piracy can be classified in three different categories, depending on the nuances or colors of the "hat". The word has originated in the old western films where the color of the "hero" was "white" and the roof of the destruction was "black". It can also be said that it is clearer the color, the less serious is the intention to harm it.

White Hat Hakers

White pirates are put down and paid by companies, with good intentions and a moral reputation. He is also known as a computing-technician. Your task is to protect the internet, business, business networking and tackle systems. Some companies see computer scientists trying to penetrate their servers and computers to prove their safety. Hack for the benefit of the company. It breaks security to test your security system. White pirates are also called eti pirates. Unlike the pirates in white caps.

Black Hat Hackers

Black Hat Hackers are designed to destroy computer and network systems. It blocks security and gets annoying in the network and earns data to redirect the network. They remove web pages, send data, and secure the security. Compiled programs and passwords to access the network or an unauthorized system. They do so for their own personal benefit, such as money. Also known as "crackers" or merciful hackers that are not black and white caps.

Grey Hat Hackers

Gray hat hacking is the also one of the type of hacking. As in the case of inheritance, the derived class inherits some or all of the characteristics of the basic classes / classes, just as a gray chopper inherit the characteristics of the black hats and

white. They are those who have the ethics. The Gray Hat hacker collects information and comes into the computer system to improve the security to notify the administrator of security breaches and to inform that the system may be compromised. Then they can provide a treatment themselves. They know exactly what is right and what is wrong, but sometimes they do negative. Gray Hat can remove the computer security of businesses and can use and process them. However, they usually make changes to existing programs that can be corrected. After a while, they are themselves responsible for the security vulnerabilities of the company. Hack an or get unauthorized entries on the network just for fun and not for the structure of organizations damaged by the network. When hacking a system, independent of piracy (piracy) or piracy (black piracy), the hacker should follow some steps to access the computer system that can be analyzed as following.

Hacking Phases

Hacking Can Be Done By Following These Five Phases:

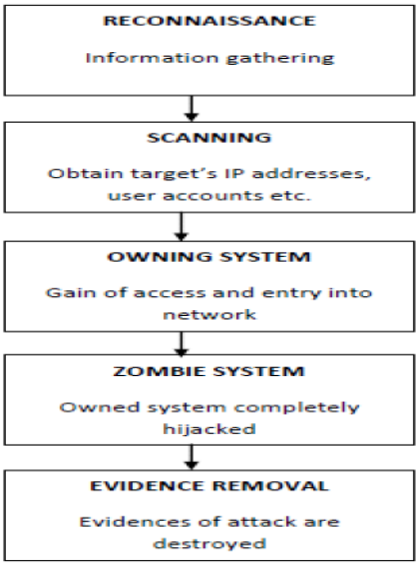

Figure 4: Hacking Phase

Phase 1: Reconnaissance

The questionnaire may be active or negative: in negative identification the information is collected in relation to the target without the target group (or the individual). This can be easily done by searching for information about goals on the Internet or to safeguard an employee of a particular company providing open and information for hackers.

This process is called "collecting information". In this approach, the hacker is not required to collect information about the system or business network. In active order, the hacker in the network will discover different hosts, IP addresses and network services. This process is also called "unstable doors". In this way, the risk of falling in high proportion to the negative opinion.

Phase 2: Scanning

In the explosive phase, the information collected in the phase 1 can tell us the network. Tools such as bookmarks, gate scanners, etc. Used to be used. Through the hacker to check the network and get revenue in the system and the business network.

Phase 3: Owning the System

This is actually true in real life. Hacker uses the information that has been detected twice because you may not have access to the local area network (LAN, turned on) from local computers, the Internet or offline. This step is also called the "property of the system".

Phase 4: Zombie System

One of the hackers has access to the system or network, maintains access to future attacks (or additional attacks) through changes in the system so hackers or other staff cannot access the system of the attack. In such a case, the proprietary system (referred to in step 3) as a "zombie system" is called..

Phase 5: Evidence Removal

Hacker is currently negotiating and destroying any evidence and piracy effects such as log files or intrusion detection system alarms so they cannot be recorded or followed. It also prevents him from participating in a trial or trial. Now, once hackers enter the system, many of the test methods available are called penetration tests to detect hackers and hackers.

