Modern Era Hacking

Dr Amarendra K, Venkata Naresh Mandhala, SaiSri Damecharla, Praveen Gollapudi, Pavan Kumar Ponuganti

Abstract: Internet is a most common communication connection between people of similar boundaries or dissimilar boundaries in the modern era. As in this modern era every little detail is digitalized so this internet is the key for the hackers who are willing to hack the contents related to any organization, financial details, personal information. Any kind of such data which is crucial of the end user or an individual is precious to hacker. And in this lays the foundation for the necessity of knowing about HACKING. How can the users keep their data secured and what kind of preventive measures should the users take in order for not being hacked.

Index Terms: Internet, digitalization, organization, personal information, hacking.

1. INTRODUCTION

In this day to day life in modern era, computer plays an essential role. The details related to business, the data related to banking and finance and personal information like contacts of people, pictures likewise everything can be stored in computer or a smart mobile. When two people are connected through internet for the communication, internet plays as a background for the hacker. Hacking can take places when the systems of the users connected not only using internet but also when they are connect without using internet like Bluetooth or tethering connection. Irrespective of the medium through which the computer systems or mobile devices connect, if there are any loopholes in the devices through which the data is being transmitted then that gives leverage to any criminal or a hackers who wants to do damage to the users. The damages to the individuals does not always means physically but also technically or financially.

2 LITERATURE REVIEW

TITLE: Ethical Hacking
AUTHOR: SusidharthakaSatapathy, Dr.Rasmi Ranjan Patra
In this paper, the authors described about the how the growth of internet took place in today's world. How the information must be utilized. How Ethical Hacking comes into the picture and why it is necessary. And also gives the details about the timeline and events that took place in the progress of the ethical hacking.

TITLE: Hacking Attacks, Methods, Techniques And Their Protection Measures
AUTHOR: Dr. Sunil Kumar, Dilip Agarwal
In this paper, the authors gave the detailed explanation about what is ethical hacking and group of hackers who are good and bad like grey hat, white hat and black hat. They also gave the details about tools used by hackers and top ten trending tools used for hacking.
TITLE: Survey on Ethical Hacking Process in Network Security
AUTHOR: U. Murugavel, Dr. Shanthi
In this paper, the authors gave the explanation about what is penetration testing and need of penetration testing. The details about the types of penetration testing, merits of penetration testing.
TITLE: Study Of Ethical Hacking
AUTHOR: Bhawana Sahare, Ankit Naik, Shashikala Khandey
In this paper, the authors described about the access levels of permissions given to the different users. The necessity of security and the security life time. The description of ethical hacking and the phases of the ethical hacking. The phases of ethical hacking include Reconnaissance, Scanning, Owning the System, Zombie System, Evidence Removal. The impacts and benefits of the ethical hacking in different industries or sectors. And finally the limitations of ethical hacking.

TITLE: A COMPREHENSIVE STUDY ON ETHICAL HACKING
AUTHOR: Suriya Begum, Sujeeth Kumar, Ashhar
In this paper, the authors gave the information about the concept of hacking, classification of hackers. Different types of operating systems used in hacking. Various techniques present in hacking. These techniques may be Phishing Hack, FTP Brute Force Hack, Denial of Service (DoS), Malware. And the advantages and disadvantages of the ethical hacking.

TITLE: ETHICAL HACKING (Tools, Techniques and Approaches)
AUTHOR: Brijesh Kumar Pandey, Lovely lakhmaniBalani, Alok Singh
In this paper, the authors gave the explanation about the ethical hacking, what type of activities ethical hacker perform and how do ethical hackers evaluate the system's security. The minimum security policies that any organization must follow in order to keep their organizations information secured. The vulnerability analysis and the exploitation used by hackers. The process of information gathering and information security.

3 HACKING OVERVIEW

HACKING can be defined as the presence of vulnerabilities that helps the breaching into a system. Hacking always necessarily does not mean in a negative way. Sometimes hacking can give positive meaning like hacking the computer system or a mobile device to check if it has any vulnerabilities such performance of hacking is ETHICAL HACKING. Likewise the hackers who performing the hacking are in different types.

3.1 Hackers:

- *Dr Amarendra K, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, A.P., India. Email:amarendra@kluniversity.in*
- *Venkata Naresh Mandhala, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, A.P., India. Email:mvnaresh.mca@gmail.com*
- *SaiSri Damecharla, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, A.P., India.*
- *Praveen Gollapudi, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, A.P., India.*
- Pavan Kumar Ponuganti, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, A.P., India.

