CR Subscription Agency
Exploring and Distributing Knowledge Globally

Innovative Journal of Computer Technology
Volume 1 Issue 1

Tools and Techniques of Ethical Hacking

Deep Patel[1], Hetal Patel[2], Dharmendra Patel[3],
[1]Student, [2]Assistant Professor, [3]Professor
Smt.Chandaben Mohanbhai Patel Institute of Computer Applications,
CHARUSAT, Changa, Gujarat, India
****Corresponding Author***
Email Id: shailaja1234@rediffmail.com

ABSTRACT

As you all know, now a day's, people are searching online like activities for gathering of information, getting proper knowledge to learn things in a proper way. The information can be destroyed or steal of website without improper knowledge of the person. The purpose of this article is to give introduction about hacking, who are hackers and what is ethical hacking, etc. The various type of hackers, phases of hacking, and its tools and technique are discussed in the various parts of the paper including INJECTION attack SQL attack DOS attack

Key words: *Ethical Hacking, SQL Injection, Kali Linux*

INTRODUCTION

Ethical hacking is authorized practice of bypassing system security to identify potential data branches and threats in a network. The company that owns the system or network allows cyber security engineers to0 perform such activities in order to test the system defences. Thus, unlink malicious hacking. This process is planned approved and more importantly, legal.

There are two types of hacking: Legal hacking and illegal hacking. In the world, all most hackers are including in second type but few hackers are including in first type and it is call to ethical hacker and all country government are hired the ethical hackers and ethical hackers are register for USA in EC COUNSILING and they are all certified by CEH CERTIFIACT and certificate provide all legal permission.

Thee ethical hackers aim to investigate the system or network for weak points that malicious hackers can exploit or destroy. They collect and analyse the information to figure out ways to strengthen of the security of the system/network/application. By doing so, they can improve the security footprint so that it can better withstand attacks or divert them.

Ethical hackers are hired by organization to look into the vulnerabilities of their system and networks and develop solution to prevent data branches. Consider it a high tech permutation of the old saying" it takes a thief to catch a thief" [2].

Types of Hackers

Mainly three types of hacker are available. 1. Black hat hacker 2. White hat hacker 3. Grey hat hacker the white hat and grey hat hacker is also ethical hacker but black hat and another hacker are not call for ethical hacker it is call to illegal hacker [1].

Black Hat Hacker: This type of hacker is not worked for offensively. They believe in break the security they are work without any permission

White Hat Hacker: This type of hacker is work for defensively. They perform hacking and security checks with authority. They are known for security.

Grey Hat Hacker: This type of hacker is like for a coin they work for coin two sides offensively and defensively.

The other hacker is illegal hackers and these types of hacker is used to ready material and use google and this type is hacker is harmful for security level and human but this type of hackers is list out of illegal hacker. Below list are of illegal hackers:

1) Suicide hacker
2) Rootkits
3) Key loggers
4) Vulnerability Scanner
5) SQL Injection Attack
6) Distributed Denial-of-Service (DDoS)

1. Phase of Ethical Hacker

Reconnaissance: This is the first step of Hacking. It is also called as Foot prints and information gathering Phase. This is the preparatory phase where we collect as much information as possible about the target. We usually collect information about three groups, Network, Host and People involved

There are two types of Foot printing: Active and Passive. In active, directly interacting with the target to gather information about the target.

For example, using Nmap tool to scan the target. In passive, they are trying to collect the information about the target without directly accessing the target. This involves collecting information from social media, public websites etc.

Covering Tracks: No thief wants to get caught. An intelligent hacker always clears all evidence so that in the later point of time, no one will find any traces leading to him. This involves modifying/corrupting/deleting the values of Logs, modifying registry values and uninstalling all applications he used and deleting all folders he created.

Scanning: Three types of scanning are involved: Port scanning and Vulnerability Scanning. Port scanning: This phase involves scanning the target for the information like open ports, live systems, and various services running on the host.

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

Maintaining Access: Hacker may just hack the system to show it was vulnerable or he can be so mischievous that he wants to maintain or persist the connection in the background without the knowledge of the user. This can be done using Trojans, Rootkits or other malicious files. The aim is to maintain the access to the target until he finishes the tasks he planned to accomplish in that target.

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

All these phases are interdependent on each other as shown in below figure 1. Cyber Laws in India, when internet was developed, the founding fathers of Internet hardly had any inclination that Internet could transform itself into an all pervading revolution which could be misused for criminal activities and which required regulation. Today, there are many disturbing things happening in cyberspace.

Due to the anonymous nature of the internet, it is possible to engage into a variety of criminal activities with impunity and people with intelligence, have been grossly misusing this aspect of the Internet to perpetuate criminal activities in cyberspace. Hence the need

for cyber laws in India.(For more : http://www.cyberlawsindia.net/)

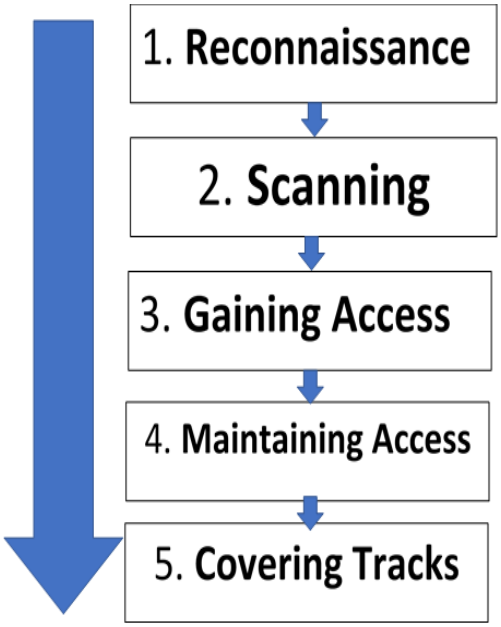

Fig. 1. Phases of Ethical Hacking Attack

TYPES OF ATTACK

The main types of attacks are categorised as Denial-of-service (DoS) and distributed, denial-of-service (DoS) attacks, cross-site scripting (XSS) attack and denial of service.

