Impact Of Ethical Hacking In Data Security

Dr Thara L[1], Arun Karthik K[2]
[1]Assosciate Professor, Dept of MCA
[2]Dept of MCA
[1, 2] PSG College of Arts and Science, Coimbatore, India

Abstract- *Since ancient times wireless communication has been a part of our human evolution where pigeons were used to send messages,smoke grenades to identify lost soldiers during world war etc.Now we use electromagnetic waves to transmit signals to the other end.There are other varying types of waves such as microwaves,radio waves,IR waves used to transmit signals.They provide Flexibility and wide range of transmission compared to Wireless Communication networks.In this paper,we will discuss about the data security Wireless Communication including the risks of online data theft and how security can improved using ethical hacking.*

Keywords- Wireless transmission, Data security, Ethical Hacking.

I. INTRODUCTION

The Internet's rapid development has given rise to a number of useful and appreciated solutions for our daily lives, including electronic commerce, electronic communication, and new areas for data distribution and study. The concern of an increase in criminal hackers is present, nevertheless, as with many other technical advancements.The government, private company, and the average computer user are all concerned about their facts or private information being compromised by a criminal hacker due to the advancement in Internet expertise. These hackers, often known as black hat hackers, will stealthily access the organization's data and transmit it to the public internet.Another group of hackers, known as ethical hackers or white hat hackers, emerged as a result of these major disagreements. Therefore, this essay explains ethical hackers, their skills, and how they go about assisting their clients and closing security gaps. Therefore, in terms of system security, these ethical hackers would use the same strategies and tactics as hackers use but in a legitimate way, causing no harm to the target systems or information theft. Instead, they would assess the target system's security and inform the owners of any vulnerabilities they discovered along with recommendations for how to fix them.

Fig 1 describes the most common crimes done by hackers where we can see that phishing is being used atmost by the hackers.Phishing, sometimes known as "fishing," is an assault that tries to steal your money or your identity by tricking you into disclosing personal information on websites that look official but are actually fraudulent.In a phishing effort, an attacker may send you an email that appears to be from someone you trust, such your boss or a company you do business with. It will seem genuine and urgent in the email (e.g. fraudulent activity has been detected on your account). In the email, there will be an attachment or link to click.

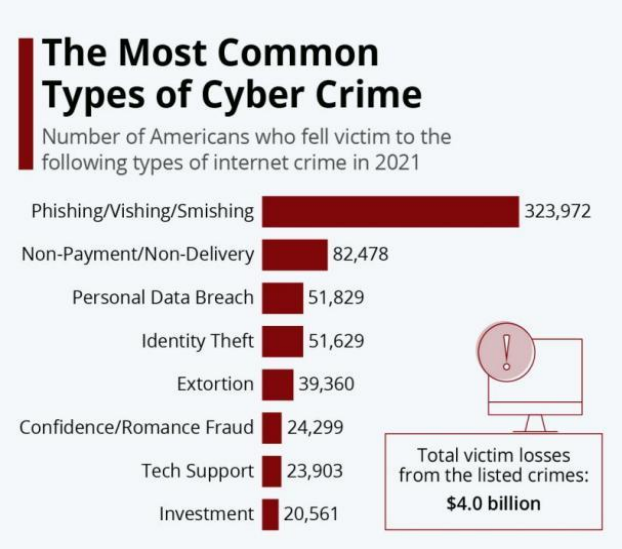

Fig 1 The most common types of cybercrime

The majority of cybercrime consists of an attack on data pertaining to people, businesses, or governments. Although the physical body is not the target of the attacks, it is the set of data characteristics that distinguish individuals and organisations on the Internet, known as the personal or corporate virtual body. To put it another way, our virtual identities are crucial components of daily life in the digital age. We are a collection of numbers and IDs in numerous computer databases that are controlled by both governments and businesses. The prevalence of networked computers in our lives and the brittleness of concepts like personal identity are both brought home by cybercrime.Ethical hacking is a test to find any potential weak points in an information technology environment. Hacking a network in an ethical manner and with good motives is referred to as ethical hacking. This paper explains in depth the cyber security as well as what ethical hacking is, what it will accomplish, an ethical hacking technique, as well as some tools that may be utilised for an ethical hack.[1]

II. ETHICAL HACKING

Companies may now test their network security using ethical hacking to see if they are susceptible to attacks from hostile hackers. This is done by having a group of hackers try to break into the company's network, analysing those attempts, and then figuring out where the system is vulnerable.Black box penetration testing, grey box penetration testing, and white box penetration testing are just a few of the several ethical hacking techniques. In terms of cyber security, each method of hacking has benefits and drawbacks. Therefore, before determining which one is best for your purposes, it is crucial to grasp the distinctions.

