Webology (ISSN: 1735-188X)
Volume 15, Number 1, 2018

Ethical Hacking- A Technical Analysis

N.K SINGH[1] , ANURAG SINHA[2]

[1]Department of computer science , BIT Mesra.

[2]Department of computer science and IT, UG SCHOLAR Amity University Jharkhand, Ranchi, Jharkhand (India)

ABSTRACT

One of the fastest growing regions in network security and an area that generates much debate is that of ethical hacking. In today's circumstance where the communication methods have brought the world together; also have brought into being stress for the machine owners throughout the planet. The main reason supporting this insecurity is Hacking-more especially cracking the computer systems. Thus the requirement of protecting the systems in the aggravation of hacking generated by the hackers is to advertise the persons who will punch back the criminal attacks Onour computer programs, the Ethical Hackers. The primary purpose of this research is to show the short idea of this ethical hacking and its affairs with the Business security. It is part of an overall information risk management program which allows for continuing security improvements.

Claims about the safety of their goods are legitimate. Ethical hacking is the practice of analyzing the imposed threat on a particular system or network by their skills, their attitudes, and the way they go about helping their customers the ethical hacking Procedure is explained in detail. Successful ethical hackers possess an assortment of skills. First and Foremost, they have to be wholly trustworthy. Ethical Hacking is in the boom, and it's High time every provider recognizes the need of a possible professional ethical hacker. Ethical hacking isn't only necessary; it is inevitable. This paper encloses the epigrammatic disclosure about the Hacking and as well the specific role of the ethical hacking as the counter measure to cracking in accordance With the corporate security in addition to the individual refuge.

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 nour 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.

In today's world where the information communication technique has brought the world together there is one of the increase growing areas is security of network ,whichcertainly generate discussion of ETHICAL HACKING . The main reason behind the discussion of ethical hacking is in securityof the network i.e. hacking. The need of ethical hacking is to protect the system from the damage caused by the hackers. The
main reason behind the study of ethical hacking is to evaluate target system security & report back to owner. This paper helps to generate a brief idea of ethical hacking & all its aspects.

INTRODUCTION:-1

Ethical hacking also known as penetration testing, red teaming and intrusion testing is a controversial act of finding vulnerabilities and weakness of computer system by duplicating the action of malicious hackers.

An ethical hacker is also called as the white hat. White hats are security professionals who use their hacking skills to defend the information systems. Nowadays CET (certified ethical hacker) .

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 insecurity .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 hacker.

Figure1.1

Overview:-1.1

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 thatahacker with a certain amount of time and skills is or isn'table 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[1.2]

Figure1.2

ETHICAL HACKING PROCESS:-1.2

Ethical hacking needs advance planning strategic andtactical issues in the ethical hacking process should be
determined , planning is important for testing.For example: - from a simple password cracking to all outpenetration 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 forethical hacking process because one needs someone to protectthe plan , otherwise testing can be unexpectedly called off.A well define plan includes the following information:-

----- System to be tested
----- Risks that are involved
-----When the tests are performed and your overall timeline
-----how the tests are performed
-----how much knowledge of the systems you have beforeyou start testing
-----what is done when a major threat is discovered.

FEATURES OF ETHICAL HACKING:-1.3

----- E.H. has some distinct features which when comparedto security and problem scanning.
-----It is highly or completely automated.
----- E.H. typically exploits the security in order to access thedata or access another system

----- It provides security to the system and network.
----- It helps to exposes the true risk causing to the system or network.

Hacking is not what we think , It is an art of exploring the threats in a system . Today it sounds something with negative
shade , but it is not exactly that many professionals hack system so as to learn the deficiencies in them and to overcome from it and try to improve the system security. Hacking is not about breaking security of computer and network. Programmers, who know different computer languages very well, they them selvesdefine 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 them selveshackers because they can break into the system and solves the problem.

