International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 01 | Jan - 2022 ISSN: 2582-3930

Ethical Hacking and Hacking Attacks

Yash Antil

Abstract

In today's world information is available online to a large number of users who access information many times in a day . Information can be used in both good and bad ways (like destroying or stealing the data of websites or databases without the knowledge of their owner/ hacking someone's account without their knowledge / Stealing bank account credentials for stealing money etc.). The purpose of this paper is to make people aware about what hacking is, who are hackers, what is ethical hacking, how to avoid getting hacked, securing our systems and how to be safe online and also how hackers took opportunity of Covid-19 to scam/hack people.

Main Motive: What Hacking is and How hackers used covid -19 as on opportunity to scam/hack people.

Keywords: Hackers, Ethical Hackers, Phishing.

1. Introduction

During the advancement of computer technology, it has pros and cons also; HACKERS. In today's world the data available on the internet is growing at a very fast rate, a large amount of data is moving online to endless number of users, therefore, data security is the major issue. Banking and transfer of money is mostly done online now a days, sending and receiving of various forms of data, thus increasing the risk of the data security. A large number of small companies, big companies, whether it's a small or large organizations, banks, and websites have been often targeted by the various types of hacking attacks by the hackers. Generally, after hearing the term hacker most of the people think Hackers are people who are computers technology experts with bad intensions, who tries to steal, leak or destroy someone's confidential or valuable data without their knowledge/with their knowledge. They are the very high skilled computer experts who breaks into someone else system for gaining access to their personal information. To avoid getting hacked by the hackers we have Ethical Hackers in the industry to protect us because they are also computer experts just like the hacker who are bounded by some set of rule and regulations by the various organizations. They protect the online moving data from various attacks by hackers and keeping the data safe with the owner. Further, this paper tells you more about hackers, ethical hackers and how to stay anonymous, code of conduct of hackers, how to avoid getting hacked and to make people aware about the technology and other tricks to stay safe online and how most importantly how hackers used Coronavirus to scam people.

1.2 Literature Survey

What is Hacking?

Hacking is an attempt to exploit a computer system or a private network inside a computer or it is the unauthorised access to take control over computer network security systems for some illicit purpose.

What is a Hacker?

Someone with good technical knowledge and skills who breaks inside a system with the permission of system's owner to steal, destroy, change or manipulate the data is known as hacker.

- Tests and breaks into those features by an uneven way.
- Makes programs to bypass these programs
- Can be a white hat or black hat.
- Hackers are paid to break the system and applications illegally.
- Hackers make our systems secure. Ethical Hackers has made surfing the internet easy for us otherwise your data can be used by someone else.

HACKERS can be classified mainly into three groups:

Different Types of Hackers:

Black Hat Hackers:

They breach into the computer system for their personal gain. These persons misuse their extensive knowledge in the computers, technology and commits various cybercrimes like leaking data, stealing password details, identity stealing, credit card fraud etc.

White Hat Hackers:

A computer security specialist that breaks into a system and finds the loopholes in the protected networks or inside the computer systems of organization or company who asks them to and improves their security. White Hat Hackers use their skills and knowledge to protect the organization or company etc. from malicious code/ scripts, viruses or from black hat hackers who try to harm their systems.
They create algorithms to break existing internet networks to solve the bugs errors

or loopholes in them.

Grey Hat Hackers:

Grey hat Hackers are Hybrid between Black hat Hackers and White hat hackers. They hack any system even without permission to test the security of the system unlike black hat hackers.

They exploit the internet systems only to make certain vast datasets of information public so that it can benefit everyone without having any bad intentions of black hats.

Red Hat Hackers:

A red hat hacker is someone who targets Linux systems. Red hats have been characterized as vigilantes. Red hats will launch aggressive attacks against their enemy to bring them down. They often destroy the black hat's computer and their resources.

Red hat hacker finds black hat hackers and then eliminate and destroy their attack and harmful schemes.

Blue Hat Hackers:

Blue hat hackers are security professionals that work outside of the organization. Organisations and Companies whether small or big, they often invite them to test the software's they developed and find security vulnerabilities before releasing them in market. They perform penetration testing and deploy various cyber attacks without causing damage to find the loopholes.

How hackers hack any system:

Reconnaissance:

This is the first phase where the hacker tries to collect information about the target. It may include identifying the Target, and then finding out the target's IP Address Range, Network DNS Records, etc.

This step is to collect information about the victim.

Scanning:

This includes usage of tools like dialers, port scanners, network mappers, sweepers, and vulnerability scanners to scan data. Hackers decide to use a couple methods for this end to help map the network(i.e. Kali Linux, Maltego and find an email to contact to see what email server is being used).