In order to protect the important data, ethical hacking entails good hackers gaining access to the system or data. Utilizing all of your knowledge to understand the tactics used by harmful attackers is a crucial component of ethical hacking. Data security in ethical hacking is achieved by pen testing, also known as penetration testing. Invasive techniques are used in ethical hacking to find critical cyber security flaws that could be found and used by an unidentified attacker. This hacking may damage crucial data, creating a dilemma for the company. A crucial piece of data loss might cost you millions of rupees or perhaps a hard-earned reputation. Ethical hacking exists to protect businesses from such a scenario. Prior to hostile hackers, they try to find security holes and problems in a company's security system.Finding security flaws in the system firewall and exploiting them to get unauthorised access to carry out damaging acts is the exact definition of hacking. For instance, hackers who manage to bypass the security could steal or erase crucial data that could endanger an individual or a business.On the other hand, ethical hacking is a type of hacking that is allowed. Computer experts are hired by businesses to review system security, identify holes, and offer suggestions for strengthening the firewall. The government can use it to track and identify potential dangers to national security.Ethical hacking is still practised to protect private and secret information from invaders. Hackers attempt to steal crucial data, but ethical hacking can stop them. Only when a company employs ethical hacking is it possible to track vulnerabilities and threats to sensitive data.To stop intelligence on swaying politics, a hostile state, and other matters from reaching the public, the government has authorised ethical hacking. The safety of every country is of utmost importance, and ethical hacking helps to prevent terrorist attacks and cyberterrorsm.

A.TYPES OF HACKING TO KNOWN BY AN ETHICAL HACKER:

1)HACKING WIRELESS NETWORKS: Hacking wireless networks entails gaining unauthorised access to a computer network, frequently by taking advantage of security flaws in the system. An excellent illustration of this is the practise of "wardriving," in which an attacker drives around seeking for open or inadequately protected networks while using a laptop or other device capable of picking up wireless signals.

2)SYSTEM HACKING: System hacking is the sacrifice of computer software to access the targeted computer to steal their sensitive data. The hacker takes advantage of the weaknesses in a computer system to get the information and data and takes unfair advantage. System hacking aims to gain access, escalate privileges, and hide files.

*3)WEB SERVER HACKING:*On the server side, real-time software applications are used to create web content. This enables hackers to use DoS attacks, port scans, SYN floods, and sniffing to target the webserver and steal personal information, data, passwords, and corporate information. Web servers are broken into by hackers in order to make money through theft, sabotage, blackmail, extortion, etc.

*4)PHISHING:*There must be a compelling reason for you to take action, otherwise you won't likely open a random attachment or click on a link in any email that you receive. Attackers are also aware of this. Attackers frequently use phishing techniques, or impersonating someone or something else, to persuade you to take a step you ordinarily wouldn't, in order to convince you to instal malware or reveal important information. Phishing attacks can be challenging to thwart since they depend on human curiosity and instincts.An attacker may send you an email in a phishing attempt that appears to be from someone you trust, such as your boss or a business you do business with. The email will appear to be real, and it will be urgent (e.g. fraudulent activity has been detected on your account). There will be an attachment or link to click in the email. By clicking on the malicious attachment, you'll infect your machine with malware. If you follow the link, you can be taken to what appears to be a trustworthy website that requests your login information so you can access a crucial file, but it's actually a trap designed to steal your login information. stop.[6]