What is Ethical Hacking?-1.4

Ethical hacking is a process of finding weakness and vulnerabilities of a computer system by duplicating the action of malicious hackers. An ethical hacker works with the permissions of the companies which they are defending. The information security team are never notified about the activities that are performed by an ethical hacker for testing the capabilities of the security team. It is called "double-blind environment." To function lawfully, an ethical hacker should always be told about the laws to be protected and to what extent the company will support the hacker efforts.

What constitutes Ethical Hacking?-1.5

For hacking to be deemed ethical, the Consumer should follow the following rules:
 Expressed (frequently written) consent to probe the community and make an effort to determine possible safety risks.
 You honor the person's or business's solitude.

 You shut out your job, not leaving anything open to you or somebody else to exploit in a subsequent moment.
 You allow the software developer or hardware manufacturer understand of any safety vulnerabilities you find in their hardware or software, or even known by the business.

Ethical hacking history:-2

Internet was greatly grown since 1980's in popularity and security of computers became a major concern for government and businesses. Internet was used as an advantage and became a medium for advertising, e-commerce and information distribution. But they remained worried that their data can be hacked which may possibly lead to loss of personal and private information related to the companies, its clients, and employees.

To reduce the worry and fear of being hacked companies realized to have an effective way to computer systems of the organization. These white hats hackers would analyze the system safety and testimony about the vulnerabilities and provide the advice to remedy them rather than damaging steal information or damage the system.
For evaluation of systems security ethical hacking has been used.

To determine that a two-level classification system is needed or not United States Military carried out many early ethical hack on their OS. Network and computer vulnerabilities began to emerge outside the army organization. Dan Farmer and WietseVenema advised about techniques that are used by hackers to access the security of a system. The report they wrote was shared on the internet publicly which described how they gathered sufficient information to negotiate security, and also they provide various ways in which the information could be exploited and collected d to control a
system and how these types of attacks could be prevented.

Farmer and Venema program was named Security Analysis Tools for Auditing Networks (SATAN) which received an enormous amount of media interest because of its implications and capabilities. This tool provides advice to correct the problems in the system, and also it helped in auditing capability.

Ethical Hacking Process:-3

These steps must be followed by an ethical hacker to achieve legal and usable results:

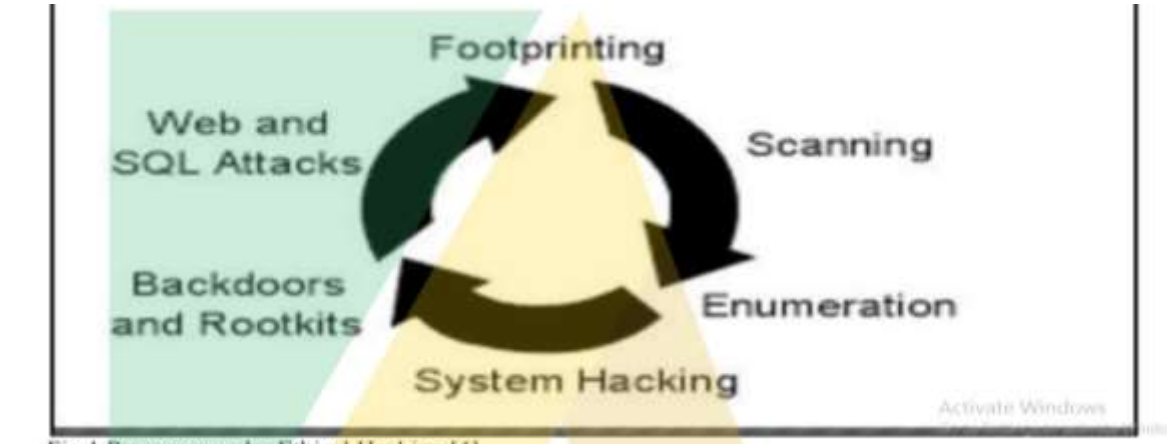


Fig.1 Processes under Ethical Hacking [4]