This step will give a path to enter into system.

Gaining Access:

Now hacker designs the blueprint of the network of the target with the help of data collected during previous steps. The hacker has finished enumerating and scanning the network and now decide that they have some options to gain access to the network.

This step makes you into the system to exploit attacks.

Maintaining Access:

Once hacker has gained access, they want to keep that access for future exploitation and attacks. Once the hacker owns the system, they can use it as a base to launch additional attacks. This is the phase where hacker completes his attack.

This step is to keep the access during the exploitation.

Clearing Tracks:

Prior to the attack, the attacker would change their MAC address and run their attacking machine through atleast one VPN to help cover their identity. Once access is gained and privileges have been escalated, the hacker seek to cover their tracks.

This step includes clearing out Sent emails, clearing server logs, temp files, etc.

Finally By doing all these tasks, Hacker has successfully hacked into your system.

1.3 Objectives

Many people are not aware of how to protect them from getting hacked. Here are some suggestions to help you secure yourself and others around you getting hacked.

How to protect yourself from Hackers:

- Don't access personal data or financial data with public Wi-fi.
- Trace when you lost and erase when you surf.

- Be skeptical. Don't open links and attachments quickly.
- Don't forget to use a password lock code or encryption.
- Choose your apps wisely.
- Turn off any data driven app if you don't need them.

7 Easy steps to secure your computer:

1. Always keep your system and software security updated.
2. Enable a firewall in your system.
3. Adjust your browser settings.
4. By installing an antivirus and anti-spyware software to secure your system.
5. Always protect your device with a strong password and also by using a software to lock the device.
6. By encrypting your data.
7. By using a VPN.

4 Ways to be Anonymous online:

1. We can stay anonymous online by using proxies
2. We can stay anonymous online by using Tor Browser.
3. We can stay anonymous by using a VPN.
4. We can stay anonymous online by using SSH Tunneling..

How hackers are using coronavirus to scam people?

1. **Fraud Registered Domains**

Hackers are providing safety masks, hand sanitisers, and other protective gear but in reality they are providing damaged or unsafe products by creating fake stories. If you entered your login credentials and other personal details on fake websites looking completely real then those credentials can be misused by the hackers.

2. **Phishing Emails and Texts**

In this pandemic, hackers are sending an email attached with a spam document or link that imitates as any kind of donation or financial support or any other kind of authorized content regarding the outbreak so that people fall for it. And whenever you will open the provided document or link , your system will get infected with unknown or maybe known malicious vulnerabilities and your online credentials will be stolen.

3. **Social Media Scams**

Yes, there are a lot of scammers or hackers active on social media who are using it for bad reasons. They are offered and are still offering various fraud healthcare schemes regarding Covid-19, requesting for

some amount for food, medicines , masks, sanitisers etc. through creating fake accounts on these platforms. It can put your money, online credentials or other data, etc. at risk. Hence, you need to be very cautious while using social media.

4. Fake Mobile Applications

This is the most often heard cybercrime that comes in Covid-19 scenerio. There are many fake mobile applications available over the internet which often claims to detect Covid-19 positive case in your area. However, these apps acts as the ransomware that infects your mobile and makes all your device data accessible to their masters. You must avoid installation of any unauthorized apps in your mobile device or computer systems.

5. Data Breach

Due to the outbreak, people are forced to do work from home. There are lots of platform over the web that acts as worthy tool for the remote working process such as Task Management Software, Video Calling platforms, etc but some of these are not reliable or secure and can result in the leak of the data o other important information.

1.4 Conclusion

Technology will grow at a high rate over the years and many peoples of all the age are putting themselves in problematic situations by helping hackers to hack them unintentionally. This paper has some steps to avoid getting hacked. Hackers will always find ways of getting into systems, whether they are doing it for good or bad but it's upto us to be aware about such happenings and take various steps to keep us safe online or offline.

REFERENCES

- RD. Hartley, "Ethical Hacking: Teaching Students to Hack", EastCarolina University, http://www.techspot.com/news/21942-
- universityoffers-ethical-hacking-course.html, , 2002.
- [3] T. Wulf, "Teaching ethics in undergraduate network", Consortium forComputing Sciences in College, Vol 19 Issue 1, 2003.
- [4] Jeffrey Livermore, Walsh College, Member, IEEE Computer Society 2007.
- [5] Logan and Clarkson, Is it Safe? Information Security Education: Are We Teaching a Dangerous Subject?, Proceedings of the 8
- th
-
- Colloquium for Information Systems Security Education, West Point, NY, 2004.
- [6] SA. Saleem, Ethical Hacking as a risk management technique, ACM New York, NY, USA, 200
-