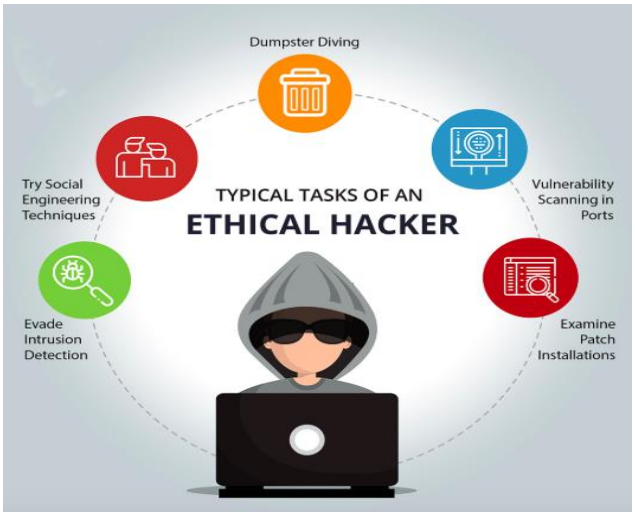

Fig 2 Tasks of an Ethical hacker

B. TASKS OF AN ETHICAL HACKER:

Fig 2 describes thefollowing tasks of an ethical hacker

*1)DUMPSTER DIVING:*Dumpster diving is the practise of searching through trash for details on a person or business that could be used for future hacking. This attack primarily targets large enterprises or corporations in order to conduct phishing on its targets by sending them phoney emails that appear to be from a reliable source.

2)SOCIAL ENGINEERING: The goal of social engineering is to get people to divulge their private information. People fall for the attacker's deception because they believe them and are uninformed. Social engineering comes in three flavours: human-based, mobile-based, and computer-based. It is challenging to identify social engineering attacks when security regulations get laxer and there are no hardware or software tools to stop them.

3)*FIREWALLS & INTRUSION DETECTION*:An intrusion detection system is a group of tools or systems that keeps track of and examines network traffic in search of any unusual activity and sends out notifications when it finds any.Similar to this, a firewall is a framework for network security that controls both inbound and outbound network traffic by allowing or disallowing packets in accordance with a set of security rules.

III. TOOLS USED BY HACKERS

A. AIRCRACK:

You may use Aircrack, one of the most well-liked wireless password cracking programmes, to break 802.11a/b/g WEP and WPA encryption. By collecting packets, Aircrack employs the best techniques to recover wireless passwords. When there are sufficient numbers of packets, it tries to retrieve the password.

B. *AIRSNORT:*

Another well-liked tool for wi-fi 802.11b network WEP encryption decryption is AirSnort. It is a no-cost programme that runs on both Linux and Windows systems. Although this utility is no longer updated, you can still obtain it from Sourceforge.

C. WIRESHARK:

The network protocol analyzer is called WireShark.Packets can be live-captured and analysed. It allows you to check data at the micron level and captures packets.

D. CLOUDCRACKER:

The online password-cracking tool for WPA-protected wireless networks is called CloudCracker. Various password hashes can be cracked with this programme. Simply run the tool, enter the network name, and upload the handshake file.[2]

IV. REAL TIME INCIDENTS

A. WORDPRESS'S FLAW ALLOWED USER INFORMATION TO LEAK:

In the past, a new WordPress plugin called Social Network Tabs was made available. WordPress is the most popular platform for creating websites. Although this plugin became very popular, no one was aware of the flaw. In essence, it assisted users in sharing website material on social networking. A French security researcher by the name of Baptiste Robert, Elliot Alderson was his internet alias. He was the one who discovered the plugin's flaw, which MITRE identified as CVE-2018-20555.The flaw in the plugin compromised the user's Twitter account. Since the plugin is connected to the user's social media account, the vulnerability leaked the user's social media details. Robert was the first to spot this leak and was fast to notify Twitter about it, which helped secure the user's accounts that got affected by it.

B. WEAKNESS IN ORACLE'S UPDATE:

Oracle unannouncedly released a security upgrade in 2019. Fans were surprised by this until they discovered why it

occurred. The security upgrade, which was of the utmost importance, corrected a WebLogic Server code vulnerability. The vulnerability was discovered by the security company KnownSec404. The vulnerability was given the designation CVE-2019-2729 and received a relatively high rating of 9.8/10. Due to a vulnerability, it was vulnerable to attacks from hackers who wanted to access two applications that the server had left online.

C. VISA CARD VULNERABILITY:

One of the most well-known ethical hacking examples to emerge online was this one. The event happened on July 29, 2019. A security flaw in Visa contactless cards that let hackers get around payment restrictions was discovered by two security experts from a company named Positive Technologies. The company would suffer a large loss due to this security issue. This one incident increased awareness of ethical hacking. In order to understand more, several students started taking online cyber security course certificates.

This was found by Leigh-Anne Galloway, the lead for cyber security resilience, and Tim Yunusov, the head of banking security. This became known after five significant UK banks were attacked. On Visa cards, the contactless verification had a maximum of £30, but because of this flaw, hackers could get around this restriction.