Figure 1.3

a) Planning

b) Reconnaissance

c) Enumeration

d) Vulnerability analysis

e) Exploitation

f) Final analysis

g) Deliverables

h) Integration

a) Planning: - For a successful project planning is an important step. Goals are to be set and allows for risk consideration to calculate how a project can be carried out. A large number of external factors are taken into consideration when an ethical hack is planned to carry out. Culture regulations and laws, security policies, and industry requirements are some of these factors. The planning phase has a deep influence on the hack to be performed and information collected andshared. It directly influences the addition and deliverable of results in the security program. This phase illustrates many of restricted attack.

b) Reconnaissance: - The freely accessible information that assists in attacking is

Reconnaissance. Social engineering, theft, tapping phones includes reconnaissance. It is a set of techniques and processes (scanning and foot printing) used to collect information of a target system secretly.

These steps must be followed during reconnaissance:-
1) Gather initial information
2) Map the network
3) Determine the network range
4) Uncover services on ports
5) Identify active machines
6) Fingerprint the operating system
7) Discover open ports and access points

This phase establishes relationship between the methods used and task to be completed to protect companies' information and belongings.

c) Enumeration: - vulnerability or network discovery is called as Enumeration. It can also be defined as an act of obtaining data gamely available from targeted networks, system and applications. This phase can be used to gain information on:-

a) Network shares
b) Passwords policies lists
c) SNMP data
d) Usernames of several systems
e) IP tables

This phase depends upon services a system offers like:-
1) DNS enumeration

2) SMB enumeration

3) NTP enumeration
4) Linux/Windows enumeration
5) SNMP enumeration
Several techniques and tools are available to draw an image of an organization Environment. It includes NMap and port scanning. Determining the value of data is also difficult. In this phase, logical conclusion plays a massive role in examining the hacker's capability.

d) Vulnerability analysis: - To successfully examine information, an ethical hacker makes useof a practical and logical strategy. From vulnerability analysis period, the accumulated material is contrasted with identified susceptibility in a sensible procedure. Information is of use regardless of what the resource is. Any tiny spot may help in finding options for manipulation and might potentially guide to discoveries which are to be discovered. Susceptibilities, events, service packs, upgrades, and even available hacker tools which are well
known can assist in finding ways of incursion. Quantities of information which may readily be connected with the structure and weak and strong points of an individual system could be found online.

e) Exploitation: - A substantial time period is spent assessed on ethical hacking which leads to enormous amounts of incursions. Such methods can easily be manipulated or can be as lethal and
complicated as a set of multiple measures that have to be implemented in specific manner to be able to obtain access. The manipulation procedure is divided into various steps which could lead to several measures or
a particular measure in initializing the assault. With each progressive step, an appraisal will make sure the anticipated result is achieved.

f) Final Analysis: - Even though the bleeding aspect has numerous tests and authorizations to guarantee success, it must categorize the susceptibilities of this machine concerning their degree of vulnerability and also to aid in the deduction of a reduction program. The terminal evaluation phase furnishes a connection between the profiteering stage and also the realization.

A detailed view attack must be provided to build a larger image of their safety from surroundings and also explain the susceptibilities in a very clear and useful way. The last evaluation is a part analysis and component factual outcomes.

g) Deliverables: - They convey the results of evaluations in a lot of ways. Some of these are brief and succinct, only supplying a listing of susceptibilities and ways to repair them, while some are lengthy and comprehensive, offering a listing of susceptibilities withorough explanations about the way they were discovered, the way to utilize them, the consequences of
having this kind susceptibility and the way to fix the circumstance.
This period is a means for an ethical hacker to communicate the outcome of the evaluations. Lately, ethical hacking became so commoditized even when a output doesn't inculcate terror in the hearts of administrators, then it can be considered as a letdown.

h) Integration: - Ultimately, it is important that there are certain resources of employing the evaluation outcomes for somewhat effective. Many times, the deliverables are coupled with prevailing substances, like hazard exploration, security coverage, earlier evaluation results, and data connected with a safety platform to boost reduction and progress treatments and spots for weaknesses.
These factors should be taken into consideration throughout the addition of any evaluation outcomes: Mitigation: In case exposure conventional risk is found then it should be secured. Mitigation of susceptibilities may incorporate analysis, testing, applying, and supporting modifications to
methods.

