Hackers and Their Techniques

Dr. Kavita Sheoran[1], Vishrut Rana[2]

[1.2]Dept of Computer Science, Maharaja Surajmal Institute of Technology, Janakpuri, Delhi, India

[1]kavita.sheoran@msit.in, [2]vishrutrana0202@gmail.com

Abstract: Nowadays, hacking is a well talked and recognized issue. Because there are so many people in the world, many of whom are hackers, it is difficult to describe and objectively identify. This article is composed to maximize awareness among the different age groups. of people/children about the different types of hackers.[1]

I. INTRODUCTION

A hacker is a person with technical computer skills. It is with the person how he uses his skill and for what purposes he uses his skills. There are different types of hackers performing several activities for different purposes. The basic question that arises to the people: How can we defend our system from black hat hackers? What is the average salary package for hackers? What are the types of attacks that an Ethical Hacker can perform on a device? Important steps performed by the Indian government. Which companies require the hackers most? How do we know that our system has been hacked? What was the history of hackers? How powerful could a hacker become in the future?[6]

So let us start our journey to the hackers with a basic technique that a hacker can perform.

II. DIFFERENT TYPES OF HACKERS

Hackers can be classified into many types but basically, there are 3 types of professional hackers (also shown in Fig. 1):

1. White Hat Hackers (Ethical Hackers).
2. Black Hat Hackers (Non-Ethical Hackers).
3. Grey Hat Hackers.

Fig:-1 Types of Hackers

The other types of hackers are:

1

1. Green Hat Hacker (intermediate hacker):

They are the ones who had just started hacking. They are the ones who perform tracking of IP addresses, packets, etc. [7]

2. **Blue Hat Hackers (revenge hackers):** They are the ones who use their skills for revenge against anyone/any organization.[5]

3. **Red Hat Hackers (aggressive hackers):** They are the ones who had quite a lot of knowledge and skill. They are used to stop the black hat hacker. They are the ones who can destroy the device completely using various dangerous viruses.[4]

4. **Script Kiddie:** A novice hacker who breaches a system using real hackers' tools, scripts, and software. They go by the name Script Kiddie. [5]

5. **Suicide Hackers**: They are those who are not concerned about being caught or receiving any other punishment because their goal is to destroy important infrastructure for a good cause. And many more… [7]

A. WHITE HAT HACKERS (ETHICAL HACKERS)

Many hackers use their skills for the world to be protected and from whom we should feel safe. A white hat hacker is a certified

person from a university that uses purely his knowledge on serving the world to be the best in technology and defense. They help the people from the black hat hackers and sometimes grey hat hackers. They are the ones who are respected to be the most by every government agency. They use their skills in making

ones who are not certified and use the knowledge for harming society. They are usually indulged in many illegal activities.

They use many different techniques to access the person's sensitive data, rob money, etc. They are the ones who can even kill a person for not fulfilling their need. They are in huge amounts around the world. [2]

their firewall, password, and smart passwords to be the maximum security and perform different types of penetration. They are the ones that are required the most in the future by every sector. They are quite friendly to us. They use to find the ports that are open in any device.[3]

B. BLACK HAT HACKERS (NON-ETHICAL HACKERS)

They are the ones who use their knowledge in harming the people, government, and world.

They are the ones from whom we should be very careful. As they are the most dangerous community in the world. They are the

Boss. For creating strong passwords, you should keep

Hackers and Their Techniques

C. GRAY HAT HACKERS

They are the ones who are neither purely black hat hackers nor they are white hat hackers. They are the ones who can do anything they want with anyone's devices. They usually care about the profit they would get. They serve as a link between grey and black hat activities. They frequently scan systems for vulnerabilities without the owner's consent or knowledge. If problems are discovered, they report them to the owner and may ask for a modest charge to correct the issue or for identifying the issue with the code. They work illegally but help the company but after repeated warning to the company they can against black hat hackers. [4]

III. HOW CAN WE DEFEND OUR SYSTEM FROM BLACK HAT HACKERS?

Use the following advice to safeguard your devices and sensitive data:

1) **Use a Firewall:** In the present technology, almost all operating systems (OS) are providing a firewall. But the OS with 2007 and below might have to install a firewall. How the firewall defends a system is shown using Fig:- 2 [5].

