An Extensive Empirical Study of Ethical Hacking

Vijay Shankar Rai[1], Prof. Ashutosh Pandey[2]
[1, 2] Dept of Computer Science & Engineering
[1, 2] ABES Institute of Technology,Ghaziabad, Uttar Pradesh, India

Abstract- *Ethical hacking as the term denotes is used for ethical, legal or good reasons. Ethical Hackers work similarly to any other black hat hacker or cracker but their aim is to provide complete security to any system to prevent other black hat hackers. They find out the loopholes in any operating systems and apply complete security to it so that other hackers would not able to attack the system. Ethical hacking-also known as penetration testing or intrusion testing or red teaming has become a major concern for businesses and governments. Companies are worried about the possibility of being " hacked " and potential customers are worried about maintaining control of personal information. [1] This paper describes ethical hackers: their skills, their attitudes, and how they go about helping their customers find and plug up security holes. The ethical hacking process is explained, along with many of the challenges and opportunities in the field of ethical hacking.*

Keywords- Automated Security, Education and Training and Ethical Hacking, Hackers

I. INTRODUCTION

Ethical hacking, as the name suggests a hacking which is ethical. It is also called as penetration testing. This is the technique which is being used by number of professionals to do hacking but that is not illegal it is rather ethical. That is the reason it is to be called as ethical hacking.

Because of the increasing popularity of computers and their continued high cost, access to them was usually restricted. When refused access to the computers, some users would challenge the access controls that had been put in place. They would steal passwords or account numbers by looking over someone's shoulder, explore the system for bugs that might get them past the rules, or even take control of the whole system. They would do these things in order to be able to run the programs of their choice, or just to change the limitations under which their programs were running.

Initially these computer intrusions were fairly benign, with the most damage being the theft of computer time. Other times, these recreations would take the form of practical jokes. However, these intrusions did not stay benign for long. Occasionally the less talented, or less careful, intruders would accidentally bring down a system or damage its files, and the system administrators would have to restart it or make repairs. Other times, when these intruders were again denied access once their activities were discovered, they would react with purposefully destructive actions. When the number of these destructive computer intrusions became noticeable, due to the visibility of the system or the extent of the damage inflicted, it became "news" and the news media picked up on the story. Instead of using the more accurate term of "computer criminal," the media began using the term "hacker" to describe individuals who break into computers for fun, revenge, or profit. Since calling someone a "hacker" was originally meant as a compliment, computer security professionals prefer to use the term "cracker" or "intruder" for those hackers who turn to the dark side of hacking. For clarity, we will use the explicit terms "ethical hacker" and "criminal hacker" for the rest of this paper.

II. WHAT IS ETHICAL HACKING

Ethical Hacking is done by computer experts who use their programming capabilities to understand the system vulnerabilities. Ethical Hacking is performed by an individual who is termed as white hat or skilled expert with computers, who is given permission to use their programming skills which will help them detect any minor vulnerability in thesystem. The computer security community is strongly self-policing, given the importance of its work. Most ethical hackers, and many of the better computer and network securityexperts, did not set out to focus on these issues.

III. NEED FOR ETHICAL HACKING

Indian corporation should invest in Ethical Hacking and penetration reviews of IT infrastructure:

- To prevent defacement of corporate websites with vulgar images and obscene text.
- To protect confidential client or financial data from being compromised.
- To prevent IT assets from being used as launch pad for virus attacks.
- To comply with industry and other IT regulatory frameworks.
- To validate risk assessment.

IV. ROLE OF ETHICAL HACKERS

- There can lots of roles and responsibilities for an ethical hacker, but to summarize their roles and responsibilities a White hat hacker can do the following for an organization
- They can find out the vulnerabilities and loopholes in any IT system.
- Ethical Hackers can also suggest the list of steps that should be taken to prevent the risk on a system and can also provide the system complete security.
- They can recommend any organization about the detailed report and analysis related to security of any IT system.

V. TYPES OF ETHICAL HACKING

There are mainly four different types of ethical hacking depending on the knowledge of the hacker. There are many hackers whose intentions are not to harm. Basically the term ethical hacking itself says that hacking which is done for the purpose of not to harm rather take preventive measures to maintain the security and safety and check the vulnerabilities in the current system.

A. HACKTIVISTS

This is the technique through which a hacker is hacking into any computer system illegally for any reason may be social or political. In this activity a hacker can leave a very large message on the main page of any well-known website or any other so called important message so that visitor will see that message and react accordingly. It may display any kind of speech or any social message which can attract users and they may participate in the discussion or forum.This may lead to hacking the system without the consent of the target. It may have any social message like ethical hacking is ethical or not which may attract number of users and they can participate in the discussion.