Defense: Susceptibilities should be dealt with strategies to diminish potential or unidentified weaknesses. Defense preparation is building a base of safety to develop and guarantee long lasting victory. Incident Management: Attacks that are done and the effects it will cause on the system assist in inventing and case response program. The hacking procedure offers opportunity for finding the numerous susceptibilities of attack on a system which could help in lessen the future attacks.

Commandments of Ethical Hacking:-3.1

Ten Commandments of Ethical Hacking are important to understand to become a believer in the philosophy of Ethical Hacking that are:-

a) You should set your goals- An Ethical hacker ought to establish easy goals, likediscovering illegal wireless access points or acquiring data from a wired networkplatform. Whatever the instance, the aims must be articulate and well communicated.

b) You should plan the work, and not to go off the path- Limitations bind ethical hackers. As a result, it's imperative to come up with a strategic plan that ought to consist ofrecognizing the networks to check, specifying the testing period, defining the testingprocedure, and getting an approval of this strategy.

c) You should ensure permission- Inscribed permission is necessary and should state anethical hacker is official to do a test in line with the policy. It also needs to say that thecompany will offer organizational and permissible provision if criminal charges or suitsarises. That is conditional on remaining within the boundaries of the accepted program.

d) You should work ethically- An ethical hacker is particular to secrecy and non-disclosureof advice they may discover. Ethical hackers also have to be obedient with their company's government and local laws. An ethical hack should not be performed whilethe corporation program or the law for that thing openly prohibits it.

e) You should preserve archives- Patience and carefulness are characteristics of a fantastic ethical hacker. A trademark of moral hacker efficiency is maintaining sufficient archivesto support customs. The date and information about each evaluation, whether they hadbeen powerful, should be listed and noted and a duplicate of this record book ought to bekept.

f) Privacy of people should be respected by you- Authority must not be abused by an ethical hacker. Ethical hackers should sneak into private company documents or personal lives.The info that's discovered ought to be treated carefully as of the private details.

g) No injury should be done by you- The activities of an ethical hacker might have unintentional consequences. It is easy to become trapped in the job and create a rejection of provision or flatten on somebody else's rights. Abiding by the original strategy is necessary.

h) Scientific ways should be used by you- The work of an ethical hacker must embrace an experimental procedure. A practical method can help establish computable objectives, acquire dependable and repeatable evaluations and supply evaluations that are legitimate in the forthcoming.

i) You should not crave neighbor’s apparatuses - Ethical hackers will constantly find new resources to support them get their occupation done. Apparatuses are plentiful online, and much further are approaching out all of the period. The desire to catch them all is ferocious. Even though it's possible to utilize each the tools which are obtainable, it's advised that an ethical hacker picks single and stay by it.

j) You should address all your data - Ethical hackers must aim to report any insecure susceptibilities found throughout analysis whenever they are found. Reports are just some way for the business to ascertain the extensiveness and carefulness of the job of an ethical hacker and offer a way for dukes to critique procedures, conclusions, diagnosis, plus decisions.

Required skills to become an Ethical Hacker :-3.2

An ethical hacker is needed to have a large planning of computer abilities. It is impossible for every ethical hacker to become a professional in each area and so tiger teams of hackers whoassociate possess accompanying skills are produced to give an association with a staff owning the whole skill set needed of an ethical hacker.

Establishments might have a vast array of computer structures, and it's crucial for almost any principled hacker to possess experience in effective systems, in addition network hardware platforms. Additionally, it is important that a hacker possesses a good base of the essentials of information security.

Certification:-3.3

On account of the argument adjoining the livelihood of hacking, the International Council of ECommerce Consultants (EC-Council) offers a specialist certification for CEH. A CEH is an ethical hacker that has got the certificate supplied via EC-Council.

