Future Expectation of Ethical Hacking

[1]Divyank Rastogi, [2]Ritu Saxena, [3]AviralPratap Singh,[4]Namit Gupta

[1,2,3] Student College of Computing Science and Technology, Teerthanker Mahaveer University, Moradabad-244001

[4]Assistant Prof College of Computing Science and Technology, Teerthanker Mahaveer University, Moradabad-244001

[1]06divyank06@gmail.com

[2]ritu142@gmail.com

[3]singhaviral3@gmail.com

[4]namit.k.gupta@gmail.com

***Abstract*—Hacking is a process, in which a person secretly get to know the personal information of individual or groups or confidential data or we can say breach in any confidential data or breach the security of individual or government data comes under the hacking.**
As of now, internet security is must, last year we all feel the pressure of hacking at a wide level when WannaCry and Ransomware named virus reached tomany computers and attacked and lock the computer and in order to remove the lock and giving the confidential data pack it demanded some ransom.
Also as well as after demonetization in India, scope for digital India / digital networking increase as well as the danger of cyber-attack or we can say hacking.
Now we all need protection and help to prevent such virus attack o hacking- ethical hacking combines all the features that can prevent the hacking and give us a major security goal to save us from illegal tenders. It is the process which is designed in order to find out the vulnerabilities and weakness on a computer system and network.

***Keywords*—Ethical hacking, Vulnerabilities, Hacker**

I. INTRODUCTION

As we all wanted to connect with each other either personally, professionally, globally or by the means of internet .We need to be very careful regarding what we are sharing on social and media platform as well as with others and special care and measure need to specify the information we reveal to each other But care needs to be taken about what information we reveal to others because those who intend on causing harm to you will use this information against you So it is important to protect oneself online from variety of threats online Gaining access of one's computer for obtaining information by means of breaching the security or by disclosing the personal data or by technologies or by advanced software .Hacking refers to gaining access to a computer to obtain information stored on it by means of password cracker software or any other technique to get data.
As hackers can theft or lock our information as well as in order to save our information we counter them back by the means of Ethical Hacking which can be used by various important companies and government organization as they could break into the web-server & create nuisance. To counter attack them ethical hackers are used in the Govt. organization, companies etc.

A.Hacking –A process or technique to detect the loop holes and attack on various systems and to get the various information from their servers. Hackers is the person who is continuously engaged in hacking activities

B.Ethical Hacking- A process used for securing & protecting computer. There are various computer security professionals – whose work is to evaluate the target system security or to keep an eye on all the threats that can damaged the system or steal the information.

In 1971, John Draper, aka captain crunch, was one of the best known early phone hacker, also known as Father of Hacking.
A art of exploring and finding the threats and loops is known as hacking Generally when we bear about the term "Hacking" it can be sounds with some negative shade Hacking is not about breaking security of computer and network. Programmers, who know different

computer languages very well, they themselves define as hackers, who are good at programming.

Hacking in simple words: breaking into private party in silence and enjoy it. Which logically means trying to get into some ones private account or to steal the sensitive data and do things that are illegal? Ethical hackers are the people who can create a firewall according to your knowledge and needs and protect all weak spots to protect private data from being hacked. The word hacking is not illegal, computer programmers called themselves hackers because they can break into the system and solves the problem. Example – we all knows computer system works in very library generally at universities. Every user has their id and registration number through which one can get the access of data. Some users who will be refused to gain the access would like to challenges and control the server.

Ethical hacking is also known as "Penetration Hacking" or "Intrusion Testing" or "Red Teaming". 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"

There are various techniques and policies which can be control for the security reason by each and every organisation and individual.

a) Information policy
b) Security policy
c) Computer use
d) User management
e) System administration procedures
f) Incident response procedures
g) Configuration management
h) Design methodology
i) Disaster methodology
j) Disaster recovery plans

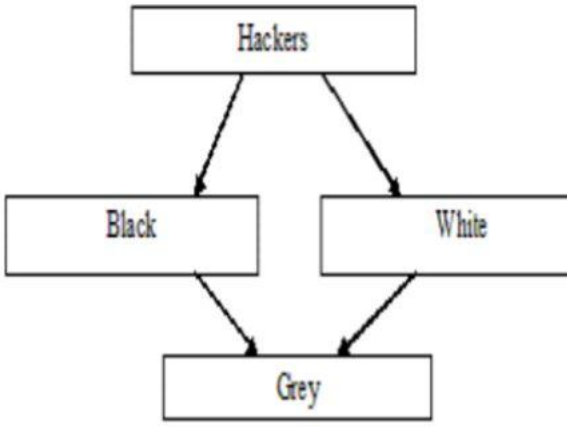
Ethical hacking, a dynamic processAreas to be tested: for the purpose are – Application servers, Firewallsecurity devices and
Various areas of security are evaluated using a ethical hacking.

II. TYPES OF HACKING

There are three types of hacking, which are as –

1. Black
2. White
3. Grey

1. ***Black Hat Hackers*** –The purpose 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
2. *White hat hackers* - authorized and paid person by the companies. 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 example – Facebook. 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.



