Introduction to Ethical Hacking

What is Ethical Hacking?

Ethical Hacking is a process in which hackers get access to a network and system to identify potential threats. The individuals undertaking this process of ethical hacking refer to White Hackers. The term “white” comes here due to their positive intention to help organizations strengthen their security. The importance of ethical hacking doesn’t end here.

The countries are always alert about each other’s movements even in cyberspace. With even small conflicts, many use their intelligence team to hack into the country’s server for information.

The question of national security comes at stake in such cases. But ethical hacking can prevent such situations. They can make use of it to identify potential threats and avoid the compromise of important data.

The government recognizes the value of ethical hackers and even offers official certifications to them. For organizations, these hackers can perform regular audits and training to keep them on their toes. They can be in their security teams or at security consultant firms.

Is Ethical hacking the same as pen testing?

Many confuse ethical hacking with pen-testing.

Pen testing is a part of ethical hacking. A pen tester only identifies the potential threats by assessing the network or the system.

An ethical hacker also works on restoring security, managing cyberattacks, and taking over government projects. His job goes above the assessment and audits. All sorts of hacking done with a positive intention and under the regulation will be ethical hacking.

Origins of Ethical Hacking

The term ethical hacking was a creation by IBM executive John Patrick in 1990. The concept and application of the process were known but a term to define it did not exist before this. When hacking became relevant in the 1960s, it was more like a compliment for great computing skills.

But soon, it became a negative association due to increasing crime rates. By the 1980s many movies came out based on the concept of hacking, making it a mass term. By 2000, commercialization of hacking had begun making a career opportunity for many.

What do ethical hackers do?

1. The first and the most most important job of an ethical hacker is to **find vulnerabilities**. They help organizations come up with effective measures to overcome these problems. They evaluate every point in the security closely and then advise on its improvement.

2. They demonstrate how cybercriminals think and will attack the organization. They take companies through stages of hacking and how it will impact their work. The companies gather knowledge of their techniques and tools and get an upper hand in the process.

3. The previous two points allow companies to prepare for potential threats. Even after securing the network, the hackers may manage to break in. Having the audit report can help them identify them and stop the attack before it’s too late.

Benefits of Ethical Hacking

- Prevent data compromise and misuse
- Discover vulnerabilities and fix them
- Implement a secure network plan
- Defend national security from terrorists
- Gain customer trust by protecting their data
- Help in network protection from assessments

Types of Ethical Hacking

- Web application hacking
- Social engineering
- System hacking
- Hacking wireless networks
- Web server hacking

Primary Types of Hackers

1. White Hat Hackers

These hackers hold certifications in this field and assist these entities in strengthening their cybersecurity.

2. Black Hat Hackers

These hackers break into the networks without authorization with the wrong intention.

3. Gray Hat Hackers

These hackers don’t hold an authorized certificate and are driven by monetary gains.

Ethical Hacker Roles and Responsibilities

1. Get authorization from the company before performing the audit.
2. Follow the legal guidelines while following the hacking process.
3. Define the objective behind the attack to respect the boundaries.
4. Report vulnerabilities to the company with relevant suggestions.
5. Respect the non-disclosure agreement to avoid lawsuits.
6. Leave zero traces behind to avoid misuse by real hackers.

Phases of Ethical Hacking

1. Reconnaissance

The first step of the process is to gather information about the organization or company. This is like preparing thoroughly for the attack. The data is mainly about the employees, passwords, and other important credentials.

They use tools like HTTPTrack and Maltego to gather this information from the web. It is the planning stage to decide the types of attack the organization will most likely fall for. Some key points in it are –

- TCP and UDP services
- Vulnerabilities
- Through specific IP addresses
- Host of a network

The collecting process is either active or passive. In Active footprinting, they collect information directly using Nmap tools to scan the network. In the case of passive, they collect data indirectly from social media accounts, public websites, etc.

2. Scanning

The second step is to scan the information collected in the initial stage. The hacker will go through user accounts, credentials, IP addresses, etc to find the quickest way of hacking in. They use tools like dialers, port scanners, network mappers, etc. to do this step. Different types of scanning are –

a. Vulnerability Scanning – the hackers target weak points of the company to exploit them. Automatic tools like Netsparker and Nmap are useful in this type.

b. Port Scanning – the hackers try to find open ports in the network to enter and exploit the systems. They use port scanners and dialers to identify open TCP and UDP ports.

c. Network Scanning – the hackers identify active devices on a network to exploit them. This is to see if there are any potential threats and open

doors.