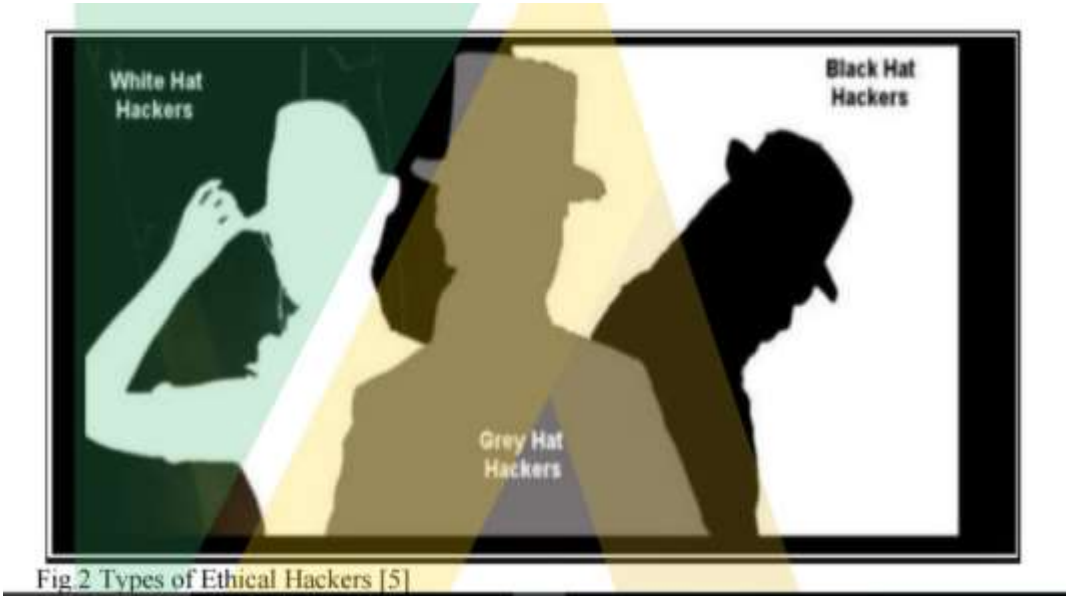


Fig.2 Types of Ethical Hackers [5]

Figure 1.3

To receive authorization, a licensed hacker has to complete a assignments comprising twenty two modules, which vary from thirty minutes to five hours or longer, based proceeding the thickness
of the data provided.
These modules are:

1. Scanning
2. Foot printing
3. Legality
4. Enumeration
5. Web Application Susceptibilities
6. Trojans & Backdoors
7. Sniffers
8. Denial of Service
9. Social Engineering
10. Session Hacking
11. Hacking Web Servers
12. System hacking
13. Hacking Wireless Cracking
14. Viruses
15. Web-based password cracking
16. SQL Injection
17. Cryptography
18. Pen Test Methodologies
19. Physical Security
20. Linux Hacking
21. Evading Intrusion Detection System
22. Buffer Overflow

A. White Hat Hackers

White Hat Hackers are authorized and paid person by thecompanies, with good intends and moral standing. They arealso known as "IT Technicians". Their job is to safeguard Internet, businesses, computer networks and systems fromcrackers. Some companies pay IT professionals to attemptto 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. Thewhite Hat Hacker is also called as an Ethical Hacker. contrast to White Hat Hackers.

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.

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 theremedy. 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, andmay 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. Whilehacking a system, irrespective of ethical hacking (white hathacking) or malicious hacking (black hat hacking), the hacker has to follow some steps to enter into a computersystem, which can be discussed as follow.