Injection Attack: In this type of attacks some data will be injected into a web application to manipulate the application and get required information. For instance, SQL injection code injection XML injection etc. The SQL injection is most common type of injection. In SQL, customized string will be passed to web application further manipulating query interpreter and gaining access to unauthorized information.

Cross site Scripting: This can be done by editing JavaScript in a webpage such that it will be executed in client browser. It can be classified as Reflected XSS attack, Stored XSS attack, DOM based XSS attack.

Denial of Service: DOS attack is an attempt to make a server or network resource unavailable to users. This is generally done by flooding the server with communication requests. DOS uses single system and single internet connection to attack a server. Distributed DOS uses multiple system and internet connection to flood a server with request making it harder to counteract. DOS can be classified as volume based attack, protocol attack and application layer attacks.

Important Ports and Protocol

This the Main Ports of Hackers used

1) TCP port 21 — FTP (File Transfer Protocol)
2) TCP port 22 — SSH (Secure Shell)
3) TCP port 23 — Telnet
4) TCP port 25 — SMTP (Simple Mail Transfer Protocol)
5) TCP and UDP port 53 — DNS (Domain Name System)
6) TCP port 443 — HTTP (Hypertext Transport Protocol) and HTTPS (HTTP over SSL)
7) TCP port 110 — POP3 (Post Office Protocol version 3)
8) TCP and UDP port 135 — Windows RPC
9) TCP and UDP ports 137–139 — Windows NetBIOS over TCP/IP
10) TCP port 1433 and UDP port 1434 — Microsoft SQL Server

Protocol is simply a set of rules which defines a standard way for exchanging information over a network. Protocol is available in 65535 ports are most used for hacker and ports support for theft the data for another users. And many protocol are used but main protocol is

1. TCP
2. IP
3. UDP

Transmission Control Protocol (TCP)

TCP is one of the core parts of IPS (internet protocol suite). Other one component is IP. TCP stands for Transmission control protocol. TCP provides the facility to exchange the

information or data directly between two hosts. Many major internet applications like e-mail, file transfer etc. rely upon TCP. This protocol contains variety of flags like SYN, ACK, RST, FIN etc.

Internet Protocol (IP)
Internet Protocol is other core part of IPS. IP is the main communication protocol with is used for exchanging packets over inter-network using IPS. IP is used to deliver packets from source to destination. Internet protocol is responsible for establishment of internet

User Datagram Protocol (UDP)
User datagram protocol (UDP) does not contain any flag. UDP allows computer application to send messages over internet protocol (IP). In UDP, data or messages are considered as DATAGRAM. UDP was designed by David P. Reed in 1980. In UDP, simple transmission model is used and there is no hand-shaking method is used which results into unreliability, duplication and missing of the information without notice. Data on the internet is generally organized into standard TCP or UDP packets. A packet is bunch of information. Different services use different ports to exchange the information. This is main type of ethical hacking protocol.

1. The Kali Linux: Useful tools and technique
There are several types of tools that come pre-installed. If you do not find a tool installed, simply download it and set it up. It's easy [3].

1. Nmap
Nmap "Network Mapper" is one of the most popular tools on Kali Linux for information gathering. In other words, to get insights about the host, its IP address, OS detection, and similar network security details (like the number of open ports and what they are).It also offers features for firewall evasion and spoofing

2. LYNIS
LYNIS is a powerful tool for security auditing, compliance testing, and system hardening. Of course, you can also utilize this for vulnerability detection and penetration testing as well. It will scan the system according to the components it detects. For example, if it detects Apache – it will run Apache-related tests for pin point information.

3. WP scan
WordPress is one of the best open source CMS and this would be the best free WordPress security auditing tool. It's free but not open source. If you want to know whether a WordPress blog is vulnerable in some way, WPScan is your friend. In addition, it also gives you details of the plugins active. Of course, a well-secured blog may not give you a lot of details, but it is still the best tool for WordPress security scans to find potential vulnerabilities.

4. Network Security
It is a collection of tools to assess WIFI network security. It isn't just limited to monitor and get insights – but it also includes the ability to compromise a network (WEP, WPA 1, and WPA 2 if you forgot the password of your own WIFI network – you can try using this to regain access.) It also includes a variety of wireless attacks with which you can target/monitor a WIFI network to enhance its security.

CONCLUSION
The whole world is moving to word the enrichment of technology, and more to more digital of the world, with the increase of this risk of security. This paper describe the working of types of hacker like malicious hacker (who tries to performing illegal activities), and on the other hand white hat hacker for an ethical hacker (who stop to do illegal breaks, maintain the security). Hacking perform a wide role in both the side good and bad. In

conclusion, it must be explained about ethical hacking is wide tool of proper utilise, it can be else in best fathom computer system and getting improvement and techniques as well.

REFERENCES

1) Hacking: Be A Hacker With Ethics Kindle Edition by Harsh Bothra
2) https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-ethical-hacking
3) http://www.speedguide.net/faq/what-is-the-typical-range-of-a-wireless-lan-330