3. Gaining Access

This step is where the implementation of the plan takes place. Hackers gain access to the target's systems, applications, or networks using the relevant information on them. The tools and techniques differ according to the hacker's comfort and expertise.

They will try to exploit the identified vulnerability and give a real attack feel to the company. They can even experiment by testing the employees with phishing techniques to identify user behavior.

4. Maintaining Access

Getting into the system is easy for most hackers, but maintaining access is tough. Hackers don't even waste a second to get information and data and try to maintain that access. This can be either by launching attacks every second or by a denial of service attack.

The idea is to make full use of information in a limited time before the user finds out. This stage allows companies to find out the root cause of their weak network. Some common weaknesses are –

- Injection attacks
- Broken authentication
- Security misconfigurations
- Sensitive data exposure

5. Clearing Track

The last step for the hackers is to clear their track, making it difficult for anyone to trace. They ensure not to leave any hint behind and avoid identification. They edit, corrupt, or delete logs of their entry and activities. Even they leave the file distribution and sequence the same way to avoid suspicion. A few ways to do it are –

- Use reverse HTTP Shells

- Delete digital footprint
- UseInternet Control Message Protocol Tunnels

Skills of an Ethical Hacker

- Programming knowledge is necessary to get access and identify which attack will work according to software.
- Scripting knowledge is crucial to deal in network-based security audits.
- Networking skills to identify threats coming from devices present in the network.
- Database management to see hackers can potentially take over the important data.
- Understanding of platforms like Windows, Linux, Unix, etc.
- Basic knowledge of hacking tools available.
- Understanding of different search engines and servers.

Ethical Hacking Certifications

1. CND: Certified Network Defender

This program is to train network administrators to protect and respond to network threats. The course has activities to try major network security tools and techniques. They get to experience real-world network security technologies through this course.

2. CEH: Certified Ethical Hacker

This course allows individuals to get knowledge on ethical hacking from a vendor-neutral perspective. It is the most well-known course that people go for in the world. It has details about 20 of the most current security domains in the information security organization. CEH practical and CEH masters are extensions of this course which have ore intensive training for the subject.

3. C|TIA: Certified Threat Intelligence Analyst

It is a collaboration between cybersecurity and threat intelligence experts. The course trains individuals to identify and overcome business risks by changing unknown threats into known threats. The program is quite extensive and teaches how to create effective threat intelligence.

4. ECSA: EC-Council Certified Security Analyst

This program is like an advanced version of CEH. It has more comprehensive methodologies that ethical hackers need to know. To get more practical knowledge, individuals can also go for ECSA Practical where they can learn about the discipline more extensively.

5. LPT (Master): Licensed Penetration Tester (Master)

This course is famous for providing individuals with challenges to experience real-time situations. It has three levels with a multilayered structure allowing them to use their skills smartly. The idea is to put them under pressure for better understanding.

6. SANS GPEN

GPEN is one of the most famous courses that SANS offers for pen testing knowledge. The individuals get in-hand experience by using different pen testing tools throughout the course. The course ends with an exam to validate their learning.

7. Offensive Security Certified Professional

This course allows individuals to get 30 days access to lab and full pen testing training with Kali Linux. There are no certain criteria to enroll but it is advisable to have a basic understanding of how Linux works.

8. Foundstone Ultimate Hacking

It is a course by McAfee that allows beginners to learn about pen-testing. The course is known for teaching about ultimate hacking on Windows, Linux, Solaris, etc. This course doesn’t have an examination at the end.

9. CREST

This is a well-known examination that individuals undertake to validate their pen testing knowledge. There are two papers for web and infrastructure pen testers. They receive a certificate after passing the examination and then can practice officially.

Ethical Hacking Jobs

The ethical hacker certification can definitely guarantee a good job to individuals. The three major areas where they can ether are –

1. Pen testing and security audits are part of the ethical hacking toolkit in all organizations. They can be part of this process and assist companies in having a stronger toolkit by contributing their knowledge.

2. They can also provide service as freelancers to different organizations. They can approach them by showing their skills to senior management. The management is always interested in how these activities can affect their organizations.