3. *Grey hat hackers*– combines 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.

III. HISTORY OF HACKING

1939: The "bombe" became the world's first ethical hacking machine. It was used by the British to decipher encrypted German messages during WWII

1960: The Computer Penetration was first discussed by leading experts with the mention of deliberate tests by professionals.

1971: The first "Tiger-Team" was formed. USAF contracted James Anderson to test time-sharing systems.

1974: The US Air Force conducts one of the first ethical hacks to test the security of the Multics OS . 1986: The US Computer Fraud and Abuse Act makes black and grey hat hacking a criminal offense. 1995: Dan Farmer & Wietse Venema released SATAN, an automated vulnerability scanner, which becomes a popular hacking tool.

1999: Software security goes mainstream with the release of Microsoft Window's 98.

2003: OWASP releases the first OWASP testing guide to teach best practices in penetration testing 2009: PTES is founded leading to an increase in ethical hacking jobs. They offer business and security service providers a common language and scope for performing penetration testing.

2014: Worldwide security spending reaches $71.1 billion. Security executives begin to use on demand penetration testing services for cost effective ethical hacking.

Pros of ethical hacking –

i. For solving a problem we have to think like a criminal(black hat, grey hat).
ii. Helps us to create secure systems less vulnerable to external attacks.
iii. Finding the loops in the security of the systems.

Cons of ethical hacking

i. Provides a detailed analysis of what is happening.
ii. We have to secure the sensitive information
iii. A secured feeling secured even when an external attack already happening

IV. ETHICAL HACKINGPROCESS

It needs advanced planning and technologies in order to solve the problem arises. For example: - from a simple password cracking to all out penetration test on a web application. Approval of plan for ethical

hacking is essential for the process of hacking. Sponsorship of the project is the most important step for ethical hacking process because one needs someone to protect the plan, otherwise testing can be unexpectedly called off. A well define plan includes the following information:-

1. System to be tested
2. Risks that are involved
3. When the tests are performed and your overall timeline
4. how the tests are performed
5. how much knowledge of the systems you have before you start testing
6. what is done when a major threat is discovered

Characteristics in tools for ethical hacking

1. Adequate and proper documentation.
2. Detailed reports on the discovered vulnerabilities, including how they may be exploited and fixed.
3. Updates and support when needed.
4. High-level reports that can be presented to managers

These above features can save our time and effort when we execute the plan. There are two key factors – which is time and patience.

We need to be very careful while providing information because some other one can be used it against us or target us.

V. CHALLENGES AND OPPORTUNITIES

Ethical Hacking also known as Internet Security while general security is based on catching criminals similarly ethical hacking has hackers to prevent the digital crimes.

They provided several specific examples of how this information could be gathered and exploited to gain control of the target, and how such an attack could be prevented. The work of an Ethical hacker is to seeking vulnerabilities, test a security system, but reports a problem instead of taking advantage of them. Ethical hacking is also known as penetration testing, intrusion testing and red teaming.

Limitations of Ethical Hacking

1. Ethical hacking is based on the simple principle of finding the security vulnerabilities in systems 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.
2. 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.
3. 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.

VI. CONCLUSION

As we know that every coins has two side the same with the Hacking process. Hacking involves both benefit and loss or we can say both side good or bad. As we know that ethical hacker help the company and government by providing services and their knowledge while back hat hackers breach the

security or target the some important document or information. It's not a new innovation or idea to break the our system own and try to find out the loops, even generally we apply this methods to ourselves like finding mistake in our system is easy instead of finding in others and correcting it. Best method is finding our cracks, loops and solve it so that any other cannot think of breaking it.

REFERENCES

[1] Stallman, Richard.
[2] "The GNU Manifesto." The New Media Reader. Eds. Noah Wardrip-Fruin and Nick Môn fort. Cambridge: MIT Press, 2003. Sterling, Bruce.
[3] Encyclopaedia Britannica. 2003. Encyclopaedia Britannica Premium Service. 28 Oct, 2003 .
[4] Cyber Terrorism. Online. Discovery Communications. 28Oct.2003. Quittner, Jeremy.
[5] Hacker Psych 101. Online. Discovery Communications. 28Oct.2003.
[6] Hackers: Methods of Attack and Defense. Online. Discovery Communications.28Oct.2003 .
[7] Wikipedia
[8] Gurpreet K. Juneja,"Ethical hacking :A technique to enhance information security" International journal of computer applications(3297: 2007),vol. 2,Issue 12,december2013
[9] K.Bala Chowdappa et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 3389-3393
[10] Eleventh LACCEI Latin American and Caribbean Conference for Engineering and Technology (LACCEI'2013)
[11] "Innovation in Engineering, Technology and Education for Competitiveness and Prosperity" August 14 - 16, 2013 Cancun**,** Mexico. "Faculty Attitudes Toward Teaching EthicalHacking to Computer and Information Systems "Undergraduates Students Aury M. Curbelo, Ph.D,Alfredo Cruz, Ph.D.
[12] Kumar Utkarsh" SYSTEM SECURITY AND ETHICAL HACKING"