International Journal For Technological Research In Engineering
Volume 8, Issue 4, December-2020 *ISSN (Online): 2347 - 4718*

ETHICAL HACKING

Aakash jethani[1], Ayush Saxena[2], Shubham[3], Mrs. Indu Khatri

[1,2,3]Students, [4]Assistant Professor(HOD)
Department of Computer Science Engineering
Bhagwan Mahaveer College Of Engineering And Management, Sonipat, India

ABSTRACT: -To present work is aimed to study the Ethical Hacking, types of Ethical Hacking, Hackers and what rules should they follow while doing it. So many people start learning hacking now-a-days for their good or bad intensions and how we can protect us from threats.

1. INTRODUCTION

Whenever you listens the word hacking, you probably associate it with sending an encrypted program to another user, and then being able to get unauthorized access i.e. taking any permission on a remote computer. However, the name hacking was basically used to define any act of tinkering a computer's hardware or software other than its intended use, in order to upgrade it and find out how electronic devices can work electronically.

Hackers	Crackers
Not illegal but depends upon in which manner people use it.	Mainly associated in stealing, breaking password, brute force accounts, reverse engineering.
Mainly focuses on exploiting vulnerabilities on target system to gaining access.	Cracking is crime because they are not taking permission
Hacking is legal as it involves taking permission on the first basic.	Illegal side of hacking.

2. TYPES OF HACKERS

1. White Hat Hackers
White hat hackers are well known as ethical hacker. Their intension is not to harm a system; rather they try to find out the weakness in a opponent computer or a network system as a part of penetration testing and vulnerability. It is not illegal.

2. Black Hat Hackers
They are also known as a cracker. They are those who hack in order to gain unauthorized, i.e. without taking permission, access to a system and harm its operation or steal sensitive information. They are always illegal bas they have bad intent which includes stealing corporate data, violating privacy, damaging the system etc.

3. Grey Hat Hackers
They are blend of both black and white hackers. They do it for their fun, they exploit a security weakness in a computer system or network without taking the owner's permission or knowledge.

Types of Attacks in Hacking

1. Non-Technical Attacks
Non-technical attacks basically it involve manipulating people to get their passwords, willingly or not. An example of this is by duping a co-worker to divulge passwords and usernames. Another form of non-technical attack is simply walking into another person's room booting the computer, and then gathering all the information that you need – yes it may sound like Tom Cruise and his mission impossible team, but in actuality, these non-technical attacks are a serious part of hacking tactics.

2. Attacks on an Operating System
Operating system attacks are one of the most frequent hacks performed per quota. Well, it's simply a numbers game. There are many computers out there and a lot of them don't even have high level protection. There are a lot of protections in many operating systems – even the newest ones around still have a few bugs that can be exploited. One of the way for operating system attacks is password hacking or hacking into encryption mechanisms. Some hackers are just want to hack other people's passwords just for the sheer thrill of it.

3. Attacks on Applications
Applications, especially the ones online and the ones that deal with connectivity, get a lot of attacks. Examples of which include web applications and email server software applications. Some of the attacks include spam mail. Spam mail can carry code that can hack into your computer system. Malware and malicious software are also another tool in the hands of a hacker when they try to attack pretty much everything, especially apps. These software programs include Trojan horses, worms, spyware and any more. A lot of these programs can gain entry into your computer system online and get access.

Ethical Hacking Tools
Hacking tools are applications designed to serve one or several specific purposes to hack/crack. These are used to make complex hacking procedures, easy-to-use and nowadays, also offer good GUI(Graphical User Interface) to

help beginners in Ethical Hacking.

There are numerous types of hacking tools: -

1) Vulnerability scanners
2) Port scanners
3) Web application scanners
4) Password cracking tools
5) Packet sniffers

3. PHASES OF HACKING

There are mainly 5 phases in hacking. Not necessarily a hacker has to follow the given bellow 5 steps in a sequential manner. It’s a stepwise process and when follow it get a better result.

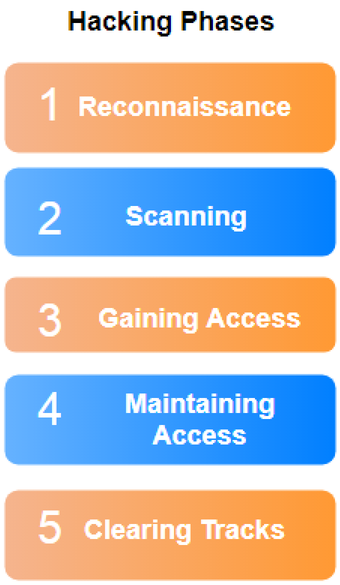

Fig 1

1. Reconnaissance:

This is the first step of Hacking. It is also commonly known as Foot printing and information gathering Phase. This is the preparatory phase where we get as much information as possible about the target. We usually collect information about three groups,

1. Network
2. Host
3. People involved

There are two types of Foot printing:

* Active: Directly interacting with the victim having aim to gather information about the target. E.g., Using Nmap tool to scan the target

* Passive: Trying to gather the information about the victim without directly accessing the target. This contains collecting information from social media, public websites etc.

2. Scanning:

Three types of scanning are involved:

* Port scanning: This phase involves scanning the victim for the information such as open ports, Live systems, various services running on the host.

* Vulnerability Scanning: Checking the victim for weaknesses or vulnerabilities which can be exploited. Usually done with help of automated tools

* Network Mapping: Finding the topology of network, routers, firewalls servers and host information and drawing a network diagram with the gathered information. This map may serve as a valuable piece of information throughout the hacking task.

3. Gaining Access:

This phase is where an attacker divides into the system/network using various tools or methods. After entering into a system, he has to increase his benefit to administrator level so he can install an application he needs or modify data or hide data.

4. Maintaining Access:

Hacker may just hack the system to show it was vulnerable or he can be so bad that he wants to maintain or persist the connection in the background without the knowledge of the user. This can be done using malicious files such as Trojans, Rootkits or many more. The goal is to maintain the access to the target until he finishes the tasks he planned to accomplish in that target.

5. Clearing Track:

No thief wants to get caught. An intelligent hacker always clears all proof so that in the future, no one will get any traces leading to him. It involves modifying/corrupting/deleting the values of Logs, modifying registry values and uninstalling all software that he used and deleting all folders that he created.

Benefits of Ethical Hacking:

1. Helps to maintain privacy and fully control.
2. Helps to find system flaws and thereby avoiding leaking sensitivity information to crackers.
3. Since, computers are getting accessible to more and more people, ethical hacking helps to maintain and strengthen computer security.

REFERENCES

1. https://www.greycampus.com/opencampus/ethical-hacking/phases-of-hacking
2. Patrick Engebretson : “The Basics of Hacking and Penetration Testing, Second Edition: Ethical Hacking and Penetration Testing Made Easy”.
3. WWW.UNSCHOOL.COM

Copyright 2020.All rights reserved.