1) WHITE HAT HACKERS: These hackers are also called as ETHICAL HACKERS as they perform ethical hacking. They helps to fix the vulnerabilities present in the system or device. These hackers perform hacking as it is their profession and they get paid for their job.

2) GREY HAT HACKERS: These hackers perform hacking as a unauthorized user to find the vulnerabilities and inform them to the respective organization or an individual. Usually Grey Hat hackers fall between White Hat hackers and Black Hat hackers.

3) BLACK HAT HACKERS: These hackers are also called as CRACKERS because they violate the privacy of the user or an organization to steal the data or the performing the money transactions as a unauthorized user.

4) SCRIPT KIDDIES HACKERS: These hackerscomes under non-skilled hackers as they performing hacking with already designed tools.

5) HACKTIVISTS: These hackers perform hacking and send the messages in political, religion ways. They usually perform hacking for their entertainment.

6) PHREAKERS: These hackers perform hacking only on the telephones but not on computer systems.

3.2 Stages in Hacking:

1) RECONNAISSANCE: This is the first stage in the hacking. Most of the time reconnaissance deals with the collection of the information. This information may be an individual's personal details, or an individual's financial details or an organization's employees operations in the computers of the company. Generally reconnaissance can be either active or passive.

- Passive Reconnaissance: Collection of victim's information without their consult.
- Active Reconnaissance: Collection of victim's information with their consult.

2) SCANNING: This is the second stage of hacking. In this stage the hacker scans all the information that is gathered in the reconnaissance stage. Scanning operation are the verification of the IP address of the victim, the operating system used by the victim and the sockets that are used in victims computer system are open or not. Scanning process is done before performing hacking.

3) GAINING ACCESS: This is the third stage of hacking. This stage refers to gain the access of the platform or the operating system or the applications that the victim is using. This is the stage where once the victim's system is comprised when a vulnerability is found, thus the connection can be established and the hacking process can be started.

4) ZOMBIE SYSTEM: This is the fourth stage of hacking. Zombie system means maintain the access which is established with the victim's system in the gaining access phase. In this phase the main operations like installing the virus and worms or Trojan horses in the victim's system or creating the duplicate data to lure the users is done. The users generally don't have any idea about this and utilize the fake websites or the virus included data and thus help the hacker to gain their information.

5) EVIDENCE REMOVAL: This is the fifth and last stage of hacking. In this stage the hackers removes their details or hide any of the hacker's traces from the victim's system so that they cannot get caught.

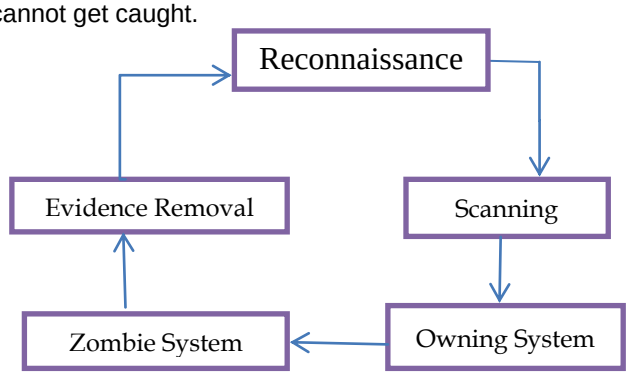

***Fig. 1** stages of hacking.*

3.3 Hacking Attacks:

The hacking attacks that are possible are generally can be performed on a web server, on a web application, and on a mobile device.

ATTACKS ON WEB SERVER:

INPUT VALIDATION ATTACK: In this type of attack, usually there are some of the coding parts of web servers like input data type, data ranges that does not require any validation. So such details are keys to the hackers in this case. Tampering of details at data type or on a data range is possible. And when a hacker did such a thing at a request that has been made by a client who is willing to access the web server then web server gets compromised. So the care to be taken at URL, HTTP Headers, POST requests and cookies. All the web server related information is stored in a database. When a web server is compromised with an attack that eventually leads the database to get compromised.

DENIAL OF SERVICE(DOS):It is one most common type of attack that hackers use to attack the web servers. Denial of service attacks can be in three types. They are volume attack, protocol attack, application layer attacks. Flooding is a common trick used by crackers in order to get the web server shut down. Hackers send in numerous invalid data at a time so that crashing takes place at server. A huge traffic occurs and get server shuts down.