D. DSLR RANSOMWARE:

Eyal Itkin attended the DefCon27 in 2019, which took place. He worked for Check Point Software Technologies as a researcher of vulnerabilities. He disclosed that the Picture Transfer Protocol (PTP) vulnerability in the Canon EOS 80D DSLR allowed ransomware to be installed on the camera over the WiFi connection. He continued by pointing out that the PTP had six flaws, making it a prime target for hackers. Using this flaw in the firmware, they may simply gain access to the DSLR.

Canon was alerted to the security breach risk by the Eyal team. A few months later, Canon issued a warning informing users that the vulnerability had never been used by hackers, which means it was never found. They did, however, also advise consumers to adopt security measures to protect themselves.

E. ZOOM ISSUE:

Jonathan Leitschuh revealed a very serious vulnerability in Appel's Macs on July 9, 2019. Hackers were able to take control of the user's front camera thanks to this vulnerability in the security system. Due of this, a person could be coerced by various websites into joining a Zoom call without their knowledge or consent. Millions of users who would hold meetings or even use Zoom in general were at risk from this invasion of privacy. Due to the fact that it was exposed on social media to raise awareness, this is a significant ethical hacking case. Zoom immediately released a quick-fix patch to resolve the problem.

F. ZOMAT0:

The security of Zomato, one of the most popular online restaurant directories and meal ordering apps, was breached in 2017. The hacker has five objectives. names, emails, user names, passwords, and numeric user IDs. Since 17 million users were the intended targets, massive amounts of data were lost. Before initiating contact with the company, the hacker was able to sell this information on the darknet to anyone. One of India's most frightening ethical hacking cases was this one. People began to doubt the nation's cyber security as a result of this.Zomato published a few blogs after this case was made public in which they discussed the actual perpetrator of this breach. According to reports, the activity was carried out by an ethical hacker who wished to raise awareness of the problem of national cyber security. It was successful because cyber security became a hot topic across the nation

.

G. THE REWARD PROGRAM:

The goal of this incentive scheme was to encourage talented individuals to use their hacking prowess to find flaws in the company's security measures. These days, many businesses employ this application to identify security flaws. Millions of dollars have been invested in this effort by businesses like Google, Microsoft, and Facebook to identify system weaknesses and strengthen their defences against cyberattacks.If the person can identify and resolve the problem, they may receive monetary rewards or even recognition. This has shown a wide range of problems in addition to numerous incidents of skilled, ethical hackers that we have never seen before.[6]

V. CONCLUSION

Hacking offers both advantages and disadvantages. Hackers come in a wide variety. They might put a business out of business or safeguard the data, raising profits.

The conflict between harmful or "black hat" hackers and ethical or "white hat" hackers is a protracted one with no clear victor. While malevolent hackers break into networks

unlawfully and cause damage for their own personal gain, ethical hackers assist corporations in understanding their security needs.Ethical hackers assist businesses in identifying current hidden issues with their servers and corporate network. When used appropriately, the tool of "ethical hacking" can help one understand a network's vulnerabilities and how they might be exploited. This supports the notion that hacking is a significant element of the computer world. It discusses both the good and the unpleasant parts of existence. A lot of sensitive information is maintained and saved thanks to ethical hacking, but malevolent hacking can completely destroy it. The hacker's intentions are what ultimately matter. Since the human mind cannot be controlled, it is nearly impossible to close the gap between ethical and malicious hacking, but security measures can be tightened.It can be concluded that wireless networks has opened up the game to new levels for data security s the development is being rapid the data is also being exposed open at a very large rate.So it is also very important to secure the data that is being shared.Development without security isnt really the true growth of communication so simultaneous growth in both is what real development is.Security is also being now enhanced and by using firewalls,data encryption,private network we can prevent the data from being stolen where Ethical hackers play a main role nowadays.

REFERENCES

[1] Aman Gupta and Abhineet Anand,”Ethical Hacking and Hacking Attacks”-2017
[2] Prabhat Kumar Sahu, Biswamohan Acharya,”A review paper on Ethical Hacking”-2020
[3] C.Nagarani,”Ethical hacking and its value to security”-
[4] Bhawana Sahare, Ankit Naik, Shashikala Khandey-”Study of Ethical Hacking”-2015
[5] URL:”https://www.knowledgehut.com/blog/security/ethical-hacking-case-study”
[6] URL:”https://www.knowledgehut.com/blog/security/types-of-ethical-hacking”