B. CYBERWARRIOR

Cyber warrior is a kind of hacker who is being hired by an organisation or by an individual to creep into the system or computer network. Cyber warrior will act as a wicked hacker will try to find out the

C. WHITE BOX PENETRATION

TESTERS White box penetration testers are also called as white box hackers. They are the employees those are hired by the organisation to break into their current system orcomputer network. They are the legal penetration testers. They are legally breaking into the system or computer network for the organisation or for an individual to help them by telling the vulnerabilities and weaknesses in the present system. White box testers are working in the same way as cyber warriors are working the only difference is that cyber warriors do not haveknowledge of the system or computer network of the organisation or of individual whereas white box hackers are having full knowledge of the system or computer network of the target. We can also consider it as that the attack is being simulated by an insider of the organisation.

D. CERTIFIED ETHICAL HACKER / LICENSED PENETRATION TESTER

As the name says itself that certified ethical hacker or licensed penetration tester are those certified or licensed professional in the field of hacking who are performing the duties of both i.e. black box hacker and white box hackers. They are responsible to look into the system and networks to find out the vulnerabilities and weaknesses

VI. TYPES OF HACKERS

- **Script Kiddie**

Script Kiddies don't really care about hacking into systems and stealing things. They simply copy code and use it for a virus, SQLi or something else. Script Kiddies will never hack for themselves, they will just download some overused software (such as LOIC or Metasploit) and watch a YouTube video on how to use it. A very common Script Kiddie attack would be a DOS (Denial of Service) or DDOS (Distributed Denial of Service), where they flood an IP with so much useless information that it collapses, preventing other people from using it.

- **White Hat**

White Hat hackers are also known as ethical hackers, and they're the good guys of the hacker world. They help you remove viruses, perform pen tests and generally help people understand where their vulnerabilities are and fix them. Most White Hat hackers will hold some form of computer or security related qualification, and often pursue careers in hacking and cyber security. They love the challenge of finding the holes but have no interest in doing anything with them. There are even a number of qualifications specifically for them – Offensive Security Certified Professional (OSCP), CREST Certified Infrastructure Tester and CREST Certified Application Security Tester.

- **Black Hat:**Black Hat hackers, or 'crackers' are the types of people you often hear about on the news and from businesses trying to sell cyber services. They find banks and big companies with weak security systems and steal credit card information, confidential data or money. Their methods are varied but actually fairly basic most of the time.

- **Grey Hat:**As with everything in this world, nothing is just black and white. Grey Hat hackers don't steal information or money like Black Hat hackers (though they may sometimes deface a website for fun), nor do they help people out like white hack hackers. Instead, they spend most of their time just playing around with systems, without doing anything harmful. This type of hacker actually makes up most of the hacking community, even though Black hat hackers garner most of the media's attention.

- **Green Hat:**Green Hat hackers are the babies of the hacker world. They are new to the game and mainly use script, like Script Kiddies, but they have aspirations of becoming full blown hackers. They are often found asking questions of fellow hackers and listening with childlike curiosity.

- **Red Hat:**Red Hat hackers are the vigilantes of the hacker world. They're like white hats in the sense that they put a stop to Black hat attacks, but they are downright scary in how they do it. Instead of reporting the malicious hacker they find lurking inside a business, they shut them down by uploading viruses, DoSing and accessing their computer to destroy it form the inside out. Red hats use many different aggressive methods to force the cracker out and potentially even kill their computer. The good news is, businesses don't need to worry about these.

- **Blue Hat:**And finally, we have the Blue Hat hackers. If a Script Kiddie ever took revenge, he would become a Blue Hat Hacker. Blue Hat hackers will seek vengeance on anyone who has made them angry. Most Blue Hat hackers are fairly new to the hacking world, but unlike green hats they have no desire to learn.

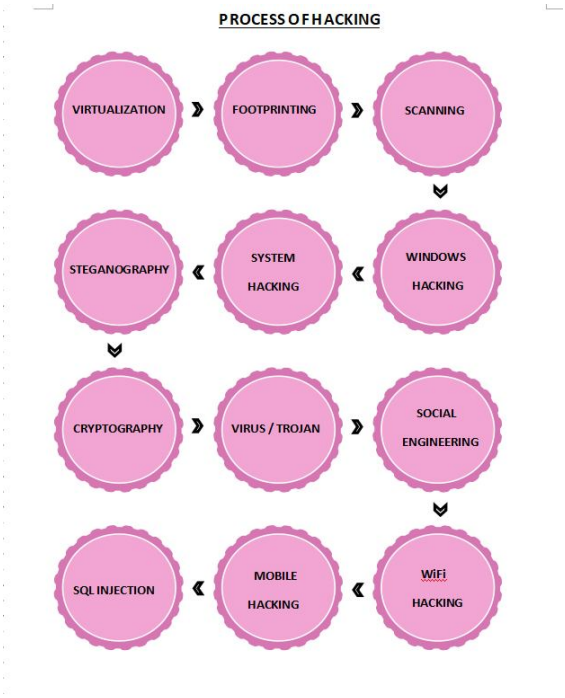
VII. ETHICAL HACKING PROCESS

WHY IS VIRTUALIZATION USEFUL?

