International Journal of Engineering Applied Sciences and Technology, 2021
Vol. 6, Issue 4, ISSN No. 2455-2143, Pages 379-383
Published Online August 2021 in IJEAST (http://www.ijeast.com)

A REVIEW ON OVERVIEW OF ETHICAL HACKING

Ms. Vaishnavi Bhagwat Savant
Student, Department of Computer Science and Engineering, Government Residential Women's Polytechnic Latur, Maharashtra, India

Ms. Rupali D. Kasar
Lecturer, Department of Computer Science and Engineering, Government Residential Women's Polytechnic Latur, Maharashtra, India

Ms. Priti B. Savant
SBSPM'S B Pharmacy College, Ambajogai-431517, Maharashtra, India

Abstract: The explosive growth of the Internet has brought many good things such as E-commerce-banking, E-mail, cloud computing, but there is also a dark side such as Hacking, Backdoors, Trapdoors etc. Hacking is the first big problem faced by Governments, companies, and private citizens around the world. Hacking means reading email's of someone, stealing passwords, stealing credit card numbers etc. An ethical hacker is one who can help the people who are suffered by this hackings. This paper describes about Ethical hackers, it's types and phases of hacking.

Keywords:- Hacker ,Cracker, Ethical hacking, hacking Phases.

I. INTRODUCTION

The internet has been one in every of our most transformative and fast-growing technologies. The vast growth of Internet has brought many of the nice things like electronic commerce, email, quick access to vast stores of reference material etc. More and more computers get connected to the web, wireless devices and networks are booming largely. due to the advance technology of the web, the govt., private industry and thus the everyday soul have fears of their data or private information being comprised by a criminal hacker. These forms of hackers are called black hat hackers who will secretly steal the organization's information and transmit it to the open internet. So, to beat from these major issues, another category of hackers came into existence and these hackers are termed as ethical hackers or white hat hackers. So, this paper describes the term hacking, then ethical hackers, their skills and their work in any organization, different phases of hacking etc. So, just in case of computer security, these tiger teams or ethical hackers would use the identical tricks and techniques that hacker use but during a legal manner which they'd neither damage the target systems nor steal information. Instead, they may evaluate the target system's security and report back to the owners with the vulnerabilities they found and directions for the thanks to remedy them. This paper will define ethical hacking, difference between hackers and crackers, provide a list of phases of hacking, different types of hackers and their work.

II. WHAT IS HACKING?

Hacking is the activity of recognizing weaknesses in a computer system or a network to exploit the security to gain access to personal data or business data. It states that an unauthorized access of another's computing system. Hacking refers to the abuse of devices like computers, smartphones, tablets and network to cause harm to or debase systems, steal data or disrupt data-related activities.

Difference between Hacker and Cracker :-

Table 1. Hacker and Cracker difference

Hackers	*Crackers*
A person who can hack for actual knowledge devotions.	A evil person who can halts into a organizations system for paybacks.
They are skilled and have a advance knowledge of computers OS and programming languages.	They may or may not be skilled persons, but some of the crackers just distinguishes a little trickeries to steal the data.
They work in an organisation to help protecting there data and giving them expertise on internet security.	These are the persons from which the hackers safeguard the organisations.
Hackers share the knowledge and never damages the data.	They can just erase the data, if they found any loop hole.
Hackers have legitimate credentials with them For Example : CEH certificates.	Crackers may or may not have certificates, as there purpose is to sojourn unspecified.

There are 3 types of Hackers :

- White Hat Hacker
- Black Hat Hacker
- Grey Hat Hacker

✓ ***White Hat Hacker :-***

This type of hackers is someone who has non-malicious purpose whenever he breaks into security systems. A large number of white hat hackers are security experts themselves, who want to push the boundaries of their own IT security ciphers and shields or even penetration testers specifically hired to test out how vulnerable or impenetrable (at the time) a present protective setup currently is.[1]

✓ ***Black Hat Hacker :-***

A Black hat hacker is also known as a “Cracker” is a computer hardware and software expert who breaks into the security of someone with malicious intent or bad intentions of stealing or damaging their important or secret information, comprising the security of big organizations, shutting down , or altering functions of websites and networks.[2] His malicious purpose can range from all sorts cybercrimes. Such as piracy, identity theft, credit card fraud, damage and so forth.

✓ ***Grey Hat Hacker :-***

The Grey Hat Hacker is a combination of White hat hacker and the Black hat hacker.[3]They sometimes access to data and the disrupts law, But they never have the same intention as like black hat hackers, they frequently work for collective good. The main difference is that they abuse vulnerability openly whereas white hat hackers do it privately for company. They are computer hackers, but they doesn't have any malicious intentions like other hackers(black hat hackers).