Benefits of Ethical Hacking

This type of "test" can be convincing evidence of real threats to the system or network through access control. While these results may be negative, the identification of each exhibit may be proactive to improve the overall security of your systems.

However, the information security must not be limited to the mechanisms of networks and the strengthening of information systems. MEP is a set of strategies, procedures, technical standards, network standards, configuration parameters, and auditing practices. Entrepreneurs that provide easy and direct attacks against the operating system or the network interface can be attacked by a variety of procedural, political or human weaknesses.

The moral trick, which overcomes the vulnerability of the operating system and the network, is an example. If it shows that your firewall can get an attack, because there is no trespass, but no one has asserted the attacks, you can be better off to improve the detection of intruders. Bread of the safety of the organization. The outcomes must give a clear picture of the success of the filling, such as the revisions to be present. A "test" of this type can also identify weaknesses, such as the fact that many security system administrators are not familiar with pyramid techniques such as hackers trying to protect. These findings can strengthen the need to improve communication between system administrators and technical entities, or to identify the training companies.

Senior managers often have little alertness of security. Traditional diagnostic work focuses on the potential for threat, which often leads to an accidental vision of the threat, delaying the need to respond immediately to requirements. Through the practice of moral penetration, especially when the results are negative, senior management will better understand the problems and can better prioritize the requirements. Improve the detection of hackers.

Limitation of ethical hacking

Ethical penetration is based on the simple principle of security disabilities in systems and networks for hackers, using techniques that are known for "hackers" to get this knowledge. Unfortunately, general definitions of such keys usually stop on operating system, security settings, and "errors". By expanding the practice at the technical level by making a series of pure technical tests, the practice of moral penetration is not better than a limited "diagnostic" of the security of

the system. The time is also a critical factor in this type of test. Hackers have a lot of time and patience with systemic capabilities. You are likely to create a "trusted third party" to do these tests. The time you need is money. Another discussion is to talk about using a "third party" to test out, ensures "internal information" to conquer the process and save time. Discovery possibilities can be limited as people can work by applying the information they are offered.

Another disadvantage of this type of test is that it usually focuses on external areas in the area of internal territories, so that only half of the equation can be viewed. If it is not possible to examine the system internally, how can you talk about being "safe from attack" based on purely external evidence? Essentially, these tests can only provide absolute security barriers. Therefore, these evaluation techniques may initially cause defect and limited value, and all the weaknesses cannot be found.

Conclusion

The idea to test the security of the system when trying to access is not new. In practice, the safety problem will remain as long as the manufacturers remain connected to existing system environments that are strictly required for security. Provided that ad hoc arrangements and security systems are supported for such inappropriate designs and that the ghosting results of the penetration equipment are acceptable as proof of the security of the computer system, secure security will not be a problem. Periodic evaluation, intrusion detection, good system management practices and computer security awareness are important elements of the organization's security agencies. An error in one of these areas may increase the organization for electronic sabotage, wasting, loss of income, reasonable or worse. Each new technology has its benefits and risks. While ethnic hackers can help the clients, their safety may need to be better understood, it is up to them to keep their protections in place.

References

1. Gurpreet K. Juneja," Ethical hacking :A technique to enhance information Security "international journal of computer applications(3297: 2007),vol. 2,Issue 12,december2013
2. Meenaakshi N. Munjal,"ETHICAL HACKING: AN IMPACT ON SOCIETY", Cyber Times International Journal of Technology & Management Vol. 7 Issue 1, October 2013 – March 2014.
3. C. C. Palmer, "Ethical hacking". IBM Systems Journal, Volume: 40, Issue: 3, 2001.
4. Susidharthaka Satapathy , Dr.Rasmi Ranjan Patra, "Ethical Hacking", International Journal of Scientific and Research Publications, Volume 5, Issue 6, June 2015.
5. Regina D. Hartley,"Ethical Hacking Pedagogy: An Analysis and Overview of Teaching Students to Hack", Journal of International Technology and Information Management, vol-24, issue-4, pp-95-104, 2015.