Impact of Hacking on Cyber Security

Vijay Ramalingam, Department Of Computer Science and Engineering
Galgotias University, Yamuna Expressway Greater Noida, Uttar Pradesh
E-mail id - r.vijay@galgotiasuniversity.edu.in

Abstract: The rising growth of the internet and machinery whether its mobile or computer technology has brought many good and proficient things for people such as E-commerce, E-mail, Cloud Computing, Data Sharing, Application and many more but there are also a dark and hidden sides of it, such as Network Hacks, Computer hacks, Mobile Breach, Backdoors etc. As we all know that Cybercrime been one of the common practices made by the computer experts and is increasing rapidly in numbers. As we all know, cybercrime was one of the common practices of computer experts and is growing rapidly in numbers. Cybercrime is responsible for disrupting the Organization's networks, stealing valuable data, documents, and hacking a bank account. The government has taken preventive measures a lot of times. In this paper, we're going to discuss the types of hackers.

Keywords: Cyber security, Ethical hacking, Mobile Hacking, Wi-Fi hacking.

INTRODUCTION

Cyber security is a wide range of security across different types of networks. There are many different types of security on the subject. Security is an interesting subject taught in colleges and schools to make people aware of the surroundings and to make them more secure and ready with weapons to carry attacks and viruses in a rich way. Cyber Security is a field of technology, processes and activities designed to protect you from hackers, viruses and malware. It is concerned with both security and computer security. Hardware and security devices deal with physical devices that are responsible for the security of a networking system. Widely driven software security is the idea of engineering that it continues to function properly against a malicious attack. Elements of cyber security include network security, application security, endpoint security, data security, identity management, database and infrastructure security, cloud security, mobile security, disaster recovery / business continuity planning, and end-user education. However, application security, security of the Information Security Network and data security are key areas covered by cyber security. Some steps are taken to make the network less vulnerable, such as access control, authentication, integrity, non-repudiation. Second, cyber security concerns computer security, which ensures that computer systems are protected from theft, viruses and damage to their personal computers. Widely driven software security is the idea of engineering that it continues to function properly against a malicious attack. Elements of cyber security include network security, application security, endpoint security, data security, identity management, database and infrastructure security, cloud security, mobile security, disaster recovery / business continuity planning, and end-user education. Is cybercrime growing at a very high rate that includes sending fraud mails with malware in it that attract users saying that they have won ransom amount of some greedy amount and asking for their account details to make use of the offer that people can easily get trapped in and get hacked. Backdoor in computer systems or crypto-system bypasses normal authentication or security controls that hackers may add to their welfare. Ethical hacking is the way hackers only try to find weakness, also known as "Penetration Testing." There are different stages of hacking. Ethical hacking is the type of hacking that hackers do not harm the computers of the user because it does not contain malicious content. Ethical hacking is the most important thing in life today, as information is the most important asset of an organization that keeps this information secure can only save the company's image. Ethical hacking is a legal hacking that is bound by the rules, if the rules are denied, then the hacker must pay a high price in the form of penalties that can be either monetary or otherwise) that are being scanned, owned by the system, the zombie system as well as the removal of evidence. These are some of the phases that hackers are taking to bypass the user's device[1]. Figure 1 shows a hacker and his elements used for hacking.

Fig.1: Hacker and His Elements Used For Hacking

Background of Security:

Computer security is the protection of the computer system and the data stored and accessed by users.[1] Computer Security enables the university to perform its stress-free mission by:

1. Enabling people to work, Research, Education
2. To support the critical business process.
3. Protecting personal and sensitive information

Cyber attacks or incidents have increased rapidly to address the current environment, and advisory organizations are promoting a more proactive and adaptive approach. It was 13,301 in 2011 and increased to 22,060 in 2012 and increased rapidly to 3,000,000 in 2015. The National Institute of Standards and Technology (NIST) recently issued updated guidance in its risk assessment framework that recommended a shift to continuous monitoring and real-time assessments. Like worms, viruses and data breaches, they have grown rapidly in the last 25 years, increasing day by day according to the current scenario. It has been a difficult task for cyber security vendors and law enforcement agencies to cope with these advances. Some of the initial security attacks are summarized below.[2]

The First Computer Worm (Late 1980s-Early 1990s):

Robert Morris was the creator of a worm known as the first computer worm. This virus has spread to a lot of people who make up a lot of loopholes. This virus has brought down the entire internet. It was the first widespread case of a denial of service (Dos) attack. The Morris worm attack led to the industry, including the CERT (Computer Emergency Response Teams). [3]

The First Viruses (1990s):

The first virus was called virus Melissa and virus ILOVEYOU. It makes 10 million contaminated computers. It blocks the email function entirely. These threats render the necessary antivirus sector more difficult to operate. When the virus is transmitted by corporate communications, the organization may be challenged and could be put into the public eye.[4]

Credit Cards under Attack:

It Took Place in the Years 2005 and 2007. Albert Gonzalez Stole The Details From 45.7 Million Payment Cards Used By TJMAXX, Tkmaxx Outlets Owned By US Customers. There Was A Significant Breach Of Security That Cost Some $256 Million. The Data Involved In Breaches Have Been Monitored, And Accidents Allow Authorities And Funds To Be Notified.[5]

Hackers:

A Hacker Is A Person Who Uses His Technological Skills To Perform The Task With The Aid Of Computer And Network. Hacker Is A Person Who Makes Use Of His Or Her Efforts To Obtain Unauthorized Access To Systems And Networks To Commit Cyber Crime. He May Steal All Important Information, Such As All Bank Accounts, All Personal Information, And Use It To Cheat The Victim And Ask For Ransom Wares To Return Data..[6]

Advantages of Ethical Hacking:

Most of the advantages and profits of ethical hacking are cleared, but many of them are taken lightly. Some of which can be summarized as following:

- Prevention against cyber theft - Fighting against terrorist attacks such as stealing and frauds.

