International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 11 Issue 5 –NOVEMBER 2014.

Ethical Hacking and Countermeasures

Dr. P.B.SandhyaSri

HoD, Dept of Physics, KBN College, Vijayawada, A.P., India

sandhyasri.prathipati@gmail.com

Abstract— Hacking is one of the most dangerous disease from which the global world is suffering from. This project concentrates on how the malicious attacks and the effects of hacking caused to our community .It provides complete picture and preventive measures so solve the problem of hacking. Different aspects of hacking are discussed over here. Today's generation is still lagging in solving the problem of hacking attacks and in taking out the preventive measures in solving this global problem which is increasing day by day. To solve this problem of hacking attacks sophisticated security tool are invented. That's why we should start to think about hacker's psychology as the main way to prevent and stop attacks by understanding their needs or desires.

The invention of internet has solved many problems and brought many new things to this world like electronic commerce, easy access to vast stores of reference material collaborative computing, e-mail, and but at the same time it gave rise to the most dangerous problem called hacking. Governments companies, and private citizens around the world are anxious to be a part of this revolution, but they are afraid that some hacker will break into their Web server and replace their logo with pornography, read their e-mail, steal their credit card number from an on-line shopping site, or implant software that will secretly transmit their organization's secrets to the open Internet. This study describes the skill, attitude and how this will help the customers finding and plugging security holes and the ethical hacking problem is explained and along with global problems and solutions to those problems are listed out.

I. INTRODUCTION

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. So, this paper describes ethical hackers, their skills and how they go about helping their customers and plug up security holes. Ethical hackers perform the hacks as security tests for their systems. This type of hacking is always legal and trustworthy In other terms ethical hacking is the testing of resources for the betterment of technology and is focused on securing and protecting IP systems. So, in case of computer security, these tiger teams or ethical hackers would employ the same tricks and techniques that hacker use but in a legal manner and they would neither damage the target systems nor steal information. Instead, they would evaluate the target system's security and report back to the owners with the vulnerabilities they found and instructions for how to remedy them. 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.

II. HACKING METHOD

Phising Method-Phising is the method that you are familiar with. You create a Fake Account and ID in yahoo and fool your friends by telling them to send the victim's ID, their own ID and their own Password in your Fake Yahoo Account. Brute Force Hack-Brute Force Hack is a Hacking which takes much time to get Password of the Victim and it needs a Hacker to learn about JavaScript's and all the non-sense. Fake Login Hack-Fake Login Hack is the Hacking used by most of you for your goal by creating a Fake Login Page and telling your friends to login there and the Password would come to you. Cookie Steal Hack -Cookie Steal Hack is somewhat similar to Fake Login Hack as you prepare a Cookie Stealer and tell your friends to open your Cookie so that his Password would come to you. Web Mail Hack-Web Mail Hack is the toughest method to learn for Hacking as it also needs a Hacker to learn about JavaScript's, Computer Tricks and much more and there is also software for this type of Hack

III. WHO ARE ETHICAL HACKERS?

These early efforts provide good examples of ethical hackers. Successful ethical hackers possess a variety of skills. First and foremost, they must be completely trustworthy. While testing the security of a client's systems, the ethical hacker may discover information about the client that should remain secret. In many cases, this information, if publicized, could lead to real intruders breaking into the systems, possibly leading to financial losses. During an evaluation, the ethical hacker often holds the "keys to the company," and therefore must be trusted to exercise tight control over any information about a target that could be misused. The sensitivity of the information gathered during an evaluation requires that strong measures be taken to ensure the security of the systems being employed by the ethical hackers themselves: limited-access labs with physical security protection and full ceiling-to-floor walls, multiple secure Internet connections, a safe to hold paper documentation from clients, strong cryptography to protect electronic results, and isolated networks for testing.

Ethical hackers typically have very strong programming and computer networking skills and have been in the computer and networking business for several years. They are also adept at installing and maintaining systems that use the more popular operating systems (e.g., UNIX**or Windows NT**)used on target systems. These base skills are augmented with detailed knowledge of the hardware and software provided by the more popular computer and networking hardware vendors. It should be noted that an additional specialization in security is not always necessary, as strong skills in the other areas imply a very good understanding of how the security on various systems is maintained. These systems management skills are necessary for the actual vulnerability testing, but are equally important when preparing the report for the client after the test.

In the computer security realm, the ethical hacker's task is the harder one. With traditional crime anyone can become a shoplifter, graffiti artist, or a mugger. Their potential targets are usually easy to identify and tend to be localized. The local law enforcement agents must know how the criminals ply their trade and how to stop them. On the Internet anyone can download criminal hacker tools and use them to attempt to break into computers anywhere in the world. Ethical hackers have to know the techniques of the criminal hackers, how their activities might be detected, and how to stop them. These issues. Most of them were computer users from various disciplines, such as astronomy and physics, mathematics, computer science, philosophy, or liberal arts, who took it personally when someone disrupted their work with a hack.

