Grenze International Journal of Engineering and Technology, Jan Issue

Research on Ethical Hacking

Yash Singh[1], Harshi Adamya[2], Aryan[3], Sanidhya[4] and Sayyad[5]
[1]Computer Science Engineering, Chandigarh University, Mohali, India
Email: yashs3326@gmail.com
[2-5]Chandigarh University, Mohali, India
Email: adamyaaksh123@gmail.com ,aryan08012003@gmail.com ,sanidhya.sharma720@gmail.com
sayyadshahi2712@gmail.com

***Abstract*—Hacking is defined as the process of exploiting the sensitive and valuable information of any system, group, or any organization which may even lead to leak of any confidential information or data. Deriving from the concept of hacking, ethical hacking is a kind of hacking meant for societal benefit, for helping governmental organizations, or may even help the organizations to test and analyze its security. Which in turn, helps an individual or an organization to counter any security threats or vulnerabilities. Ethical hacking is one of the most important modern-day techniques to keep our privacy in check. The aim of this paper is to find out the process involved in ethical hacking and penetration testing in network security, with a view to exploring whether ethical hacking can be applied to the field of cyber-security.**

***Index Terms*— ethical hacking, cyber security, penetration testing, hackers, phases of hacking and white hat hackers.**

I. INTRODUCTION

With the advent of a new technical era, cyber-crime is a frequent affair. Hackers are getting successful in exploring the loopholes of any system and thus, exploit it. And here the role of ethical hackers comes into picture. Ethical hackers are professionals who use the same methodology and techniques used by hackers to explore security threats and vulnerabilities in systems. Once this process is complete, the security team gives the detailed report to the clients with the threats they identified and instructions on how to counter such loopholes in the security. As the name suggests, ethical hacking is the process of analyzing the loopholes of any system, trying to figure out its vulnerabilities, flaws and security weaknesses with a good motive. It is intended to explore the security mechanism of any system and then prepare a report on the vulnerabilities examined and finally, give suggestions to the organizations on how to handle the security threats.

It not only helps an organization prosper but also helps it in retaining its name and fame among its customers. It also helps the Government in preventing any threat of data in terms of data piracy or security breaches which may directly or indirectly affect our country. In today's scenario, every data is available online, if not safeguarded efficiently may lead to threat to confidential and sensitive information, which might be very important for the country or the organization.

Suppose your ATM's pin is known to any person without your knowledge, it may lead to financial loss as the person would be in power to withdraw money without your knowledge. This is a small example of breach of confidentiality. Likewise, there is a lot of sensitive data which needs to be managed properly for smooth running of any organization, group or country.

Grenze ID: 01.GIJET.9.1.512_1

II. LITERATURE REVIEW

U. Murugavel and Dr. Shanthi, published how ethical hackers apply their knowledge and network skills to find out the security flaws of any system at client side and make the customer aware of it and secure the system. Penetration testing is more relevant to identify the security flaws that might have crept into the system. It prevents data theft, financial loss and farsighted elimination of identified threats. Implementation of penetration testing through regular auditing, threat and flaws detection and a smooth system administration can safeguard confidential data and valuable information from hackers. It is a cost-effective security measure which may be adapted by an organization or individual to avoid any data threat.

Ahmad Mtair et al (2020), reviewed the importance of cybersecurity and the ethical use of hacking techniques to protect user data. Organizations can prevent cyber threats and protect the security of user data by implementing basic security mechanisms for packet filtering, intrusion detection, authentication systems, maintain and update operating systems and business platforms, and encrypt data. All of these will ensure the security and integrity of the data.

Shivanshi and Dr. Yojna, described ethical hacking as a Lifeguard technique as it works as a life saver for the victims of hacking, they discussed about different type of hacking and Hackers. The paper explains the difference between hacking and ethical hacking, the duty of ethical hackers (white hat hackers) is to make the hackers fail in their bad intentions.

Idimadakala Nagaraju published the ethics behind the ethical hacking and the complication with the ethical hacking. As this technology has emerged at a high rate and is continuously growing and scholars have put themselves in unsafe positions by helping independently to hack. Hackers will always be figuring out methods to hack into the system, whether their intention is good or not.

K. Bala Chowdappa, S. Subba Lakshmi, P.N.V.S. Pavan Kumar published about the Network Penetration Testing, which is one of the skills used in ethical hacking and discussed about the Security Life Cycle, the dark side of hacking and the views of citizens and media. They described the benefits and risks of hacking. Some hacker's intentions have been bad like bankrupting a company and some have been working hard to protect the data. And the never-ending war has been going on between ethical hackers and malicious hackers.