ATTACKS ON WEB APPLICATIONS:

PASSWORD BASED ATTACKS: In this attack, when the user needs to access a web application they must use their login credentials. Login credentials consists of username, password. The login credentials are validated every time when the user uses web applications. The password attacks takes place when the passwords are weak or short. A strong password has certain rules that must be followed. If those rules aren't followed then the password can easily guessed and the web application attacked and the data present in that web application gets compromised.

URL INTERPRETATION ATTACK: This attack can also be called as URL POISIONING. As the name itself suggests that the semantics are changed in a URL so that attack is possible. In this type of attack only the semantics of URL is changed but syntax is always kept same so the user doesn't have any idea that they accessing wrong URL. Most of the CGI- based websites are prone to URL interpretation attacks.

SQL INJECTION ATTACK: This type of attack occurs usually on e-commerce websites or the websites that use huge databases. The databases that have huge data does not validate some of the parameters in the URL. So using SQL language those parameters can be impersonated and crack the database. If the database is exploited then the information of the organization is leaked to the hacker. So there will be a lot financial loss.

3.4 Ethical Hacking:

In this largely growing cybercrime, the users or an individual need know the importance of ethical hacking. Ethical hacking helps in recovery of the system that has been compromised and that is hacked. The hackers who perform ethical hacking are called ETHICAL HACKERS. Like every coin have sides there are advantages and disadvantages of ethical hacking.

Pros of ethical hacking:

- Protection against cybercrimes and data breaches.
- Role of government bodies increases.
- Helps in improvising the security and knowledge with respect to social engineering.
- Better services can achieved with the help of modern hacking.

Cons of ethical hacking:

- Ethical hacking is expensive and hectic.
- Malicious activities can't be prevented.
- System failure and errors takes place all the time.

3.5 Counter Measures:

- As the malware can enter into a system at any time and cannot be promised that they do not enter into one's system so it is advised to always install antivirus in all the devices that are being used.
- Keep a check on firewall, when an attacker tries to attack the firewall tries to prevent it. So when the firewall failing to prevent the attack it notifies the device user then pay attention for notification received from firewall.
- Maintenance of security infrastructures to prevent security threats, have intrusion detection systems to check on systems when intrusion takes place.
- When codes are being used in any program, take care that program is safe from worms, Trojan horses, virus.
- All the mails should be filtered and do not open the mails received from the unknown sources as they are designed to lure the users.
- The passwords that are kept for the social media or any other must be long and strong but not weak.
- Do not open any of your work details or website login credentials in the unauthorized systems.
- Whenever a system must be connected to the internet, check the whether the server is secured or not. Do not connect to public wi-fi connections.

4 CONCLUSION

In this paper MODERN ERA HACKING we are interested to show how important it is to a non-technical person to know about hacking and every person who is using a network connection like internet, LAN, WAN, intranet must have an idea about networking attacks, what web applications they are accessing, how a person should be conscious about using the public networks. Every little detail must be kept hided, protected, safeguarded and secured from the hacker. All these steps must be followed by every individual who is using internet to prevent the financial loss, security threats and life loss in some cases.

REFERENCES

[1] http://www.ijcstjournal.org/volume-2/issue-6/IJCST-V2I6P2.pdf
[2] http://www.ijsrp.org/research-paper-0615/ijsrp-p4237.pdf
[3] https://www.researchgate.net/publication/271079090_ETHICAL_HACKING_Tools_Techniques_and_Approaches
[4] https://www.researchgate.net/publication/271079090_ETHICAL_HACKING_Tools_Techniques_and_Approaches
[5] https://www.greycampus.com/opencampus/ethical-hacking
[6] TOWARDS THE IMPACT OF HACKING ON CYBER SECURITY, Kumar et al. 2018, IIOABJ, Vol. 9,2, 61-77
[7] A (lack of) review on Cyber-security and Privacy Concerns in Hearing Aids,2018 IEEE 31st International Symposium on Computer-Based Medical Systems.
[8] A COMPREHENSIVE STUDY ON ETHICAL HACKING, IJESRT, Begum* et al., 5(8): August, 2016.
[9] Study Of Ethical Hacking, International Journal of Computer Science Trends and Technology (IJCST) – Volume 2 Issue 4, Nov-Dec 201.
[10] Survey on Ethical Hacking Process in Network Security, INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY, Murugavel, 3(7): July, 2014.
[11] Ethical Hacking, International Journal of Scientific and Research Publications, Volume 5, Issue 6, June 2015