Ethical Hacking: An Introduction and Analysis

Amit Giri, Navpreet Kaur Walia
Student, Assistant Professor
Department of Computer Science and Engineering.
Chandigarh University, Gharuan
Mohali, Punjab-India

ABSTRACT:-

Today, we are living in Cyber world. And our security is concerned as a major problem. Our every data and information is on the internet and there are many people who are interested in interacting with data. Some do for gaining knowledge that how to destroy data without the knowledge of the owner and some do for the requirement purposes. In the growing era of internet, computer security is the outmost concern for the organization and government. But at the same time, data and network security is the serious issue that has to be talked about. In this paper, we are going to discuss about the Hackers(people who can interact with data without the knowledge of owner) and how their intentions differentiate them in categories. We are also going to review about how it works and some of the law and rules for hacking and cybercrime.

Keywords:-vulnerabilities, malicious, DNS.

INTRODUCTION:-

Digital security is the most discussed point and the most concerned region in the present online world. Security is the significant reality in the present region where web implants is extremely tremendous and quickly developing. Each association has issues identified with security about their delicate and secret information. This is a result of hacking. Moral hacking does flawlessly fit into the security life cycle (see Fig 1)[5]. Moral hacking is a method for completing a security appraisal – a present circumstance (from a specialized perspective) can be checked. Like every other evaluation (or reviews), a moral hack is an arbitrary example and passing a moral hack doesn't mean there are no security issues. The data, for example, charge card numbers ,phone numbers, places of residence, ledger numbers and so on that are accessible on system may effortlessly be hacked by unsocial components. This is a direct result of the expanding prevalence and utilization of PCs, access to them was restricted to approved or concerned work force. Be that as it may, when a few clients were declined to get to the PC, they would think about it literally, and would challenge the entrance controls. They would take passwords and other data by encroaching into the framework to take control of the whole framework. They would do such things just to fulfill their inner self of not been given the control to get to the framework, or only for the sake of entertainment, or for cash.

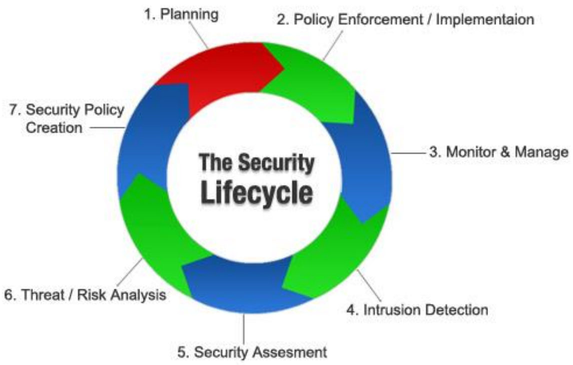


Figure 1:- security life cycle

●WHAT IS HACKING?

Hacking is an activity in which a person exploits the vulnerabilities in a system,which allows the hackers to gain access in the network or into the system. After taking control of network or system, hackers can do anything they want to do(depend upon their intentions). He is a computer enthusiast and extremely proficient in programming languages, computer systems and networks. It is the hackers who built Internet and make www to work. The operating system UNIX is a gift from hackers too. [2]

●WHO ARE THEHACKERS:-

Hackers is a person who hacks into a system or takes unauthorized access of system and steel/destroy data or report the vulnerabilities of systems to the organization.It is depends upon which type of hacker they are.[2]

There are three types of hacker.Which are following:-

1. **BLACK HAT HACKERS:-** A Black hat hackers are those hackers who hacked into an organization and steel or destroy their confidential data. We can also say that the intentions of black hat hackers are to harm organization. They are **Malicious hackers.**

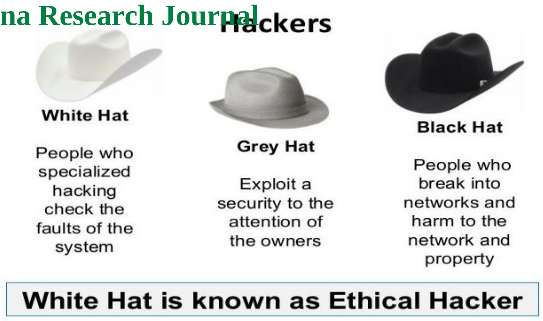

Hackers
White Hat
People who specialized hacking check the faults of the system
Grey Hat
Exploit a security to the attention of the owners
Black Hat
People who break into networks and harm to the network and property
White Hat is known as Ethical Hacker

