Introduction to Ethical Hacking

Introduction to Ethical Hacking:

- Ethical hacking is to scan vulnerabilities and to find potential threats on a computer or network.
- An ethical hacker finds the weak points or loopholes in a computer, web application or network and reports them to the organization.
- Ethical hackers aim to investigate the system or network for weak points that malicious hackers can exploit or destroy.
- They can improve the security footprint to withstand attacks better or divert them.
- Ethical hackers aim to investigate the system or network for weak points that malicious hackers can exploit or destroy.
- They collect and analyze the information to figure out ways to strengthen the security of the system/network/applications.
- By doing so, they can improve the security footprint so that it can better withstand attacks or divert them.

Types of Hacking

We can define hacking into different categories, based on what is being hacked. These are as follows:

1. Network Hacking
2. Website Hacking
3. Computer Hacking
4. Password Hacking
5. Email Hacking

Network Hacking: Network hacking means gathering information about a network with the intent to harm the network system and hamper its operations using the various tools like Telnet, NS lookup, Ping, Tracert, etc.

Website hacking: Website hacking means taking unauthorized access over a web server, database and make a change in the information.

Computer hacking: Computer hacking means unauthorized access to the Computer and steals the information from PC like Computer ID and password by applying hacking methods.

Password hacking: Password hacking is the process of recovering secret passwords from data that has been already stored in the computer system.

Email hacking: Email hacking means unauthorized access on an Email account and using it without the owner's permission.

Goal/Importance of Ethical hacking

- In the existing industry, there are many jobs for ethical hacking. In the organization, to test the security systems, ethical hacking is really useful. Ethical hacking ensures that all the systems are secure and not vulnerable to black hat hackers. These days, there are a lot of hacking attacks. That's why the demand for ethical hackers is huge.
- We hear that attackers are hacked the big companies and big systems. Sometimes ago, a hacker hacked the Uber website. Due to this, the important information of around 50 million users was exposed. Many big companies like Google, Yahoo, Instagram, Facebook, Uber, they hire hackers. The hackers try to hack their systems. After hacking the system, they tell all the places where they found the weakness so that the company can fix it. Many companies also perform bug bounty programs. In this program, all the hackers around the world try to hack the website or web of that company. If the hacker finds any bug, the company will pay them a reward for the bug.
- Ethical hacking is used to secure important data from enemies. It works as a safeguard of your computer from blackmail by the people who want to exploit the vulnerability. Using ethical hacking, a company or organization can find out security vulnerability and risks.
- Governments use State-sponsored hacking to prevent intelligence information about influence politics, an enemy state, etc. Ethical hacking can ensure the safety of the nation by preventing cyber-terrorism and terrorist attacks.

- Hackers can think from an attacker's perspective and find the potential entry point and fix them before any attacks.
- Ethical hacking helps us learn new skills used in many roles like software developer, risk management, quality assurance tester, and network defender.
- In a company, the trained ethical hackers are the main strength. To ensure the functions of software aptly, ethical hackers can apply quick security tests under extreme and standard conditions.
- Ethical hackers develop many tools and methods and quality assurance tester to eliminate all the system's vulnerabilities.
- In an organization, ethical hacking can identify the weakness of your software security. Using the hacker's perspective, you can look at your security and fix any anomalies before making a problem in the company's success.

Types of Hackers:

Hackers can be classified into three different categories:

1. Black Hat Hacker
2. White Hat Hacker
3. Grey Hat Hacker

Black Hat Hacker

Black-hat Hackers are also known as an Unethical Hacker or a Security Cracker. These people hack the system illegally to steal money or to achieve their own illegal goals. They find banks or other companies with weak security and steal money or credit card information. They can also modify or destroy the data as well. Black hat hacking is illegal.

White Hat Hacker

White hat Hackers are also known as Ethical Hackers or a Penetration Tester. White hat hackers are the good guys of the hacker world.

These people use the same technique used by the black hat hackers. They also hack the system, but they can only hack the system that they have permission to hack in order to test the security of the system. They focus on security and protecting IT system. White hat hacking is legal.