Jean-Paul A. Yaacoub et al suggested that a new kind of modern penetration testing system should be introduced through the cooperation between different security factors and penetration tests. According to them a semi-automatic approach for ethical hacking and penetration testing is must to ensure the security.

Petar Cisara, Robert Pinterb published a summary of the Kali attack on the client and server side and highlights its importance. They discussed the benefits of this operating system like having a large library of hacking tools in a single place. Kali sticks to the FHS (File-system Hierarchy Standard) and facilitates vulnerability assessment and security testing through various tools which are essential for ethical hacking.

Ms. Vaishnavi Bhagwat Savant, Ms. Rupali D. Kasar, Ms. Priti B. Savant, published the overview of hacking, its types, and concept behind ethical hacking. It has explained the detailed procedure behind ethical hacking, its advantages and disadvantages. It enlists the role of ethical hacking in curbing down the rate of cyber-crime.

Dr Amarendra K, Venkata Naresh Mandhala, SaiSri Damecharla, Praveen Gollapudi, Pavan Kumar Ponuganti, published how important it is for all to learn the general idea of hacking while we work on any system or network. This would help the users take measures to prevent their systems from being hacked. It explained how the hacking is done, general idea behind types of hackers, meaning of ethical hacking, process of ethical hacking and finally the preventive measures to overcome any vulnerabilities of the system.

Bhawana Sahare, Ankit Naik, Shashikala Khandey published that there has been weak security on the internet and as all the work has been digital and stored online which increases opportunities for the criminal and to gain access to the sensitive information. To protect it, ethical hackers find various ways which help governments, businesses as well as citizens. They have also talked about the benefits and risks of hacking and due to ethical hacking, we have been able to maintain and protect a lot of sensitive information from malicious hackers who could destroy everything.

Prachi Arora, Mishita Poojary and Ishita Pate published that the white hacker's job has been to protect our system as much as possible and block other hackers. Even though the white hat hacker has the same skills, skills and tools as the black hat hacker, the attack has been non-destructive. Society should have understood the difference between hackers. This modern need has to understand the difference and appreciate the work of white hackers.

C. Nagarani published that public and private organizations are moving to the internet, so there has been risk of illegal attacks and to protect it we have ethical hackers or white hat hackers. The publisher has described ethical hacking and the value of security very briefly and also addressed ethical hacking from several points of views.

Many techniques and ideas have been implemented for testing the security to improve it. And ethical hacking might be the most effective way to prevent cyber-crimes.

Meenaakshi N. Munjal described that there are some fields in computing where hackers mark their impact on society. In this paper I have tried to look in depth of different ways that how we can make ethical hacking a safe and more and more ethical. Hacking may be defined as legal or illegal. Since we know that the technology is growing so rapidly and with the overall technological advancement there are also many sides of one technology. We need to work on our security making it difficult for hackers to mark any bad impact on our society.

Sarah Delasko and Weifeng Chen published that why and what makes hackers to use Linux over any Windows and Mac OS software Linux is the most preferable OS for hackers, mainly because of its easy and easily available marketing system, compatibility of various hacking tool and terminals along with the repository with a classic hacking tool themes or an interface. Other choices for hackers are Parrot Security OS, Samurai. By learning and practicing the various methods behind cyber warfare, cyber security specialists or analysts can use preventative steps to increase network safety and security against malicious attacks.

Miss. Pratibha Prakash Jumale examined that Hacking together has its own benefits and risks. Hackers may break an organization or may safeguard their data, legal hacking shows a major role in maintaining and securing a lot of sensitive data and information, whereas illegal hacking can harm everything related to data security in some cases downfall of organizations and corporations.

Vivek Shrivastava Monika Pangaria concluded the different aspects of hacking. It is important for all to learn and understand the different methods and steps of ethical hacking to avoid hacking and prevent themselves from its malicious effects. For this purpose, only, they have to find loopholes in a system in order to keep it safe.

Aman Gupta and Abhineet Anand suggested hacking, hackers and a brief about ethical hackers. They described how some people do hacking for good and some use this skill for destruction. They have also discussed types of hacking attacks. The malicious hackers try to find new ways to break into the network so there is need for ethical hackers and when ethical hacking is done in a proper way then it will be easy to protect the data from these malicious hackers.

Prabhat Kumar Sahu and Biswamohan Acharya published that all the businesses and jobs have moved digitally, and some are still moving, so they all search for ethical hackers to protect the data and increase security so that a malicious hacker would not be able to exploit the data. As new technology has its own advantages and disadvantages. The data should be monitored and as well as security should be made strong and a single mistake can lead to loss of data and revenue as well as fame. So, in order to avoid it, there is a need for ethical hackers.

