International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 06 | June - 2022 Impact Factor: 7.185 ISSN: 2582-3930

The Basic of Hacking

SWATHI S[1] AND DR. SMITHA GOPAL[2]

Post Graduate Student, Department of M.C.A, Dayananda Sagar College Of Engineering, Bangalore, India Head of Department (HOD), Department of M.C.A,
Dayananda Sagar College Of Engineering, Bangalore, India

Abstract

One of the fastest growing areas in network security, certainly an area that generates much discussion is that of ethical hacking. Ethical Hacking known as "white hats," ethical hackers are security experts that perform these security assessments. The purpose of this paper is to describe the following things who are the hacker
and types of cyber hacker, what is ethical hacking, tools to carry out hacking,phishing and its technique.

Key words: - Hackers, Types of cyber hackers, 5 Phases, Ethical Hacking, Phishing

Introduction

The term hacking has been around for a quite long time now the first recorded instance of hacking dates back to the early 1960s in MIT where both the terms hacking and hacker coined since then hacking has evolved into a broadly followed discipline for the computing community.

Ethical hacking involves an legal permission to gain illegal access to a computer system, application, or data.

Ethical hacking is legally breaking into computer and devices to test an organization defenses from the hacker.

What is Hacking?

It is the art or technique of finding and exploiting the security loopholes in a system. This system can be software, website, computer, network or even a human being.

Hackers:-

Hacker is the person who is responsible for finding out the loopholes or crack the code for exploiting the information either legally or illegally.

Hacker can be classified into following groups

1. Black Hat Hackers
2. White Hat Hackers
3. Gray Hat Hackers
4. Miscellaneous Hackers

Black Hat Hackers:-

A black hat hackers is also known as unethical hacker or security cracker who uses and manipulates technology with vicious and often illegal intent. Black hat hacker are illegal who hacks the system software, website, computer, network with any authorized access for their personal gain.

White Hat Hackers:-

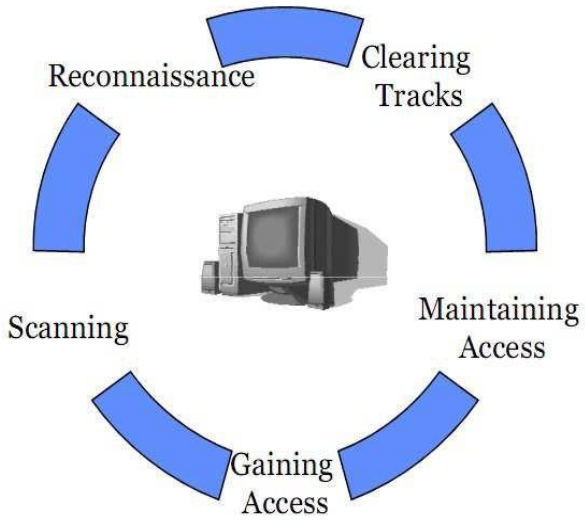
White hat Hackers are also known as Ethical Hackers or a Penetration Tester. White hat hackers are the good guys of the hacker world who protect the system or software from unethical hackers.

These people use the same technique and tools which is used by the black hat hackers. They also hack the system or software, but they can only hack the system with authorized access which means that should have permission to hack in order to test the security of the system. They mainly focus on security and protecting IT system from the threats. White hat hacking is legal.

Gray Hat Hackers:-

A Grey Hat Hacker is a combination of both white hat hacker and black hat hacker where they don't work for their own gain but sometimes they may be illegal does not have any malicious intentions.

The Phases used by Hacker to crack the code is as follows



Reconnaissance

The term reconnaissance stands for gathering the information which is used for find our target system.

Reconnaissance is the process of studying the behavior and integrity of the target which is willing to hack. Finally the hacker will be holding a enormous amount of information which will be very useful to track the which he wanted to hack.

We usually collect the information about three groups.

1. Network
2. Host
3. People involved

Reconnaissance involves two types namely

Active Reconnaissance: - In active reconnaissance you actually interact with the target directly to gain information to prop the target with bing request and analyze the traffic going back and forth from the target you also find the maximum request that target can handle at a time to find the denial of service liability.

Passive Reconnaissance: - In Passive Reconnaissance you don't interact directly with target to gain the information, you find other ways like internet.

Tools used in reconnaissance

Tool: Google
OS: Supported by all
Description: Google provides all the basic necessary information which will be very helpful for the user.

Tool: WhoisLookup
OS: Linux, Windows and Mac OS (using website, Fedora
Description: It is a query and response protocol i.e broadly used for quering database which stores the registered users or assignees of an internet resource such a domain name, ip address etc.