Figure 2:- types of hackers

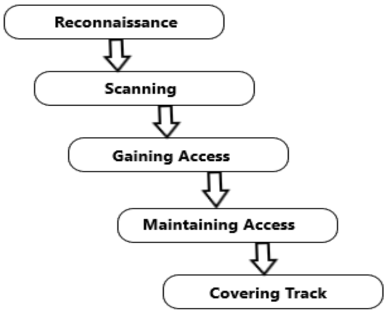
2. **WHITE HAT HACKERS:-**White Hat Hackers are authorized and paid person by the companies, with good intends and moral standing. White hat hackers are also known as **Ethical hackers.**
3. **GREY HAT HACKERS:-**AGrey Hat may breach the organizations’’ computer security,, and may exploit and deface it. But usually they make changes in the existing programs that can be repaired. It is themselves who inform the administrator about the company’s security loopholes. They hack or gain unauthorized entry in the network just for fun and not with an intension to harm the Organizations.

HACKING METHODOLOGY:-

In hacking, there is no specific step by step methodology used by all hackers, a typical hacking process comprises of the following phases:[3]

Figure 3:- phases of hacking

Phase 1
RECONNAISSANCE:-



Before performing any hacking method, a hacker has to get information as much as possible about victim. The first phase, reconnaissance also known as foot-printing, hacker collects the information about their targets from any sources for example through Google hacking database, shodan etc.Hackers move to the next step after gaining information.

Phase 2

SCANNING:-

Scanning is the second step of hacking. It is a procedure of identifying live hosts, ports, services and discovering operating system and architecture of the victim. After this hacker identify the vulnerabilities and threats in victim’s system or network.
It also refers that the advance reconnaissance techniques.

Phase 3
GAINING ACCESS:-

After scanning the victim’s system or network, hacker try to gain access of the victim’s system by using some kind of hacking methods. The malicious gain of access is the first point upon which legality truly comes into play. Attempting to crack the password to a system or support denial of service can be lead to fine or even imprisonment.

Phase 4
MAINTAINING ACCESS:-

While gaining access of a victim’s system, hacker should have to maintain the access to a system as much as possible.

Phase 5
COVERING TRACKS:-

Covering or clearing the track is the last step of hacking in which hacker clear all the logs and records that are generated by unauthorized access in the victim’s system which could be the cause of the hacker get caught by the security administrator.

INFORMATION SECURITY:-

An ethical hacker has to know that how to secure their organization’s data if someone Trying to steal those data and secure the organization. This is the one of those things that an ethical hacker is supposed to do in an organization. While taking care of the data of the organization, the ethical hacker takes the CIA triad keep in their mind. Basically the CIA triad is consisting of confidentiality, integrity and availability.CIA triad is a basic concept of hacking. These are the security conditions of cyber security and data security. It is also known as core principle of information hacking.[3]

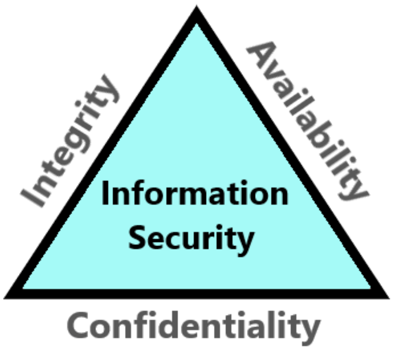


Figure 4:- CIA triad

CONFIDENTIALITY:-

Information has a value and confidentiality refers to keep the data private. Privacy of a data is must important as the other things in the organization. If the data of any organization compromised then the organization has to face the huge losses in finances and their reputation as well.

INTEGRITY:-

Integrity means that the system and the data or information in it have not been improperly altered or changed without authorization. It is the most subtle but most important part of the information security. It is the second pillar of the cyber security.