The techniques and features that Virtual Box provides are useful for several scenarios:

- Running multiple operating systems simultaneously.
- Easier software installations.
- Testing and disaster recovery.
- Infrastructure consolidation.

FOOTPRINTING: Footprinting is the first and most convenient way that hackers use to gather information. about computer systems and the companies they belong to. The purpose of footprinting to. learn as much as you can about a system, it's remote access capabilities, its ports and. services, and the aspects of its security.



STEGANOGRAPHY: The art and science of hiding information by embedding messages within other, seemingly harmless messages. Steganography works by replacing bits of useless or unused data in regular computer files (such as graphics, sound, text, HTML, or even floppy disks) with bits of different, invisible information. This hidden information can be plain text, cipher text, or even images.

Steganography sometimes is used when encryption is not permitted. Or, more commonly, steganography is used to supplement encryption. An encrypted file may still hide information using steganography, so even if the encrypted file is deciphered, the hidden message is not seen.

TYPES OF STEGANOGRAPHY:

Steganography is of three types.They are

- Text Steganography
- Image Audio Steganography
- Video Steganography

Phishing: Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication.

VIII. CHALLENGES

As in every aspect there are some good sides and also some bad sides. So some drawbacks are also in ethical hacking:

- The person involved in ethical hacking may become dishonest towards their organization.
- They may allow the crucial details to be seen by some unauthorized persons.
- Ethical hackers may send some malicious code or virus to the system which can destroy the whole network.[5]

IX. PROSPECTS

Today software companies whether government or private is dealing with hardcore security problems. Crackers and intruders enter databases and web servers for stealing, damaging and spreading of irrelevant programs. This brings in the need of ethical hackers and courses on ethical hacking. Ethical hacking in India is grabbing the market fast and is doing a brisk business. It is the job of ethical hackers to protect the networking infrastructure and corporate websites.

X. CYBER LAW

Cyber crimes can involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation and mischief, all of which are subject to the Indian Penal Code. The abuse of computers has also given birth to a gamut of new age crimes that are addressed by the Information Technology Act, 2000.

XI. CONCLUSION

To conclude the paper I must say that the work "hacker" carries weight. Hacking may be defined as legal or illegal, ethical or unethical. As we all know that technology is growing so fast and it will continue to do so. With the technological development there are many faces of one technology.

Human mind is very powerful tool and actually has no control. Hackers will always find some way out to get into the system, irrespective of seeing good or bad intentions. It is my hope that in future hackers and ethical hackers will have different ways out for doing the things.

The ethical hackers would have an ongoing responsibility to ensure the safety of any information they retain, so in most cases all information related to the work is destroyed at the end of the contract. The idea of testing the security of a system by trying to break into it is not new. Whether an automobile company is crash-testing cars, or an individual is testing his or her skill at martial arts by sparring with a partner, evaluation by testing under attack from a real adversary is widely accepted as prudent.

Many companies are of the opinion that investing in Ethical Hacking is waste of time and money but reality is that is ignorance can cost company millions of Rupees.. Ethical hackers make sure that any of these vulnerabilities are fixed and problems plugged to protect data from fraudulent use. As the technology increases, everyone becomes machine dependent. They start saving their whole crucial data in their personal gadgets like mobile phones. But with this the fear of data loss also increases. We all know about the hackers. In layman language, the hacker is the person who enters into the system without any permission through internet and destroy system. But we have basically three groups of hackers, white, black and grey hat hacker. White hat hackers are the ethical hackers who helps the organization to protect their systems from any malicious attack. But as every coin has two sides, there are also some benefits and limitations of ethical hackers. One must use the technology as they are made for human convenience but use with precautions so that this technology will not get you into trouble.

REFERENCE

[1] Gurpreet K. Juneja," ETHICAL HACKING: A TECHNIQUE TO ENHANCE INFORMATION SECURITY",
International Journal of Innovative Research in Science, Engineering and Technology ,Vol. 2, Issue 12, December 2013.
[2] http://courses.cs.vt.edu/cs3604/lib/Hacking/notes.html
[3] "A Closer Look at Ethical Hacking and Hackers", Marilyn Leathers East Carolina University ICTN 6865
[4] http://www.brighthub.com/internet/security-privacy/articles/77412.aspx
[5] htttp:/:www.cyberlawindia.net