Tool: NSLookup
OS: Windows OS, Mac OS, Linux, Solaris
Description: NSLookup is an network administrative command line tool. It is used to check whether Domain name service(DNS) working properly on the computer system.

Scanning

Scanning refers to the premeditative phase when the attacker scans the network for specific information on the basis of the information which were gathered during the reconnaissance.

Three types of scanning namely

- Port Scanning
- Vulnerability Scanning
- Network Mapping

Tools used in scanning

Tool: Ping
OS: AIX, Linux, Windows, HPUX, Solaris, Mac OS, SunOS
Description: Ping stands for Packet internet groper which is a simple and broadly used utility tool to troubleshoot in the network or internet.

Tool: Tracert
OS: Mac OS, Windows, Linux, FreeBSD, Windows NT
Description: It is a network diagnostic command which display our route.

Tool: Nmap
OS: Linux, Micros oft Windows, OpenBSD, Solaris, IRIX, Mac OS X, HP-UX, Sun OS
Description: Nmap stands for network mapper it is one of the best open source tools used for scanning the network, with the help of nmap we can scan open ports and the services running on them including their version number.

Tool: Nikto
OS: Website Vulnerability Scanner AIX, Linux, Windows, HP-UX, Solaris, Mac OS, SunOS Nikto
Description: It is a open source free vulnerability scanner software which scans web servers for 6700 potentially dangerous files. It also captures any cookies received

Tool: Netcraft
OS: Ubuntu, Fedora, Solaris Netcraft

Gaining Access

Gaining access phase requires taking one or more network devices in order to either extract data from the target, or to use those device to launch the attacks on the targeted network. Gaining access such as password cracking, denial of service, session hijacking or buffer overflows etc.

Tools used for gaining access:

Tool: John the Ripper
OS: UNIX, Windows, DOS, Mac OS, OpenVMS John the Ripper,
Description: It is one of the oldest brute force password cracker.

Tool: Wireshark
OS: Linux, Mac OS, BSD, Solaris, Microsoft Windows.
Description: It is a open source network sniffing software, which was designed to track network packets and through the use of different filter options available in the software.

Tool: KonBoot
OS: Windows OS, Mac OS
Description: Linux, Mac OS, BSD, Solaris, Microsoft Windows.

Maintaining Access

Maintaining access phase is the point when an attacker is trying to maintain the access, ownership and control over the compromised systems.

In these phase, an attacker may steal the information by connecting the information to the

remote serve, download any file on the resident system, and manipulate the data and configuration.

Clearing Tracks

An attacker must hide his identity by covering the tracks such as disable auditing, clearing logs, modifying logs, registry files, removing all files, folders created etc.

Once you came to know hacking and shadow of the hacker there should be some of the techniques or method to secure the data or information from the malicious hacker, therefore the term **"Ethical Hacking", "Ethical Hacker"** came into existence in the industry.

Ethical Hacking

Ethical hacking is the branch of security where they secure the information from the malicious hacker. It is a type of hacking where an individual or the company, helps to find out the threats or loopholes in the network or computer system security for the organizations. The ethical hacking uses the same methodologies and techniques to protect their computer system or network's with authorized access in a legal manner.

Ethical Hacker

Ethical hacker are the professional hacker who hacks the system with an authorized access legally to check the system software. Whether the System is not attacked by threat or malicious hacker.

Phishing

Phishing is the technique of social attack which aims for gathering sensitive information of a target such as username, password, login information, credit card number, online banking pin number etc., by disguising as a trustworthy entity.

Conclusion

The entire world is moving with the new technology, which may increase the insecurity of the computer system or computer network. This paper describes the basic of hacking where the hacker tries to hack the system with the malicious intention in illegal manner to fulfill his personal needs. As hacking world has both good and bad hacker who uses same tools and technology to hack the system but their intention will be different. This paper also describes the what is hacking, who is hacker, types of cyber hacker, phases of hacking, Phishing etc. where as Ethical hacking is technique which is used the hack the system with the good intention for better understanding of the security of the computer system.

References: -

https://www.researchgate.net/publication/316431977_Ethical_Hacking_and_Hacking_Attacks

https://slideplayer.com/slide/3975562/

https://iaeme.com/MasterAdmin/Journal_uploads/IJARET/VOLUME_11_ISSUE_12/IJARET_11_12_018.pdf

http://wiki.cas.mcmaster.ca/index.php/Ethical_Hacking