Gray Hat Hacker

Gray hat Hackers are Hybrid between Black hat Hackers and White hat hackers. They can hack any system even if they don't have permission to test the security of the system but they will never steal money or damage the system.

In most cases, they tell the administrator of that system. But they are also illegal because they test the security of the system that they do not have permission to test. Grey hat hacking is sometimes acted legally and sometimes not.

5 Phases of Hacking

1. Reconnaissance: This is the first phase where the Hacker tries to collect information about the target. It may include Identifying the Target, finding out the target's IP Address Range, Network, DNS records, etc. Let's assume that an attacker is about to hack a websites' contacts.

He may do so by using a search engine like maltego, researching the target say a website (checking links, jobs, job titles, email, news, etc.), or a tool like HTTPTrack to download the entire website for later enumeration, the hacker is able to determine the following: Staff names, positions, and email addresses.

2. Scanning: This phase includes the usage of tools like dialers, port scanners, network mappers, sweepers, and vulnerability scanners to scan data. Hackers are now probably seeking any information that can help them perpetrate attacks such as computer names, IP addresses, and user accounts. Now that the hacker has some basic information, the hacker now moves to the next phase and begins to test the network for other avenues of attacks. The hacker decides to use a couple of methods for this end to help map the network (i.e. Kali Linux, Maltego and find an email to contact to see what email server is being used).

3. Gaining Access: In this phase, the hacker designs the blueprint of the network of the target with the help of data collected during Phase 1 and Phase 2. The hacker has finished enumerating and scanning the network and now decides that they have some options to gain access to the network.

4. Maintaining Access: Once a hacker has gained access, they want to keep that access for future exploitation and attacks. Once the hacker owns the system, they can use it as a base to launch additional attacks. In this case, the owned system is sometimes referred to as a zombie system**.** Now that the hacker has multiple e-mail accounts, the hacker begins to test the accounts on the domain. The hacker from this point creates a new administrator account for themselves based on the naming structure and tries and blends in. As a precaution, the hacker begins to look for and identify accounts that have not been used for a long time. The hacker assumes that these accounts are likely either forgotten or not used so they change the password and elevate privileges to an administrator as a secondary account in order to maintain access to the network.

5. Clearing Tracks (so no one can reach them): Prior to the attack, the attacker would change their MAC address and run the attacking machine through at least one VPN to help cover their identity. They will not deliver a direct attack or any scanning technique that would be deemed "noisy". Once access is gained and privileges have been escalated, the hacker seeks to cover their tracks. This includes clearing out Sent emails, clearing server logs, temp files, etc. The hacker will also look for indications of the email provider alerting the user or possible unauthorized logins under their account.

1.7 Rules of Ethical Hacking

The Ethical hackers have to follow some guideline or code of conduct that is given as follows :

Hacker Ethics

1. Early hackers developed a code of ethics, which has been adopted in large part by computer professionals today.
2. Code of ethics has evolved based on technological and societal changes.
3. Some hackers reject this code for a variety of reasons.

ACM Code of Ethics and Professional Conduct

1. Contribute to society and human well-being.
2. Avoid harm to others.
3. Be honest and trustworthy.
4. Be fair and take action not to discriminate.
5. Honour property rights including copyrights and patents.
6. Give proper credit for intellectual property.
7. Respect the privacy of others.
8. Honor confidentiality Know and respect existing laws pertaining to professional work.
9. Improve public understanding of computing and its consequences.
10. Access computing and communication resources only when authorized to do so.

11. All these rules highlight a need to obey the law, avoid harm, and respect others' privacy and property, but also to further knowledge and understanding.

Ten Commandments of Computer Ethics (CEI)

1. Do not use a computer to abuse and harm other people.
2. Do not interfere with other people's computer work.
3. Do not peep in around other people's computer files.
4. Do not use a computer for theft
5. Do not use a computer to convey false witness.
6. Do not use a duplicate copy of proprietary software for which you have not paid.
7. Do not use other people's computer resources without permission.
8. Do not appropriate other people's intellectual output.
9. Always think about the social importance of the program you are writing or the system you are designing.
10. Always use a computer in ways that assure consideration and respect for your companion humans.