Danish Jamil and Muhammad Numan Ali Khan published about the problem faced during ethical hacking and the intention of the ethical hackers. And there should be research which could help with ethical hacking. They have gathered a lot of information regarding ethical hacking and issues faced so we all should look into it. As technology keeps growing and hackers with bad intentions are coming in a different way, we also teach about ethical hacking to protect ourselves from these attacks.

Vinitha K.P. described the sudden growth of the Internet which has good outcomes like Emails, Banking, etc. and some bad outcomes like Malicious Hacking, etc. Malicious hacking is the biggest problem for everyone whether it is the government, citizens and companies. Hacking can lead to stolen credit card details, exposing someone on public platforms and many more. The author has discussed the ethical hacker, their skills and how they use their skills to help these citizens or companies. Ethical hackers secure the data in a legal method and they have the same skills as malicious hackers but they use their skill to help unlike malicious hackers who use their skills in a destructive manner.

III. Ethical Hacking

Ethical Hacking is defined as the systematic process of finding out the vulnerabilities in the system of any company, organization or individual. It enhances the security which ultimately hinders attackers from exploiting the system. Ethical hackers are called “White-Hat Hackers”. It is a part of Cybersecurity, as it is done with the permission of the client for a great cause. With the permission of the client, ethical hackers interfere with the system, exploit it, identify the vulnerabilities and loopholes in it. They find out all the weaknesses which could be targeted by the attackers. Ethical hacking is a measure undertaken by any company, individual or organization to make its security unbreachable and secure. It involves thinking like a cracker and trying to find out all the vulnerabilities that could be targeted by the attackers and thus eradicating those weaknesses, making the system more secure. It is our misconception that hacking and ethical hacking are the same. Although Ethical Hacking is very much similar to traditional hacking, the only difference between them is their purpose and the objective.

IV. Types of Hackers

Hacking and hackers can be categorized into three main categories based on their intentions. These are named on the color of “hats”. The term hat is taken from vintage game concepts where heroes wear white caps and villains wear black ones. So, the brighter the color of the hat the less intention to harm someone.

A. Black Hat Hackers

or The Criminal Hackers. They are the cyber criminals who breach into a system for pure evil intentions. Black hat hackers are the ones who you probably picture when you think of a hacker. They exploit or breach a system for financial gains or other malicious purposes. They can do serious harm to an organization, individual and sometimes even the government by stealing the sensitive data. Their One and only motive is to profit from the breaches.

B. White Hat Hackers

They are the ones hired by the organizations in order to keep their system security in check. They use their skills to find vulnerability on the network and computer system of the organization. So, they are the ones with good intentions and hack the system in order to find the vulnerability and secure it from future attacks.

C. Grey Hat Hackers

Also sometimes referred to as “just for fun” hackers. As the name suggests they are the Intersection of black hat and white hat hackers. They breach an organization's system just for fun and they might even let the owner know about the weaknesses found in the system during their attacks. So, they are the hackers with mixed intentions and all they want to do is test out the hacking skills they learned without taking proper permissions (even though their true intention is not to harm the system).

Apart from these three main categories there are numerous other types of hackers known as miscellaneous hackers like script kiddies (amateur hackers), Green hat hacker (hacker in training), Red hat hacker (Govt. Hired hacker), Blue hat Hacker (authorized software hackers) etc.

V. Phases of Hacking / Ethical Hacking

A. Reconnaisance

Also Known as the foot printing or information gathering phase, it is the very first step while hacking in which a hacker tries to collect various information like IP addresses, TCP and UDP services, vulnerabilities etc., of the system they have to hack. They gather this information using several different tools such as search engines (e.g., Malte go) or HTTP trackers etc.

B. Scanning

In this phase hackers try to gather information that can help them to penetrate into the system such as computer names, user accounts, specific IP addresses etc., using tools like dialers, network mappers, port scanners, sweepers etc. The four main types of scans used in this phase are: pre attack, port scanning/sniffing, vulnerability scanning & information extraction.

C. Gaining Access

Till this point hackers have already collected all the required information, so in this phase they try to decide and carry out the attack to gain access. There are many types of attacks to choose from like phishing, Man in the middle, Brute force, Dos (denial of service), session hijacking etc.

D. Maintainig Access

Now once hackers have breached into a system, they need to maintain the access in order to collect the data or exploitable data in the future so that they don't have to perform previous steps again. Certain access maintaining files, Rootkits and trojans can be used for this purpose.