AVAILABILITY:-

Availability means being able to use the system as anticipated. It becomes a security issue when and if someone tries to exploit the lack of availability in some way.

TESTING STRATERGIES:-

Basically there are three types of testing strategies which is used by hackers to perform any attack on the organization. These three testing are the followings:

1. Internal testing strategy
2. External testing strategy
3. Blind testing strategy

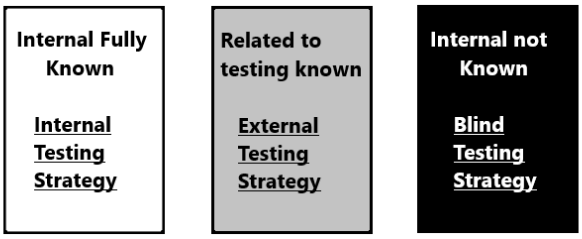


Figure 5:- testing strategies(test box)

INTERNAL TESTING STRATEGY:-It performed within the organization's technology environment. This test imitates the attack on the internal network by the discontented employee or an authorized visitor having standard access privilege. This test performed just to check whether the penetration of the network is possible or not. And if the penetration is possible in the network then how many things can attacker do on the network. This is also known as white box testing.[2]

EXTERNAL TESTING STRATEGY:-External refers to attack on the organization's network from outside the organization's system through internet or extranet. This test begins with publicly accessible information about client by network enumeration and targeting company's external visible servers such as DNS, email server, web server etc. This is also known as grey box testing.[2]

BLIND TESTING STRATEGY:-A blind testing strategy simulates the actions of a real hacker. The testing teams attempt the hacking with no information of the organization's system. The testing team uses publicly available information such as web sites to collect information and attempt hacking. This is also known as black box testing.[2]

There is one more testing strategy which is derived from blind testing strategy named as DOUBLE BLIND TESTING STRATEGY.

DOUBLE BLIND TESTING STRATEGY:-

In this testing, IT and security teams of organization do not informed before testing activities. It is an important part of testing which can test the organization's monitoring identification and response procedure.

CYBERCRIME AND HOW IT AFFECTS THE WORLD:-

Cybercrime is the crime which consists of computers and internet or network to steal and misuse the data of any person or organization.

Business loses billion dollars yearly as a result of hacking and other data breach. Many times, true cost cannot by evaluated because of security breach. Companies can lose consumer's confidence. The cost from recovering from an attack can spread quickly such as legal fees, investigating fees; reputation management etc. companies are spending more and more money to preventing the attack before it happens.

There is a survey from Norton by Symantec which describes the breach in security without the person's knowledge.

As indicated by NORTON inc. new and rising security dangers building up each day, much has been composed about online wrongdoing. This online review of 20,907 shoppers and 21 markets was authorized by Norton by Symantec to give a worldwide perspective of online wrongdoing and the toll it goes up against consumers.[4]

Key findings:[4]

44%
of consumers surveyed don't believe there are enough connected device users for them to be a worthwhile target for hackers.

Here are a couple of statistical data points from the 2016 Norton Cyber Security Insights Report that will change the manner in which you consider digital security.

- Forty percent of Millennial report having experienced cybercrime in the previous year.

- Nearly three of every 10 individuals can't identify a phishing assault.

- Another 13 percent need to figure be-tween a genuine message and a phishing email, which means four of every 10 are vulnera-ble.

- Eighty - six percent of individuals said they may have encountered a phishing inciimprint.

- 7 in 10 shoppers wish they could make their home Wi-Fi arrange more secure.

- Yet just 27 percent trust it is likely their home Wi-Fi system could be imperiled.

The Impact:[4]

Within the last year,
689 MILLION PEOPLE
in 21 countries experienced cybercrime.
In the 17 countries surveyed in both 2015 and 2016, we've seen a 10 percent increase since last year.

Within the past year, cybercrime victims have spent $126 billion globally and lost 19.7 hours – the time it would take to fly from New York City to Los Angeles four times – dealing with cybercrime.