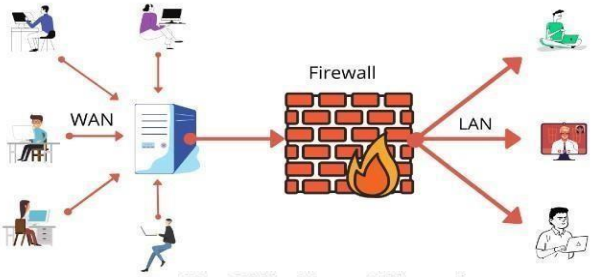

Fig:-2 Working of Firewall

2) **Install Antivirus Software:** A person should install an antivirus that can protect the computer from getting hacked. Bitdefender, Panda Free Antivirus, Malwarebytes, Avast, and McAfee are some of the antivirus programs you can utilize.[2].

3) **Install an Anti-Spyware Package:** Spyware is a specific kind of software that covertly watches and gathers data from individuals or businesses. Unwanted advertising and search results that are meant to send you to other (sometimes malicious) websites are difficult to spot and deliver. [1]

4) **Use Complex Passwords:** The hackers usually hack a device by hit and trial method i.e. by using the global libraries from a source such as GitHub. Try to use such password managing websites that provide you security as well as suggest some strong passwords, such as Dashlane, Sticky Password, LastPass, or Password

in mind that the password should not contain any relative person's name, numbers. It should be random. You can use special characters such as '=','@','!', contain your mobile number, etc… also the password should not be too short to be guessed.[7]

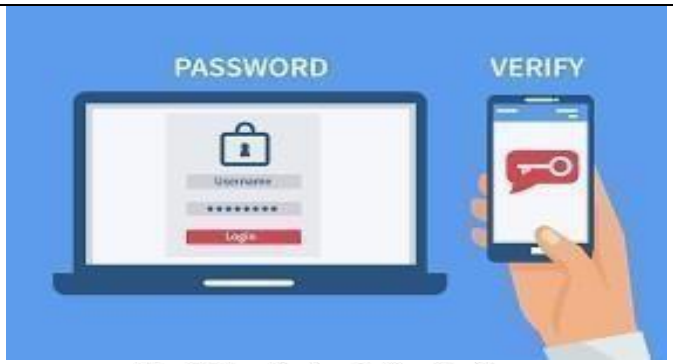

Fig:-3 Two-Factor Authentication

5) **Use Two-Factor Authentication:** Many websites allow you to enable two-factor authentication, which increases security by requiring you to enter a numerical code in addition to your password when logging in. This code is sent to your phone or email address. It is a two-way login process as shown in [5] Fig. 3.

6) **Other Measures:** Use a browser that doesn't show any ads or irrelevant ads such as Brave, Tor, Mozilla Firefox, Vivaldi, Epic, or opera, or add an extension such as DuckDuckGo. For Apple or mac users there are additional websites Apple Sufari[3].

7) **Camera:** In laptops make sure the camera light is off when you are not using the device camera. If it is not getting off then cover the camera or preferably fold your laptop [5].

IV. AVERAGE SALARY PACKAGE OF AN ETHICAL HACKER

The average salary package of an ethical hacker in India is Rs 6,11,094 per year according to glassdoor.com. The height salary offered in India at present for an Ethical Hacker is from Rs1,21,641 to Rs9,10,630 by the company Infosys Limited [7].

Fig:-4 Package of an Ethical Hackers

The average salary package around the world is between $67,209 and $103,583 per annum according to various salary aggregate websites. The salary distribution on the basis of experience is:

- 0–1 year experience: $75,027
- 1-3 years experience: $80,440
- 4-6 years experience: $89,399
- 7-9 years experience: $98,991