E. Clearing Tracks

After the work is done, a smart hacker always clears the tracks so that he can't be traced back in the future. They do this by: clearing cache and cookies, corrupting or deleting the values of logs, closing all the open ports etc.

It is not necessary for the hackers to follow these five steps approach every time or sequentially. However, proceeding in this way can lead to more accurate hacking.

VI. Skills Required For Hacking / Ethical Hacking

A. Understanding of operating system

So, the first point is that we have knowledge of the operating system. We are not going to work on windows. So the question that arises here is where we are going to work in ethical hacking. The most common operating system is LINUX. A candidate should have a solid understanding of Linux. Linux is used by many web servers. There are many more operating systems we have, like Ubuntu, Parrot OS, etc. To check for cyber security breaches and defects, one should be familiar with operating systems such as Linux, Ubuntu, Red Hat, and others.

B. Computer and Networking Skills

A pioneering hacker must have a deep and thorough understanding of computers and networks. Hacking is basically known for exploiting computer systems and networks. So, the aspirants have highly practiced computer and networking skills. They should also know how to use networking commands such as the OSI model, IP or MAC addresses, subnetting, and routing to enable ethical hacking.

C. Understanding in Coding Skills

You will undoubtedly excel in the ethical hacking field if you have strong coding skills. Because many websites and applications employ coding, analyzing codes can help you start a career in ethical hacking. So, knowing different programming languages, such as Python, Java, JavaScript, C++, and C, allows hackers to spot harmful code or flaws in the code.

D. Cryptography Skills

As an ethical hacker, it is our obligation to ensure that communication between various members of the organization is sent and received without affecting the privacy of the users. Cryptography is the technique of transforming or encoding text messages into an un understandable format so that hackers won't be able to read them even if they are exploited.

VII. Tools Required For Hacking / Ethical Hacking

A. NMAP

It is also known as Network Mapper. It is a free and easily available tool used extensively for the detection of networks and for testing security. It was designed to scan networks that are larger, and can perform equally well for a single host. Network administrators use NMAP in tasks like network assets, service management and development schedules, etc.
It makes use of raw IP packets to find out the following things:

- strangers in the network,
- The services that they perform,
- Apps used by them,
- The firewall they are using.

B. Metasploit

It is one of the greatest exploitation tools. It is available in two versions, first a version that is being used commercially and one needs to pay in order to use it, and a free to use version. It can also be executed from a command prompt or with a Web UI. With Metasploit, you can do the following activities -

- Perform simple login check or tests on smaller networks
- Test risk usability
- Find a network or import scanning data
- Browse exploit modules and use each exploit for strangers

C. Burp Suite

It is a famous platform and is widely used to perform security check or tests for web applications. It is loaded with the variety of tools that together works to support the whole process of testing, from the initial design to the detection and use of security risks. It can be easily used and gives full control to administrators for integrating advance manual methods and automation for better testing. Burp can configure easily and has features to help experienced inspectors.

D. Angry IP Scanner

It is capable of scanning different IP addresses of any range. It can be used anywhere and freely. This tool simply scans each IP address to find out whether or not the address is alive, and then, the data collected about each and every host can be saved in .TXT, .XML, .CSV, or an IP-Port files. Using plugins, Angry IP Scanner is able to collect information about scanned IPs.

VIII. Benefits of Ethical Hacking

Cybercrime is one of the international conflicts increasing from time to time. There are hackers who are determined to exploit any system of any organization, individual or any government organization. There are many terrorist organizations that give malicious hackers a lot of money so that they could promote terrorism, exploit national security and many more crimes. So, we need ethical hackers a lot so that they can defend us from cyber-attacks.

Ethical hackers keep on searching for vulnerabilities in the network structure in order to protect the data from malicious hackers as they can steal it and it can be misused. They use a fuzzing tool to enter in our code to crash it, as it will reveal if there is any issue in the security and then they will fix it.

Sometimes security threats and vulnerabilities can be far away from the data network structure so ethical hackers keep testing on their data to improve the security.

We can improve the network structure by taking the help of ethical hackers who find out the weakness in the system. It will help all types of organizations, whether it is private or government sector, to build their network structure stronger by using firewalls, shielding network ports, and finding weakness and upgrading to the latest network security.

Ethical Hackers will protect us from cyber-attacks by informing us about the threat and enable the security to protect our data. As cyber-attacks can make us bankrupt and even defame us. So ethical hacking is very beneficial in this digital world.

IX. Limitations of Ethical Hacking

Ethical hackers have limitations to the tools and it depends on which organization they are working.as they have to take the permission of the owner or manager of the organization when they are using the tool.