3. They can work as risk managers in the companies. They will not only perform regular audits but also increase the team's efficiency. Also, they will assess everything inside the organization and identify potential threats from them.

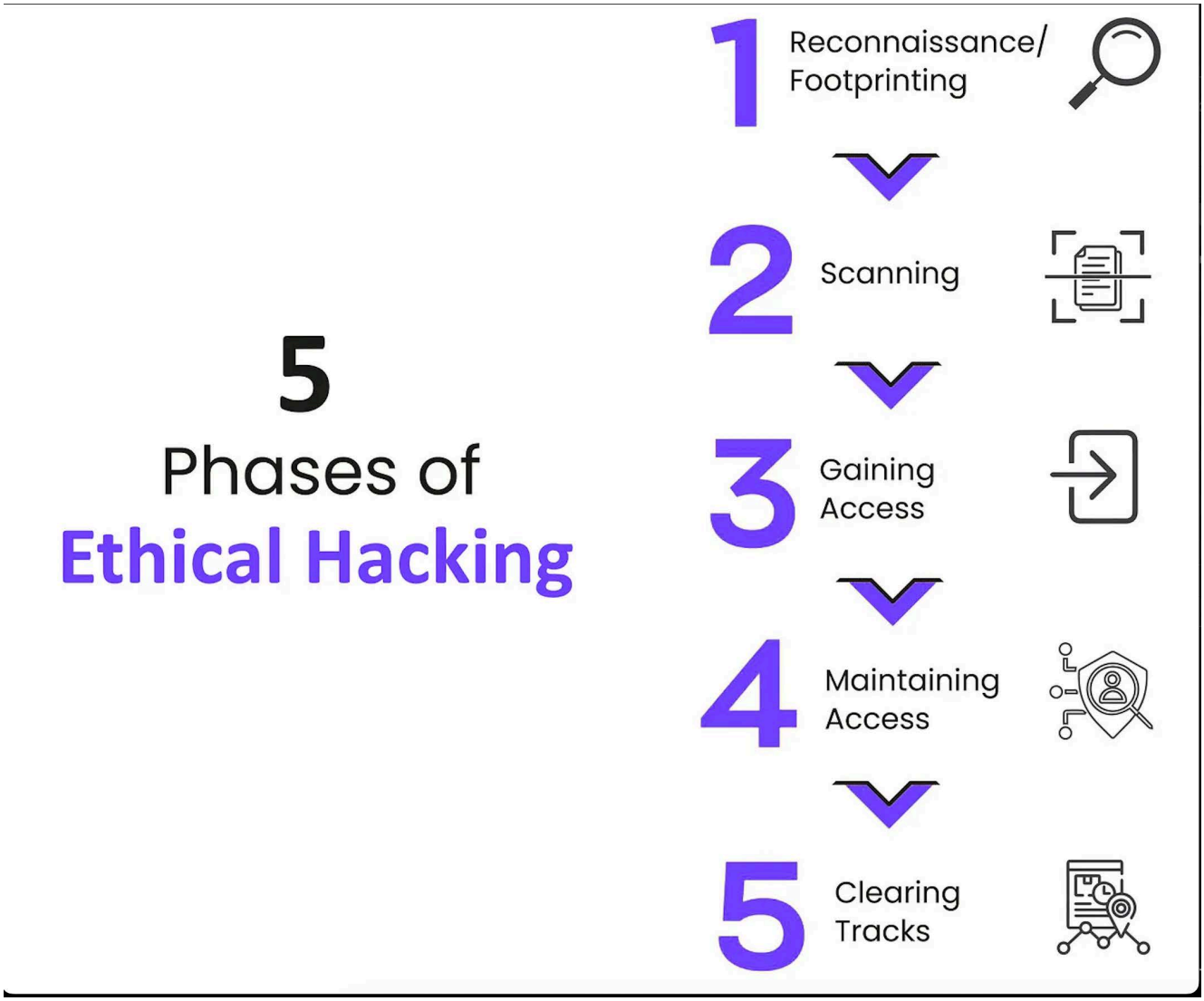
Limitations of Ethical Hacking

- There is limited scope for hackers because they have defined boundaries.
- The resources are less because of budget and power accessibility.
- The choice of the method is in the hands of the organization becoming another drawback.