V. DIFFERENT TYPES OF ATTACKS THAT AN ETHICAL HACKERS CAN PERFORM ON A DEVICE

There are 7 types of Attacks as shown in the Fig. 5

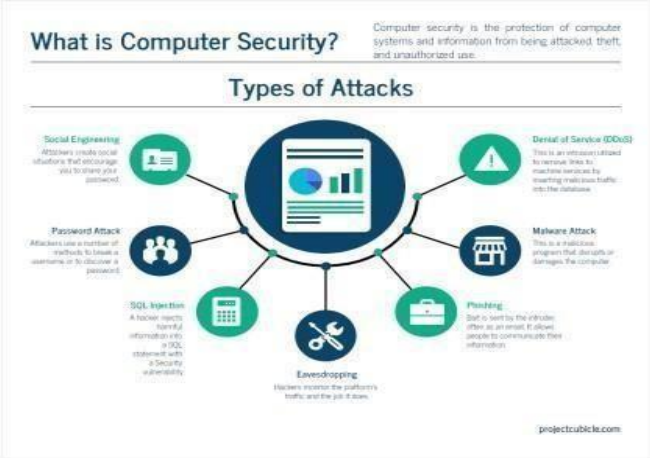

Fig:-5 Types of attacks

There are 10 types of attacks that a hacker can perform:

1. **Malware Attack [Malicious software Viruses]:** It contains trojans, worms, spyware, ransomware, and adware. A valid piece of software is the trojan virus. It restricts access to the vital parts of the network. Software known as spyware grabs all of your private information without your awareness. Adware is software that shows users advertisements on their screens, like any fruit. Malware enters a network and can seriously harm both a human and a device. It

   happens when a user clicks on a risky link, downloads an email attachment, or uses a pen drive that is contaminated. The rate of malware breaches is as shown in [6] Fig. 5

2. **Phishing Attack:** It is currently one of the most prevalent and pervasive forms of cybercrime. In this scenario, the hacker delivers the victim(s) harmful links via messages or emails. On clicking on such types of link(s) the hacker gains access to confidential information and sometimes account confidentiality

9. **Zero-Day Exploit:** The seller makes the users aware of the vulnerability, but the attackers also learn about it. It depends on time how much time would the vendor could take. In the meanwhile, the attackers are the focus of the attackers. They take care to use the flaw to their advantage even before a patch or other fix is put in place.[7].

10. **Watering Hole Attack:** Here, a specific segment of an entity or area is the victim. Here the attacker targets the website(s) that are frequently used by that group/ organization. The Watering Hole Attack technique is done as shown in the [5] Fig. 7.

Hackers and Their Techniques

through which a person can lose his/her credits from the account.[7]

3. **Password Hacking:** Now a day's password hacking also had become an easy task as hackers most of the time use the inbuilt password libraries and have to implement some of the combinations to crack them. But still while using some strong or difficult password gives the victims some time to stop the hacking. We can get to know whether the device is not responding or showing the filling of the option repeatedly (unless there is an external error)[3].

4. **Man-in-the-Middle Attack (eavesdropping attack):** During the COVID-19 pandemic it has been practiced for quite some time. In this, an attacker intercedes between the two parties. In other words, the attacker interferes with Clint(s) and Host's conversation(s) [4].

5. **SQL Injection Attack:** When a hacker modifies a typical SQL query on a database-driven website, it results in a Structured Query Language (SQL) injection attack. It occurs when malicious code is introduced or introduced into the search field, forcing the server to divulge important information. This gives the attacker access to the database's tables for viewing, editing, and deletion. Through this, attackers may also obtain administrative rights. [2].

6. **Denial-of-Service Attack (DOS-attack):** This is a very dangerous attack as it floods the target system using a network resulting in the device to get shutdown or slowing down of the device [1].

7. **Insider Threat:** It is the attack performed by the insider (known person). The person could be dangerous if he is an intermediate as it could be hard or difficult to track the person [2].

8. **Cryptojacking:** These are the attackers who attack to steal/mine cryptocurrency (online currency). They also use online ads in which the JavaScript code was embedded in the emails. The victims are ignorant of this since the Crypto mining code operates in the background; the only indication would be a delay in the execution. [3].

Fig:-7 Watering Hole Technique

VI. IMPORTANT STEPS PERFORMED BY THE INDIAN GOVERNMENT

According to annual data on cybercrime, the number of security breaches has increased by 69% since 2015 and by 11% since 2018. And hence the Indian government has created a law for the same [10]. Also, the Indian government had spent about $945 million US dollars to enhance the cybersecurity of the nation.

Certain acts are made by our government:

The patents(amendment) act, was formed in 1999.