ETHICAL HACKING PHASES:-4

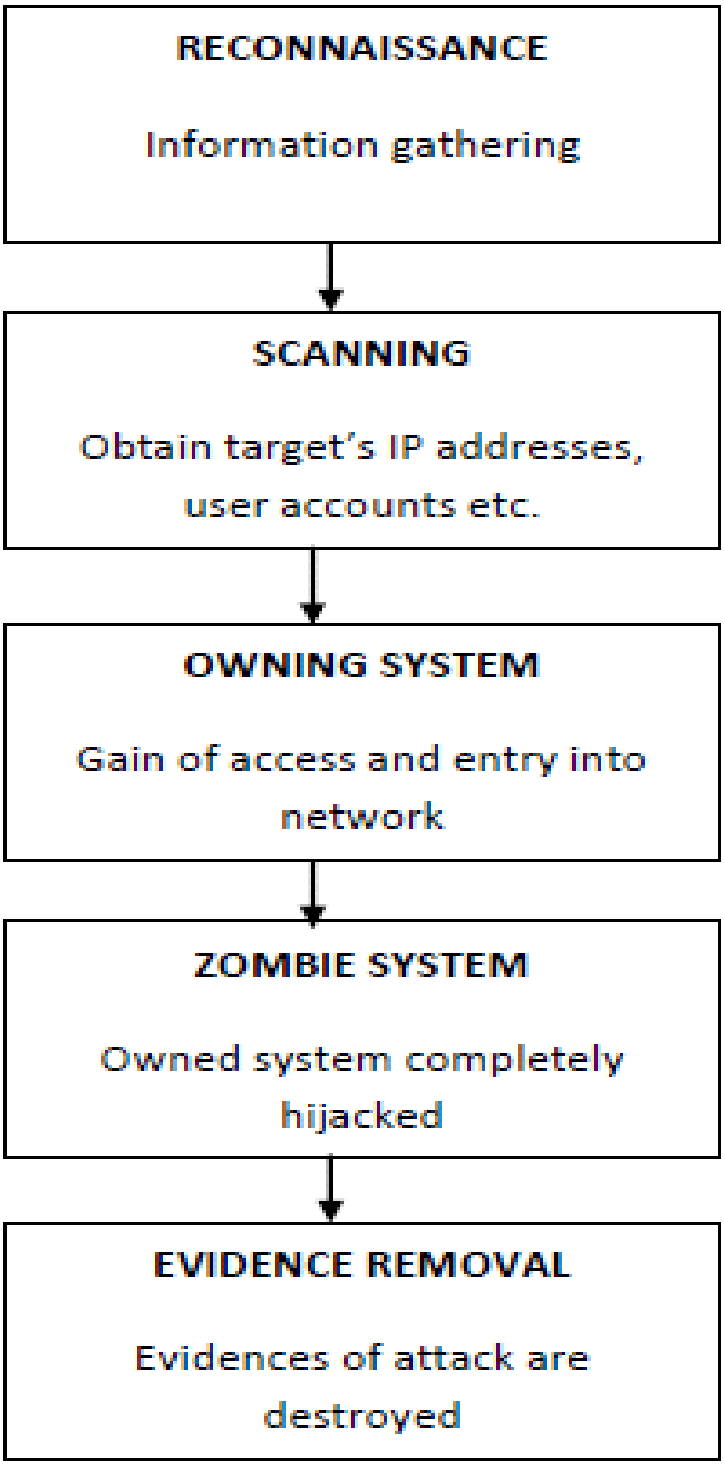
Hacking Can Be Done By Following These Five Phases:

Phase 1: **Reconnaissance**: can be active or passive: inpassive reconnaissance the information is gatheredregarding the target without knowledge of targetedcompany (or individual). It could be done simply bysearching information of the target on internet or bribing an employee of targeted company who would reveal andprovide useful information to the hacker.

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 activereconnaissance, the hacker enters into the network to discover individual hosts, ip addresses and network services. Thisprocess is also called as “rattling the doorknobs”. In thismethod, there is a high risk of being caught as compared topassive 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


RECONNAISSANCE
Information gathering
SCANNING
Obtain target's IP addresses, user accounts etc.
OWNING SYSTEM
Gain of access and entry into network
ZOMBIE SYSTEM
Owned system completely hijacked
EVIDENCE REMOVAL
Evidences of attack are destroyed

.

FIGURE 1.4

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]

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 here in .By using this information you agree that Scan Alert shall beheld harmless in any event.