Various Online Hacking Tools for Reconnaissance

Footprinting

Footprinting means gathering information about a target system that can be used to execute a successful cyber attack. To get this information, a hacker might use various methods with variant tools. This information is the first road for the hacker to crack a system.

There are two types of footprinting as following below.

- Active Footprinting: Active footprinting means performing footprinting by getting in direct touch with the target machine.
- Passive Footprinting: Passive footprinting means collecting information about a system located at a remote distance from the attacker.

Different kinds of information that can be gathered from Footprinting are as follows:

- The operating system of the target machine
- Firewall
- IP address
- Network map
- Security configurations of the target machine
- Email id, password
- Server configurations
- URLs
- VPN

Sources are as follows:

1. **Social Media**: Most people have the tendency to release most of their information online. Hackers use this sensitive information as a big deal. They may create a fake account for looking real to be added as friends or to follow someone's account for grabbing their information.
2. **JOB websites:** Organizations share some confidential data on many JOB websites like monsterindia.com. For example, a company posted on a website: "Job Opening for Lighttpd 2.0 Server Administrator". From this, information can be gathered that an organization uses the Lighttpd web server of version 2.0.
3. **Google**: Search engines such as Google have the ability to perform more powerful searches than one can think and one had gone through. It can be used by hackers and attackers to do something that has been termed Google hacking. Basic search techniques combined with advanced operators can do great damage. Server operators exist like "inurl:","allinurl:","filetype:", etc.
   For example, devices connected to the Internet can be found. A search string such as inurl: "ViewerFrame?Mode=" will find public web cameras. "The "link:" search operator that Google used to have, has been turned off by now (2017)".
   Google can be used to uncover many pieces of sensitive information that shouldn't be revealed. A term even exists for the people who blindly post this information on the internet, they are called "Google Dorks".
4. **Social Engineering**: There are various techniques that fall in this category. A few of them are:
5. **Eavesdropping**: The attacker tries to record the personal conversation of the target victim with someone that's being held over communication mediums like the Telephone.
6. **Shoulder Surfing**: In this technique, Attacker tries to catch the personal information like email id, password, etc; of the victim by looking over the victim's shoulder while the same is entering(typing/writing) his/her personal details for some work.

Advantages:

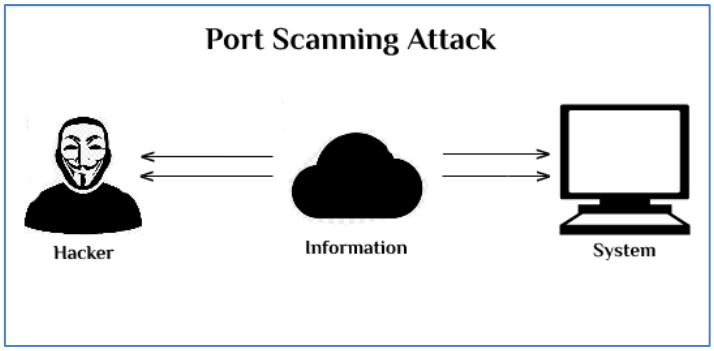
- Footprinting allows Hackers to gather the basic security configurations of a target machine along with network route and data flow.
- Once the attacker finds the vulnerabilities he/she focuses on a specific area of the target machine.
- It allows the hacker to identify as to which attack is handier to hack the target system.

Counter Measures:

- Avoid posting confidential data on social media websites.
- Avoid accepting unwanted friend requests on social media platforms.
- Promotion of education on various hacking tricks.
- Usage of footprinting techniques for identifying and removing sensitive information from social media platforms.
- Proper configuration of web servers to avoid loss of information about system configuration.

Scanning

- Scanning in ethical hacking is a network exploration technique used to identify the systems connected to an organization's network.
- It provides information about the accessible systems, services, and resources on a target system.
- Some may refer to this type of scan as an active scan because it can potentially disrupt services on those hosts that are susceptible.
- Scanning is often used during vulnerability assessment when probing weaknesses in existing defenses.
- Scanning is more than just port scanning, but it is a very important part of this process.
- Scanning allows you to identify open ports on the target system and can be used for port mapping, performing an interactive session with the operating system via those ports, or even redirecting traffic from these open ports. There are many tasks that can be performed with a scanning tool.