All the cybercrime we know is done by the black hat hackers. There are some infamous techniques which are used to steal the data and misuse those data and harm them. All the cybercrime techniques are divided into many categories and there are five main categories of cybercrime:

1. Phishing
2. Ransomware
3. Malware
4. Identity Theft
5. Scams

PHISHING:-

Phishing is some kind of social engineering technique which consist of fake pages or mails etc. to obtain their sensitive data and information such as passwords credit card numbers etc.

RANSOMWARE:-

Ransomware is also called as cyber kidnapping which is malicious software or codes which encrypt the data and block the access of victim's data unless a ransom is paid to the hacker by the victim.

MALWARE:-

Malware is a malicious code or software that can be installed in the system the user's knowledge and allow the hacker to do anything inside the user's system. Virus, Worms, Trojan horses are the examples of the malware.

IDENTITY THEFT:-

Identity theft is the intentionally use of someone else's identity to obtain the credits and the other benefits in the other person's name. In the simple way, hacker pretends like another person to obtain their credits or harm the person's reputation.

SCAMS:-

Scam is a term used to describe any fraud business or scheme that takes money or other goods from the unsuspecting person. There are thousand types of scam such as call scam, phishing, donation scam, chain mail and online surveys.

ADVANTAGE OF ETHICAL HACKING:-

[1]The ethical hacking used to prevent malicious hacking to prevent national security breach. The main benefit of ethical hacking is to protect the organization and government from big financial loss and reputation loss as well. There are the following things that are hackers are used to do which are the advantages of ethical hacking:

- [1]Fighting against the terrorism and national security breaches.
- Having a computer system that prevents the malicious hacker to gain unauthorized access to the system of the organization.
- Testing and finding all the vulnerabilities of the system in the organization that can be used to break the security of the organization.
- [1]They have etiquette to follow the rule and regulations of the organization and their intensions are to protect organization.

LIMITATION OF THE ETHICAL HACKING:-

- The moral programmer utilizing the learning they gain to do pernicious hacking exercises.
- Permitting the organization's money related and managing an account points of interest to be seen.
- The likelihood that the moral programmer will send or potentially put malignant code, infections, malware and other ruinous and unsafe things on a PC framework.
- Enormous security rupture.

These are not common; however, they are something all companies should consider when using the services of an ethical hacker.

CONCLUSION:-

Hacking affects the world in both positive and negative way. The person who has the ability to hack or gain unauthorized access in a system and network without the user's knowledge could be helpful for making the better world and also they could destroy the world, it depends upon the hacker's intension which differentiates them into good hacker called white hat hackers and bad or malicious hacker called black hat hackers. The war between these two hackers will never end.The find out about additionally reveals that the legitimate customers are the moral hackers, till their intensions are clear in any other case they are an excellent threat, as they have the get right of entry to each and every piece of statistics of the organization.

This additionally concludes that hacking is an essential issue of technical world. It offers with each facets of being precise and bad. Ethical hacking plays a critical role in keeping and saving a lot of secret information, whereas malicious hacking can wreck everything. What all depends is the intension of the hacker. It is almost not possible to fill a hole between moral and malicious hacking as human idea cannot be conquered, but safety measures can be tighten.

REFERNCES:-

[1] Sumit Kumar, Nishant Sharma, Gagan Sharma **"Li-Fi Technology in Wireless Communication"** Published in International Journal of Trend in Research and Development (IJTRD), ISSN: 2394-9333, Volume-4 | Issue-3 , June 2017, URL: http://www.ijtrd.com/papers/IJTRD8584.pdf

[2] Kumari Neha et al. "Using Reconfigurable Directional Antenna in MANET." Procedia Computer Science 125 (2018): 194-200.

[3] Kumai, Neha, et al. "Mobile ad hoc networks and energy efficiency using directional antennas: A Review." *Intelligent Computing and Control Systems (ICICCS), 2017 International Conference on*. IEEE, 2017.

[4] Singh, VK, Kumar, R. "Multichannel MAC Scheme to DeliverReal-Time Safety Packets in Dense VANET". Procedia computerscience ISSN 1877-0509, 2018.

[5] S. Kapil et al, et al. "Analysing the Role of Risk Mitigation andMonitoring in Software Development (2018).