One rule that IBM's ethical hacking effort had from the very beginning was that we would not hire hackers. While some will argue that only a "real hacker" would have the skill to actually do the work, we feel that the requirement for absolute trust eliminated such candidates. We likened the decision to that of hiring a fire marshal for a school district: while a gifted ex-arsonist might indeed know everything about setting and putting out fires, would the parents of the students really feel comfortable with such a choice? This decision was further justified

What do ethical hackers do?

An ethical hacker's evaluation of a system's security seeks answers to three basic questions:

What can an intruder see on the target systems?

What can an intruder do with that information?

Does anyone at the target notice the intruder's attempts or successes?

While the first and second of these are clearly important, the third is even more important: If the owners or operators of the target systems do not notice when someone is trying to break in, the intruders can, and will, spend weeks or months trying and will usually eventually succeed.

When the client requests an evaluation, there is quite a bit of discussion and paperwork that must be done up front. What are you trying to protect?

What are you trying to protect against?

How much time, effort, and money are you willing to expend to obtain adequate protection?

IV. TYPES OF HACKING

White Hat Hacker-Also referred as Ethical Hacker or sometimes called as Sneakers. A White Hat Hacker mainly focuses on securing corporate Network from outsider threat. They are with good intention who fight against Black Hat.

Grey Hat Hacker-They are Skilled Hacker who sometimes act legally and sometime not. In simple word you may call a Grey Hat hacker as Hybrid between White Hat and Black Hat hacker. Black Hat Hacker -Also referred as Cracker. A Black Hat Hacker's intentions to break into others Network, and wish to secure his own machine. They often uses different techniques for breaking into systems which can involve advanced programming skills and social engineering.

V. HACKING WITH ETHICS

A Locally Stored Passwords:

Most browsers, including Internet Explorer® and Netscape®, the AOL® client, and Windows® Dial-Up Connections allow you the option to store passwords. These passwords are stored on the local machine and (depending upon where and how it is stored) there is usually a method of recovering these passwords. Storing any password locally is insecure and may allow the password to be recovered by anyone who has access to the local machine. While we are not currently aware of any program to recover locally stored AOL® passwords, we do not recommend that these are secure. Software does exist that can recover most of the other types of locally stored passwords. B Trojan A Trojan is a program that

is sent to a user that allows an attacker to control functions of the target computer, recover information from the target or to delete or damage files on the target. The name Trojan is given because the program will usually come attached to some other program or file that entices you to run it. There are a wide variety of Trojans any number of which can be programmed to capture passwords as they are typed and to email or transmit them to a third party. To protect yourself against Trojans, you should never execute or download software or files that are not from a trusted source. It is critical that anyone working on internet use a virus protection program (which should catch most Trojans.) Note that since a Trojan requires the password to be typed or stored in order to be recovered, this is not an effective way to recover your own password. It could explain, however, how someone could lose their password to a hacker. Sending someone a Trojan program is certainly illegal and we do not recommend or condone this activity. A Trojan is unlikely to be effective in recovering a particular account password since it requires the target to install it. However, hackers will often bulk mail Trojans to thousands of people in the hope that a small percentage will get caught. Legitimate account holders who may have been caught by a Trojan and can authenticate themselves should contact their service provider to have their account passwords reset.

Impersonation

It is possible to impersonate a program on a computer by launching windows that look like something else. For instance, let's say you login to the MSN® service and visit a website (in this case a hostile website.) It would be possible for this website to pop-up some windows that look like something else. They could look almost identical to windows that an inexperienced user might expect from his local computer. The user could be fooled into submitting information to the hostile website. For instance, consider the effect of seeing the following series of windows:

If these could trick you into entering your password, then you could end-up sending your password to the attacker. Windows such as these could be created to mirror virtually any programmer series of actions. Your browser will likely identify your operating system and your IP address might identify your ISP. Therefore, a hostile website could target you with a series of screen shots that look exactly as they should on your system. The key is that the screen shots are not coming from your system, but are coming from the hostile website. First, creating such a hostile website is probably fraudulent and illegal. We do not recommend or condone this activity. To protect yourself against this type of attack, make sure to configure your browser for high security and enable warnings for any code that is executed on your system.

VI. CONCLUSION

It is for educational purpose only .Try to secure your pc from the hackers. Do not think hacking is crime. Hacking is not a crime depends upon user the user mind set will be change. In this generation every process along with computer we need to know whether our data is secure or not.

VII. REFERENCES

[1] www.computerhope.com/jargon/e/ethihack.htm
[2] www.eccouncil.org/certification/certified-ethical-hacker
[3] https://www.isoeh.com/
[4] www.breakthesecurity.com/
[5] www.ethicalhacking.com/