Benefits of Ethical Hacking-4.1

• This type of “test” can provide convincing evidenceof real system or network level threat exposuresthrough proof of access. Even though these findingsmay be somewhat negative, by identifying anyexposure you can be proactive in improving the overall security of your systems.

• However, information security should not be strictlylimited to the mechanics of hardening networks andcomputer systems. A mature security informationprogram is a combination of policies, procedures,technical system and network standards,configuration settings,

monitoring, and auditingpractices. Business systems, which have resist simple, direct attacks at the operating system or
network level, may succumb to attacks that exploit aseries 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.

Limitations of Ethical Hacking-4.2

• Ethical hacking is based on the simple principle ofthe security vulnerabilities in systems andnetworks before the hackers do, by using so-called"hacker" techniques to gain this knowledge.

Unfortunately, the common definitions of suchtesting usually stops at the operating systems,security settings, and "bugs" level. Limiting theexercise to the technical level by performing a seriesof purely technical tests, an ethical hacking exercise
is no better than a limited "diagnostic" of a system'ssecurity.

• 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 youwill 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" t CONDUCT you tests, you will be providing "inside information" in order to speed the process and savetime. 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 limitedvalue, because all vulnerabilities may not be sure.

CONCLUSION:-5

Hackers thus have an essential function to play in modern society since they cut down the danger of malicious attacks on computers using the exact same practices that are used by crackers. Although you might not be a computer hacker, I am certain you know the sort of destructive activities, these people are involved in. There will be a number of unique approaches taken much
like a true hacker would utilize. Certified Ethical Hackers are a smart investment for virtually any companyseeking to upgrade and for their on-line security measures. For people who are technically restrained or financially incapable of employing a professional ethical hacker, step one is recommended since it is very easy to carry out.The web has given us a typical platform and medium through which we can explore different
cultures and ideologies.

It has become an essential propagator of knowledge, both through free as
well as paid services. Internet, undoubtedly, gives you a simple and quick access to the information that you require. It serves as one of the most efficient means of communication. The World Wide Web has been mankind's best means of communication yet. It's frequently utilized to refer to the World Wide Web.

Hacking has both its benefits and risks. Hackersare very diverse. They may bankrupt a company or mayprotect 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 noend. While ethical hackers help to understand thecompanies’ their security needs, the malicious hackersintrudes illegally and harm the network for their personal benefits.

RESULTS AND DISCUSSIONS:-5.1

You can't fight hackers should you don't know the method by which they work. Whether you are aware of it or not, if you're a hacker, you're a revolutionary. Most hackers appear

to find pranks and practical jokes as harmless, no matter their psychological effect. While working on an undertaking, the ethical hacker may encounter some valuable information concerning the user or the business. He is vital to have a large preparation of computer abilities.

Administrations would love to practice the web to their benefit by using the World Wide Web as a intermediate for info distribution, e-commerce, and other accomplishments. Any organization with a network on the net or supplies an online service should think about subjecting it to a penetration test. Some various organizations store personal particulars and different vital information of their users. Planning is important for having a thriving project. The advance of the system evaluation includes the next parts. Moreover, the procedure is hard.
Sometimes, you might need to monitor the system for days or weeks to have a single chance to crack it.

Complete anonymity isn't the intent of online privacy. Privacy of the customer's information is the most prevalent issue in the area of ethical hacking. Computer security has become a significant concern on the planet today. You're going to be able to assess the system's security like its present under normal problems.

Network administrators in companies want to monitor visitors to their server, including tracking the online use by employees. Some users prefer anonymity while using the net. Most are possessive over the usage of their very own personal computer. All information needs to be free. In this respect, people intending to use details must identify themselves through the useof login info. As said above, information found on the web is extremely helpful.

REFERENCES

1) www.tutorialspoint.com
2) Book - Ethical Hacking by C.C Palmer
3) Book – Hacking for Dummies by Kevin Beaver
4) http://www.knowthetrade.com/ethical-hacking (fig.1)
5)
https://www.tutorialspoint.com/penetration_testing/penetration_testing_ethical_hacking.(fig.2)