Ethical Hacking :

Ethical hacking is a licensed act of evading the system security or framework to detect probable data fissures and threats in an exceedingly network. An ethical hacker is additionally referred to as “white hat hacker". they're information security professionals who has the identical skills as sort of a hacker and that they can even uses the identical technologies as sort of a malicious hacker ("black hat hacker"). They define the vulnerabilities and weaknesses in an organization's systems. The main purpose of ethical hacking is to assess the safety of and identifying the vulnerabilities in target systems, networks or system organization. The process that involves is finding and so trying to take advantage of the vulnerabilities to work out whether unauthorized access or other malicious actions are probable. [4]

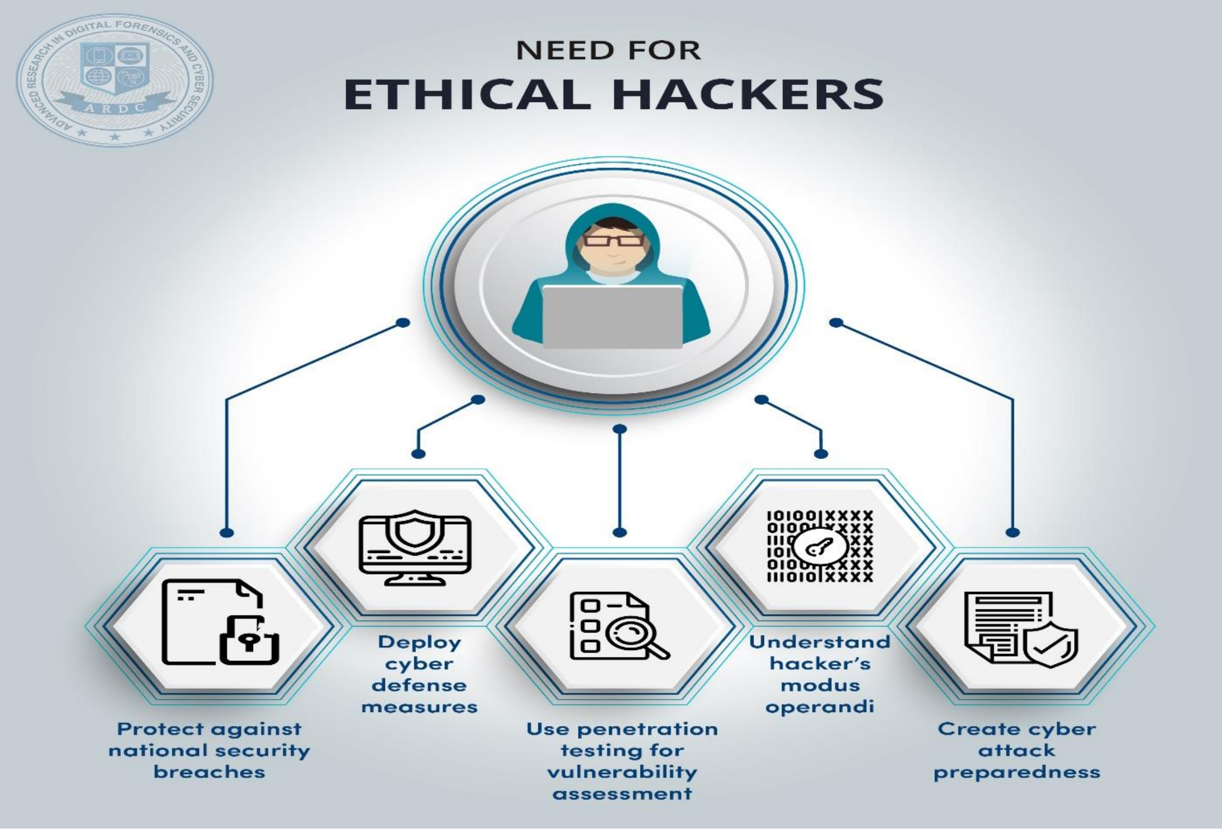
NEED FOR
ETHICAL HACKERS
Protect against national security breaches
Deploy cyber defense measures
Use penetration testing for vulnerability assessment
Understand hacker's modus operandi
Create cyber attack preparedness

Figure 1. Need for Ethical Hackers

Advantages of Hacking :

Following are some situations where Hacking is beneficial --

- To improve lost information, specifically in case if you lost your password.
- To implement penetration testing to fortify computer and network security.
- To put satisfactory preventative methods in place to prevent security breaches.
- To have a computer system that avoids malicious hackers from gaining access.

Disadvantages of Hacking :

If Hacking is done with the destructive intent, then it could be dangerous. It can effect

- Enormous security fissure.
- Unauthorized system access on the private/secretive information.
- Privacy destruction.
- Fettering system operation.
- Denial of service attacks.
- Malicious attack on the system/network.