Types of Scanning Techniques:

1. **TCP connect scan**: This is a scan that sends TCP SYN packets to each port on the target system, waiting for an RST/ACK. This is a steal their type of scan because it does not show the open ports on the target system. The last port that responds is its open port, and you can use this to your advantage to determine which ports are open.
2. **TCP syn port scan**: This is a similar type of scan, but the packets are TCP SYN packets and not TCP ACK. This type of scan sends packets to ports that are open and waiting for a reply.
3. **Network Scanning**: Network scanning is used to identify the devices and services that are running on a target network, determine their operating systems and software versions, and identify any potential security risks or vulnerabilities. Network scanning can be performed manually or automated using software tools, and can target specific systems or an entire network.
4. **Vulnerability Scanning**: Vulnerability scanning is a process of identifying, locating, and assessing the security vulnerabilities of a computer system, network, or application. This process is performed using automated software tools that scan for known vulnerabilities, as well as weaknesses in the configuration or implementation of the system being tested.

Purpose

Scanning attacks are performed by cybercriminals or malicious actors for several reasons, including:

1. **Information Gathering:** The primary purpose of a scanning attack is to gather information about a target system or network. This information can be used to plan and execute a more sophisticated attack, such as a distributed denial of service (DDoS) attack or a data breach.
2. **Vulnerability Identification**: Scanning attacks can be used to identify vulnerabilities in a target system or network. These vulnerabilities can then be exploited to gain unauthorized access, steal sensitive information, or cause harm to the target.
3. **Network Mapping:** Scanning attacks can be used to map out a target network, including its infrastructure, servers, and devices. This information can be used to plan and execute a more sophisticated attack, such as a DDoS attack or a data breach.

Enumeration

Enumeration belongs to the first phase of Ethical Hacking, i.e., "Information Gathering". This is a process where the attacker establishes an active connection with the victim and try to discover as much attack vectors as possible, which can be used to exploit the systems further.

Enumeration can be used to gain information on −

- Network shares
- SNMP data, if they are not secured properly
- IP tables
- Usernames of different systems
- Passwords policies lists

Types Of Enumeration

1. NetBIOS(Network Basic Input Output System) Enumeration:

- NetBIOS name is an exceptional 16 ASCII character string used to distinguish the organization gadgets over TCP/IP, 15 characters are utilized for the gadget name and the sixteenth character is saved for the administration or name record type.
- Programmers utilize the NetBIOS enumeration to get a rundown of PCs that have a place with a specific domain, a rundown of offers on the individual hosts in the organization, and strategies and passwords.
- NetBIOS name goal isn't supported by Microsoft for Internet Protocol Version 6.

Nbtstat Utility:

- In Windows, it shows NetBIOS over TCP/IP (NetBT) convention insights, NetBIOS name tables for both the neighborhood and distant PCs, and the NetBIOS name reserve.
- This utility allows a resuscitate of the NetBIOS name cache and the names selected with Windows Internet Name Service. The sentence structure for Nbtstat:

nbtstat [-a RemoteName] [-A IPAddress] [-c] [-n] [-r] [-R] [-RR] [-s] [-S] [Interval]

2. SNMP(Simple Network Management Protocol) Enumeration:

- SNMP enumeration is a cycle of specifying client records and gadgets on an objective framework utilizing SNMP. SNMP comprises a manager and a specialist; specialists are inserted on each organization gadget, and the trough is introduced on a different PC.
- SNMP holds two passwords to get to and design the SNMP specialist from the administration station. Read Community String is public of course; permits review of gadget/framework setup. Read/Write people group string is private of course; permits far off altering of arrangement.
- Hackers utilize these default network strings to remove data about a gadget. Hackers list SNMP to remove data about organization assets, for example, has, switches, gadgets, shares, and so on, and network data, for example, ARP tables, directing tables, traffic, and so forth.