Network security also depends on how experienced the ethical hacker is, if the hacker is inexperienced then he/she will be unable to find the security vulnerabilities as much as an experienced hacker can find. As a more experienced hacker can find a lot of weaknesses in the system which protect the data to exploit.

For small organizations, who have limited resources, it is difficult to hire ethical hackers as they demand a high amount of money.

X. Conclusions

This paper discussed ethical hacking from various points of views. Hacking has its own benefits and risks. There are various hackers, the ones who do hacking for good purpose are ethical hackers or white hat hackers and ones who have bad intentions are malicious hackers or black hat hackers. The war between hackers has been going on from the start and it seems endless. Our security system is poor, but ethical hackers do their best to protect. I think everyone should be aware of ethical hacking in order to be protected from malicious hackers. Hacking is very essential in the computer world and ethical hackers help to protect a lot of data. Overall, it depends on the intention of hackers which makes them good or bad. Hackers will always try to get into our data so we should also make our security stronger.

References

[1] Murugavel U. and Dr. Shanthi (2014), "Survey on Ethical Hacking Process in Network Security", International Journal of Engineering Sciences & Research Technology [836-839]

[2] M Ahmad and Hawamleh AL (2020.), "Cyber Security and Ethical Hacking: The Importance of Protecting User Data". Solid State Technology Vol. 63.

[3] Shivanshi Sinha and Dr. Yojna Arora (2020), "Ethical Hacking: The Story of a White Hat Hacker", JIRCST, Vol. 8.

[4] Nagaraju I. (2013), "ETHICS IN ETHICAL HACKING", International Journal of Scientific & Engineering Research, Vol. 4, pp 1592-1597.

[5] Bala Chowdappa K., Subba Lakshmi S., Kumar S.Pavan (2014) , "Ethical Hacking Techniques with Penetration Testing", IJCSIT Vol.5(3) , pp 3389-3393

[6] Paul J, Yaacoub A., Hassan N., O Salman, Ali Chehab, (2021) “A SURVEY ON ETHICAL HACKING: ISSUES AND CHALLENGES”,
[7] Petar Cisara, Robert Pinterb (2019), “Some ethical hacking possibilities in Kali Linux environment”, JATES vol.9 no.4, pp 129-149.
[8] Ms. Vaishnavi Bhagwat Savant, Ms. Rupali D. Kasar and Ms. Priti B. Savant, "A review on overview of Ethical Hacking", International Journal of Engineering Applied Sciences and Technology, Vol.6, pp379-383.
[9] Dr Amarendra K, Venkata Naresh Mandhala, SaiSri Damecharla, Praveen Gollapudi and Pavan Kumar Ponuganti (2019), "Modern Era Hacking", IJSTR Vol.8, pp 920-922.
[10] Bhawana Sahare, Ankit Naik and Shashikala Khandey (2014), “Study of Ethical Hacking”, IJCST vol.2 (4), pp 6-10.
[11] Prachi Arora, Mishita Poojary and Ishita Patel (2021), “A Review Paper on White Hat Hackers”, IJARCST vol.12 issue 1, pp 282-287.
[12] [12] C. Nagarani (2015), “Ethical Hacking and Its Value to Security”, GJRA vol.4, pp 163-164.
[13] N. Munjal Meenaakshi (2014), “ETHICAL HACKING: AN IMPACT ON SOCIETY”, Cyber Times International Journal of Technology & Management vol.7, pp 922-931.
[14] Sarah Delasko and Weifeng Chen, “Operating Systems of Choice for Professional Hackers”, International Conference on Cyber Warfare & Security
[15] Pratibha P. Jumale (2019), “Impact of Ethical Hacking on Business and Governments”, IRJET vol.6, pp 1088-1092.
[16] Vivek Shrivastava and Monika Pangaria (2013), “Need of Ethical Hacking in Online World”, International Journal of Science and Research vol.2 issue 4, pp 529-531.
[17] Aman Gupta and Abhineet Anand (2017),” Ethical Hacking and Hacking Attacks “, IJECS Volume 6 Issue, Page No. 21042-21050
[18] Prabhat Kumar Sahu, Biswamohan Acharya (2020), “A REVIEW PAPER ON ETHICAL HACKING”, International Journal of Advanced Research in Engineering and Technology (IJARET) Volume 11, Issue 12, pp 163-168
[19] Danish Jamil and Muhammad Numan Ali Khan (2011), “IS ETHICAL HACKING ETHICAL?”, International Journal of Engineering Science and Technology (IJEST), vol 3 No. 5, pp 3758-3763.
[20] Vinitha K. P (2016), “Ethical Hacking”, International Journal of Engineering Research & Technology (IJERT), vol 4 issue 6.