Trade Marks act.1999

B. TRADE MARK ACT

The "protection, registration, and prohibition of fraudulent use and the developer of trademarks" are the subjects of this law. A trademark is exposed vulnerability is the focus of the attackers. defined as a symbol that may be represented visually and can be used to differentiate one person's goods or services from those of another. This symbol can take the form of an object, its packaging, or a combination of colors. [9]

C. THE COPYRIGHT ACT

This act basically protects the content from getting copied by other [unauthorized] users and display it by just changing name. In it the content should not be sheared along people using

The copyright act, of 1957

Information Technology Act

A. THE PATENTS(AMENDMENT) ACT

The 1999 founding of this act. Although such patents were not permitted, this legislation "Provided the filing of applications for product patents in the fields of medications, pharmaceuticals, and agrochemicals." [8]

any mode of internet such as social-media, blogs, etc… [8]

D. INFORMATION TECHNOLOGY ACT

It is an Act that was created to give legal legitimacy to transactions that will be carried out through electronic data interchange or other forms of electronic communication, which are collectively known as "electronic commerce." In the year 2000, this law was established. [10]

VII. REQUIREMENT OF HACKERS.

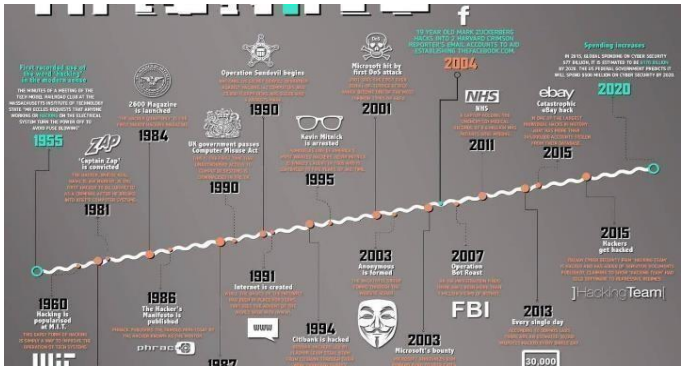

Fig:-8 History of Hacker's

X. POWER OF A HACKER IN THE FUTURE

It is believed that if there would be any war then it could be cyber war as it is quite powerful if a person gets access to any missile (nuclear missiles) so it would be quite dangerous. So according to my perspective, we should be pre-prepared for such types of dangerous things.[9]

XI. CONCLUSION

There are many knowledge in the world but it is within our hand how do we have to become in life and which company can lead

us to a successful as well as a respectful person around the world. Similarly, if there are black hat hackers so to stop them there are white hat hacker who are ready to stop the black hat hackers from defending the systems from getting hacked.

Companies that hire certified ethical hackers in India are IBM, Netsoft Technologies, Prime Infoserve, Deloitte, VISTA Infosec, Standard Chartered, Crypto Mize, and TCS.

VIII. HOW DO WE KNOW THAT OUR SYSTEM HAS BEEN HACKED?

You may experience any of the following signs if your computer has been hacked: frequent pop-up windows, particularly those that direct you to visit other weird websites, some ads that contain viruses, or websites with unsafe links from the main page. Alterations to your homepage Your email account or messages are being used to send bulk emails. It might be even possible for someone to use your device to call another person using IP spoofing [7].

IX. HISTORY OF AN HACKER

In 1955, during a meeting of the Technical Model Railroad Club, the term "hacking" was first employed with technical acumen. Members' modifications to the capabilities of their sophisticated train sets were detailed in the meeting minutes.
[9].

REFERENCES

[1] Pavan Vadapalli, “Director of Engineering @ upgrade." Upgrade cyber security, AUG 23, 2022. [2] Tim Jordan, School of Media, Film, and Music, University of Sussex, SAGA Journals, 2008.

[3] A handbook of copyright law, copyright government website,1957. [4] Authority, "Government of India",9 June 2000.

[5] Ashish Kumar, “Youtuber” WsCube tech,29 Aug 2021. [6] Peter Lipa, co-founder of Sticky Password,2001.

[7] Motoyuki Isobe, “President and Founder of Techouse”, 3 Sep, 2021. [8] Krishna Kumar CEO of Simplilearn.com also an engineer graduate from NIT, Surathkal, India and started the company from 2010.

[9] Kathy database developer and business process engineer and currently the founder of Techouse from 1995.

[10] Jason McMahon Dual B.S. in Network Security & Digital Forensics, Coleman University (Graduated 2010), 2018.

[11] Mattia Campagnano Attack & Pen Consultant with Optiv, 2018.