3. LDAP Enumeration:

- Lightweight Directory Access Protocol is an Internet Protocol for getting to dispersed registry administrations.
- Registry administrations may give any coordinated arrangement of records, regularly in a hierarchical and sensible structure, for example, a corporate email index.
- A customer starts an LDAP meeting by associating with a Directory System Agent on TCP port 389 and afterward sends an activity solicitation to the DSA.
- Data is sent between the customer and the worker utilizing Basic Encoding Rules.
- Programmer inquiries LDAP administration to assemble information such as substantial usernames, addresses, division subtleties, and so on that can be additionally used to perform assaults.

4. NTP Enumeration:

- Network Time Protocol is intended to synchronize clocks of arranged PCs.
- It utilizes UDP port 123 as its essential method for correspondence.
- NTP can check time to inside 10 milliseconds (1/100 seconds) over the public web.
- It can accomplish correctness of 200 microseconds or better in a neighborhood under ideal conditions.
- NTP enumeration tools are utilized to screen the working of SNTP and NTP workers present in the organization and furthermore help in the configuration and confirmation of availability from the time customer to the NTP workers.

5 SMTP Enumeration:

Mail frameworks ordinarily use SMTP with POP3 and IMAP that empowers clients to spare the messages in the worker letter drop and download them once in a while from the mainframe.

SMTP utilizes Mail Exchange (MX) workers to coordinate the mail through DNS. It runs on TCP port 25.

6.Unix/Linux User Enumeration:

One of the most vital steps for conducting an enumeration is to perform this kind of enumeration. This provides a list of users along with details like username, hostname, start date and time of each session, etc.

We can use command-line utilities to perform Linux user enumeration like users, rwho, finger, etc.

7. SMB Enumeration:

- Impair SMB convention on Web and DNS mainframes.
- Debilitate SMB convention web confronting mainframes.
- Handicap ports TCP 139 and TCP 445 utilized by the SMB convention.
- Restrict anonymous access through the RestrictNull Access parameter from the Windows Registry.

Difference between White-Hat, Black-Hat, and Gray-Hat Hackers:

S No.	White-Hat Hackers	Black-Hat Hackers	Gray-Hat Hackers
1.	White-Hat Hacking is done by White Hat Hackers.	Black-Hat Hacking is done by Black Hat Hackers.	Gray-Hat Hacking is done by Gray Hat Hackers.
2.	White-Hat Hackers are individual who finds vulnerabilities in computer networks.	Black-Hat Hackers are highly skilled individuals who hack a system illegally.	Gray-Hat Hackers work both Defensively and aggressively.
3.	White-Hat Hackers works for the organizations and government.	Black -Hat Hackers are criminals who violate computer security for their owner's personal gain.	Gray-Hat Hackers find issues in a system without the owner's permission.
4.	In some cases, white-hat hackers are paid, employees.	Black-Hat hackers make money by carding and selling information to other criminals.	Gray-Hat hackers find issues and report the owner, sometimes requesting a small amount of money to fix that issue.
5.	White-Hat Hacking is legal.	Black-Hat Hacking is illegal.	Sometimes Gray-Hat Hackers violate Laws.

Hacker	Cracker
The good people who hack for knowledge purposes.	The evil person who breaks into a system for benefits.
They are skilled and have advanced knowledge of computers OS and programming languages.	They may or may not be skilled, some crackers just know a few tricks to steal data.
They work in an organization to help protect their data and give them expertise in internet security.	These are the person from which hackers protect organizations.
Hackers share the knowledge and never damages the data.	If they found any loophole they just delete the data or damages the data.
Hackers are the ethical professionals.	Crackers are unethical and want to benefit themselves from illegal tasks.
Hackers program or hacks to check the integrity and vulnerability strength of a network.	Crackers do not make new tools but use someone else tools for their cause and harm the network.
Hackers have legal certificates with them e.g CEH certificates.	Crackers may or may not have certificates, as their motive is to stay anonymous.
They are known as White hats or saviors.	They are known as Black hats or evildoers

Tool :