ETHICAL HACKING

What is Hacking?

Hacking is the practice of modifying the features of a system, in order to accomplish a goal outside of the creator's original purpose. The person who is consistently engaging in hacking activities, and has accepted hacking as a lifestyle and philosophy of their choice, is called a hacker.

Computer hacking is the most popular form of hacking nowadays, especially in the field of computer security, but hacking exists in many other forms, such as phone hacking, brain hacking, etc. and it's not limited to either of them.

Due to the mass attention given to blackhat hackers from the media, the whole hacking term is often mistaken for any security related cybercrime. This damage the reputation of all hackers, and is very cruel and unfair to the law-abiding ones of them, from who the term itself originated. The goal of this website is to introduce people the true philosophy and ethics of hackers, hopefully clearing their name and giving them the social status they deserve.

Hacking may refer to:

- Computer hacking, including:

  1.Hacker culture, activity within the computer programmer subculture

  2.Security hacker, someone who breaches defenses in a computer system

  3.Cybercrime
- Phone hacking, gaining unauthorized access to phones
- Illegal taxicab operation
- Pleasure riding, horseback riding for purely recreational purposes
- Hacking (rugby), tripping an opposing player
- Hacking (falconry), the practice of raising falcons in captivity then later releasing into the wild
- Shin-kicking, an English martial art
- Joke thievery
- Hacking, an area within Hietzing, a municipal district of Vienna, Austria
- Roof and tunnel hacking, a type of urban exploration

Ethical Hacking

Ethical hacking is where a person hacks to find weaknesses in a system and then usually patches them.

Ethical hacking and ethical hacker are terms used to describe hacking performed by a company or individual to help identify potential threats on a computer or network. An ethical hacker attempts to bypass system security and search for any weak points that could be exploited by malicious

Reasons for Hacking

To make security strong:

Ethical Hacking is carried out to find the loop holes in the security of the system.

The system is hacked with the permission of the owner.

Fun event:

Some people hack a system just for fun to show off their hacking skills to others. This may prove risky sometimes as the hacker may fail to create a safe backdoor for him which may even prove dangerous to the person hacked the system.

To fetch vital information:

This are mostly the black hat hackers or crackers who enter into a system with an intension to harm the system security and to get all the confidential information from the system.

Qualities of an Hacker

Good knowledge of hardware and software:

A hacker should not only be aware of the of the software but also he/she should be well acquainted with the hardware to carry out hacking without getting caught.

Expert in coding:

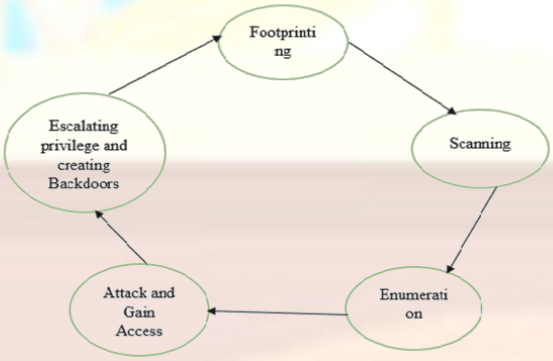
A hacker should know to operate multiple operating languages to understand various systems as every system as its own set of coding rules.

Total knowledge of the security system:

Before hacking any system the security given to the system to be hacked should be studied properly so as to fetch maximum data and decrease the risk of being caught.

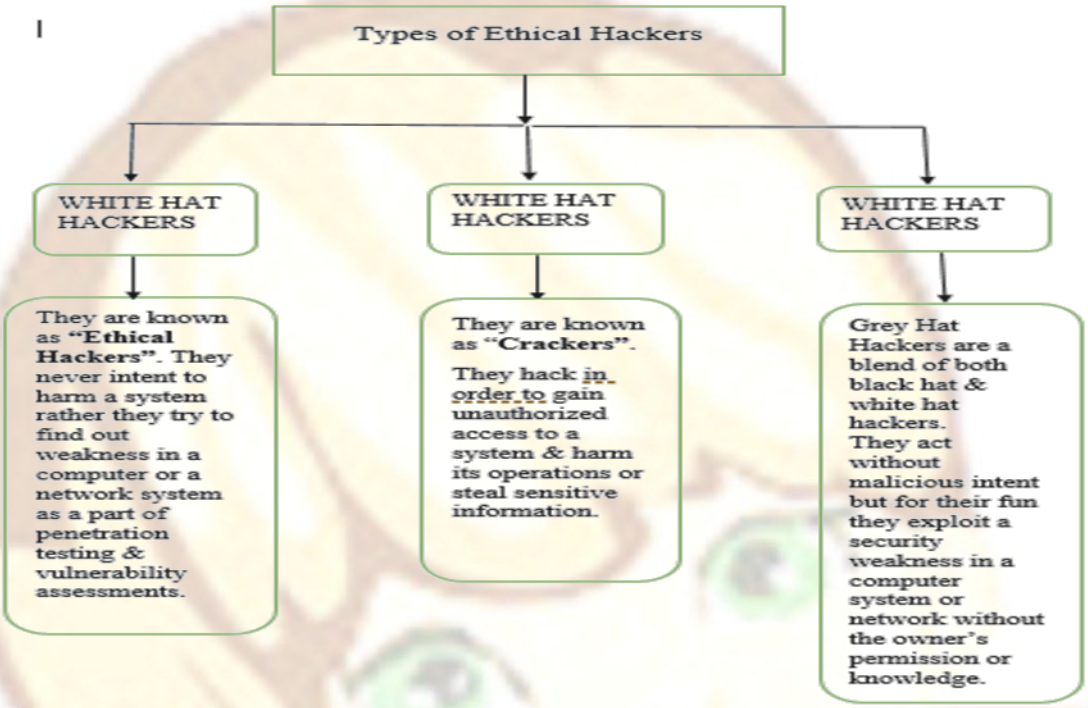
Trusted person:

An ethical hacker should be a trusted person as all the vital data is given of the system to a third person. An unfaithful



person can even use the data for personal benefits also.

ETHICAL HACKING



Footprinting:

Footprinting is a first step that a penetration tester used to evaluate the security of any IT infrastructure, footprinting means to gather the maximum information about the computer system or a network and about the devices that are attached to this network.

Scanning:

The second step of ethical hacking and penetration testing involve two terms that is scanning or port scanning. During this process the alive host, operating systems involved, firewalls, intrusion detection systems, servers/services, perimeter devices, routing and general network topology (physical layout of network), that are part of the target organisation are found out.

Enumeration:

Enumeration is the first attack on target network, enumeration is the process to gather the information about a target machine by actively connecting to it. Enumeration means to identify the user account, system account and admin account. Enumerating windows active directory to find out these stuffs.

Attack gain and access: Gaining Access refers to the true attack phase. The hacker exploits the system. The exploit can occur over a LAN, locally, Internet, offline, as a deception or theft. Examples include stack-based buffer overflows, denial of service, session hijacking, password filtering etc.

Tools used in Ethical Hacking

Footprinting- Who is, ping
Trace root, ns lookup
Scanning- nmap
nessus
Enumeration- Netcat, tcpdump
Telnet, firewalk

Advantages and Disadvantages

Advantages

Provides security to Banks & financial devices
Provides website defacement
Evolving Technique

Disadvantages

Vital information are also explored to outsiders
Expert hackers can prove to be expensive

Preventive measures

Path security hole option
Encrypt input data
Do not use unused daemon
Remove unused program
Setup loghost
Backup the system option

Pooja Tulaskar,
BE EXTC