Ethical Hacking steps :

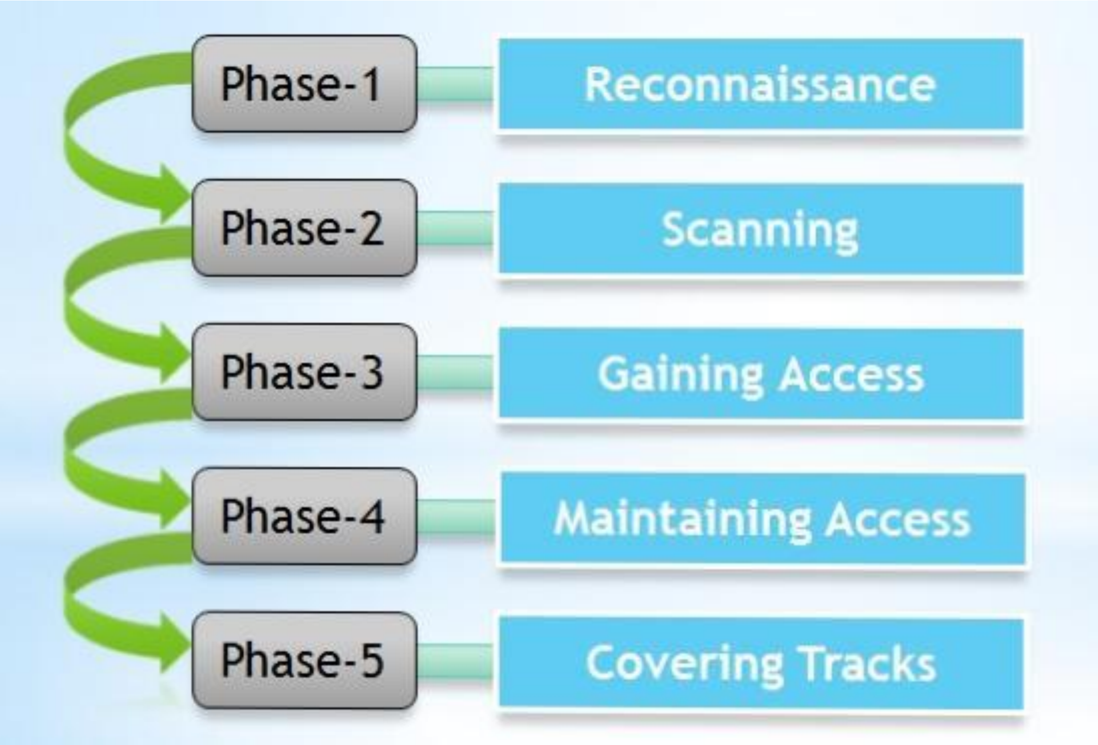

Figure 2. Phases of Ethical Hacking

There are Five Phases of hacking –

1. **Reconnaissance :**
   Process of reconnaissance will be categorized as Passive and Active Reconnaissance.

   1. ***Passive reconnaissance*** : Passive reconnaissance means gathering information without the targeted individual's or the company's knowledge of the targeted systems. Network sniffing is referred as passive reconnaissance and it may produce valuable information like IP address ranges, naming the conventions, hidden servers or networks, and other available services on the system.

   2. ***Active reconnaissance*** : It involves searching the network to get individual hosts, IP addresses, and services of the network. Active reconnaissance can provide a hacker a suggestion of security measures in situ, but the method also rises the possibility of being trapped or a minimum of floating apprehensive. [5]

2. **Scanning :**
   Scanning is a set of techniques for identifying the live hosts, ports, and services, determining the Operating system and the architecture of the target system, Detecting vulnerabilities and threats in the network. Scanning is also refers to collecting the additional information by using the complex and destructive reconnaissance techniques.
   Scanning is smashed to determine the weaknesses and faults of the service that will operate on the port. They must need to figure out the operating systems included live host,

firewalls, services, intrusion detection, routing & general networks topology [6] which are the parts of targets organization during the scanning phase.

3. **Gaining Access :**

   This is the phase where an attacker breaks into the system using various tools or procedures.[7] It is the main part of the hacking procedure where the information which is gathered in the previous two phases that is used to enter and the control of the target system over the network or physically. This phase is also known as "owning the system".

4. **Maintaining Access :**

   Once a hacker has gained access control to target computers, they expect to keep that access for future abuse and outbursts. Occasionally, hackers strengthen the system from the other hackers or the security personnel by securing their limited access with the backdoors, rootkits, and the Trojans.[8]

5. **Covering Tracks :**

   "Covering Tracks" is the last stage of a penetration test as a process. Once the hacker gains access, they cover their tracks to escape the security personnel. They can do this by clearing the cache and cookies, damaging the log files, and closing all the open ports.[9] This step is very important because it clears the system information making hacking a great deal rigid to track.

REFERENCES –

1. Mate M. Shital, Network and Information security book, Techknowledge Publication, ISBN : 978-93-89684-44-5.
2. Gupta Aman, Anand Abhineet, "Ethical Hacking and Hacking Attacks" IJECS Volume 6, Issue 4 April, 2017 , International Journal Of Engineering And Computer Science ISSN:2319-7242
3. Chowdappa Bala K., Lakshmi Subba S. P.N.V.S. Kumar Pavan, International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, "Ethical Hacking Techniques with Penetration Testing"
4. https://searchsecurity.techtarget.com
5. Vinitha K.P. , International Journal of Engineering and Research and Technology, ISSN : 2278-0181, NSDMCC-2015 Conference proceedings, volume 4, Issue 06.
6. Prabhat K.S , International Journal of Advanced Research in Engineering and Technology, volume 11, Issue 12, December 2020
7. https://www.greycampus.com
8. C.Nagarani , "Research paper on Ethical hacking and its value to security" , volume -4 , Issue 10, October 2015.
9. https://resources.infosecinstitute.com