- Protection against cyber terrorism - Preventing malicious hackers from gaining access.

- Protection against data breaches - Prevents leaking of sensitive information that is not authorized to have access to it. [7]

- Role of government bodies increases - It is very beneficial for the government bodies for security of their systems as it can lead to leak or spread their private data to world.

- Helps in understating importance of security - It gives vital information to many of the people who are still unaware of the security concerns.

- Increases knowledge - Ultimately it is creating a better learning scenario for institutions, business and personal talking about security.

- Helps in experimenting things - Testing your own computer and network security if gained deep knowledge about it.

- Protection to services and marketing - Provides security to banking and financial infrastructures.

Disadvantages of Ethical Hacking:

Though it doesn’t have any disadvantages but sometimes it leads to failures and faults which can be exploited as –

• Data breach - It may lead to harm personal privacy and sensitive information.

• Cyber contraband –Threatening persons with fear for their lives or their lives of families for money.

• System failure and errors- This may lead to corruption of systems if not properly done.

• Malicious activities - Ethical hackers sometimes can use the data for malicious and harmful purposes. • Lacking reliability- One of the main constraints related to this is the trustworthiness of the ethical hacker.

• Expensive - Hiring ethical hackers can be expensive because of their specialized work and some areas of training they need.

• Hectic - It is very time consuming and frustrating to if someone has hacked your system.

• Unsure about data privacy - Can be used for unauthorized access to data and information. [7]

Classification of Hackers:

The Hackers can be classified as Black, White & Grey category which is discussed below

White Hat Hackers; White Hat Hackers are approved by the companies and paying guy, with good thought.

We work for others with positive intentions. They are also known as "IT Technicians" These are named to boost the enterprise. The companies use them to test their own security to verify and strengthen the quality of the security. They are making efforts on their loopholes, and strengthening security.

Black hat hackers: They are also known as crackers, or hackers of malice. We locate weak- banks or other businesses and steal money or credit card information. They crack all security and make network less secure and rob all valuable information. They have only one reason which is for money.

They do it sometimes for fun but they do not hurt any organization. White hat hacker sign is seen in the

Grey Hat Hackers: -Nothing is ever either black or white; the same is true in the hacking world. They are multi-talented, white and black hat hackers have property. Often, they find a loophole and break the security and notify the organization about the security loopholes for which they are getting remedies and money.[8]

Cyber Security Challenges:

Data breaches - Large amount of data is stored on cloud servers hence it becomes an easy target for attackers to control over unauthorized and sensitive data. Cloud providers deploy security controls to protect their environments, but ultimately organizations are responsible for protecting their own data in the cloud. Compromised credentials and broken authentication - Data breaches and other attacks frequently result from.[9]

• Weak passwords, and poor key or certificate management. Hacked interfaces and APIs - APIs and interfaces is one of the most exposed systems because they’re usually

• Accessible from the open Internet. Risk increases due weak interfaces and APIs which expose organizations to security issues related to confidentiality, integrity, availability, and accountability. Exploited system vulnerabilities - System vulnerabilities have become a big problem due to wide use of cloud

- Computing: Organizations share memory, databases, and other resources with each other, creating new attack platforms. Account hijacking - Phishing, fraud, software exploits have become very common now due to the fact that

- Information is stored in cloud storage and attackers can spy on activities, manipulate transactions, and modify data. Malicious insiders - In a cloud scenario, an insider can destroy whole infrastructures or manipulate data

- Systems that depend totally on the cloud service provider for security, such as encryption, are at greatest risk Permanent data loss - The permanent data loss due to provider error have become extremely rare.[10]

- Malicious hackers have been known to permanently delete cloud data to harm businesses. Shared technology, shared dangers -. Cloud service providers share infrastructure, platforms, and applications,

- If a vulnerability arises in any of these layers, it affects everyone.

CONCLUSION

However, it does not have sufficient breadth because many businesses wanted their customers as developers, programmers or event managers, but those people who belong to or want to enter this area are paying pretty much money, It includes –it's an new branch and no ethical hacker can be sure of using the same technology over and over again, and people decided to learn and study more about this technology as a result. As e-commerce sites 'rising demands, many e-commerce marketing companies like Flipkart, Amazon and EBay will demand more from ethical hackers due to their security concerns, many businesses.

REFERENCES

[1] J. Bohannon, "The life hacker," *Science*. 2011.

[2] "Hackers — Heroes of the computer revolution," *Comput. Law Secur. Rev.*, 1986.

[3] G. Coleman, "Hacker politics and publics," *Public Cult.*, 2011.

[4] H. Cavusoglu, S. Raghunathan, and W. T. Yue, "Decision-Theoretic and game-theoretic approaches to IT security investment," *J. Manag. Inf. Syst.*, 2008.

[5] D. Hacker, "Operations Management," *ICL Tech. J.*, 1991.

[6] C. Stoll, "Stalking the wily hacker," *Commun. ACM*, 1988.

[7] G. Häcker, "The morphology of apoptosis," *Cell and Tissue Research*. 2000.

[8] S. Pfohl, "A Hacker Manifesto," *Contemp. Sociol. A J. Rev.*, 2005.

[9] "Neuroscience and philosophy: brain, mind, and language," *Choice Rev. Online*, 2008.

[10] C. C. Palmer, "Ethical hacking," *IBM Syst. J.*, 2001.