Phases of Ethical Hacking

Play -Phases of Ethical Hacking

Ethical hackers are highly needed today by businesses and government entities to tackle the growing threat to IT security. Many government organizations, experts, and companies increasingly understand that closing your doors is not enough to defend a system.



As more firms seek into the digital realm, protecting data from hackers

and cyber-attacks is more crucial than ever. Organizations are now recognizing the potential consequences of these attacks and considering preventative measures, one of which is ethical hacking.

What is Ethical Hacking?

Ethical hacking detects vulnerabilities and carefully addresses them before they worsen. The word permission is used in the hacking process, which separates ethical hacking from other hacking tactics.

Ethical hacking is the analysis of an organization's security strategy by a team of professionals known as "White hat hackers or Red Team Experts." Their primary goal is to compromise the system to address the vulnerability with explicit permission from the organization and to deliver a performance measurement system showing the possibility of risk. Public and commercial companies, as well as banks, usually employ ethical hackers to combat cybercrime.

The Advantages of Ethical Hacking

The main advantage of ethical hacking is to restrict illegal adversaries from stealing and misusing data, as well as:

- Finding weaknesses from an attacker's perspective so that vulnerabilities are addressed
- To prevent network security breaches, implement a strong and secure network
- Enhancing consumer's and shareholder's trust by maintaining the security of their services and data
- Assisting in network protection with real-world evaluations

Types of Ethical Hacking

Undoubtedly, every organization, network, website, equipment, etc., may be stolen. Ethical hackers must learn to think like malicious hackers and be familiar with the tools and strategies they are likely to employ to comprehend how the hack might occur and the impact. Here are the

common types of ethical hacking, which include:

Phases of Ethical Hacking

Organizations recruit ethical hackers to replicate an actual cyberattack on their systems and networks. This attack consists of several phases, and it requires a ton of expertise and works for ethical hackers to discover all vulnerabilities and leverage them properly.

This hypothetical attack is designed to highlight all weak areas in the enterprise and attempt to address them. The five phases of ethical hacking are as follows:

1. Reconnaissance/Footprinting

Reconnaissance is the first phase of ethical hacking, also known as the footprinting and information gathering phase. This is the preliminary phase where white hat hackers gather as much information as possible and implement security measures into the targeted system or network. The information gathered by white hat hackers usually is about three groups: network, host, and people. There are mainly two types of footprinting:

- **Active footprinting:** Communicate with the target directly to gather information about the target.
- **Passive footprinting:** Seeking to get information about the target without gaining direct access to the target. Hackers exploit social media, public websites, and other public resources.

2. Scanning

The scanning phase is the second step in an ethical hacker's methodology. It entails applying all the knowledge learned during the reconnaissance phase to the target location to search for vulnerabilities. Hackers search for data such as user accounts, credentials, IP addresses, etc. There are three types of scanning, which include:

- **Port scanning:** During this stage, the target is scanned for data such as open ports, live systems, and other services active on the host.
- **Vulnerability scanning:** This scanning technique identifies a target's vulnerabilities and weak points and attempts to exploit those bugs in various ways. It is carried out using automated tools such as Netsparker, OpenVAS, Nmap, and others.
- **Network scanning:** This method includes locating the organization's firewall and other routers and networks to assist them in their hacking operations.

3. Gaining Access

In this phase, the hacker creates the blueprint for the target's network using the data gathered in Phases 1 and 2. Now the hacker has all of the information he requires. So he creates the network map and decides how to carry out the attack? There are various alternatives, such as:

- Phishing attacks
- Brute force attack
- Spoofing attack
- Man in the middle attack
- Dos attack
- Session hijacking
- Buffer overflow attacks

The hacker obtains access to the network, programs, and system and then extends their access permissions to manage connected systems.

4. Maintaining Access

When a hacker gains access, they choose to maintain it for future exploitation and attack. In addition, the hacker gains access to the organization's Rootkits and Trojans and utilizes them to execute more network attacks. An ethical hacker attempts to keep access to the target until they have completed the activities or intend to complete in that target.

5. Clearing Tracks

Once a hacker has obtained access, they leave no trace to prevent detection by the security team. They execute this by deleting cache and cookies, interfering with log files, and closing all open ports. This incorporates some of the steps an ethical hacker uses to cover and eliminate their footprint.

- Deleting/corrupting all logs
- Changing the values of logs or registries
- Removing all of the folders established by the ethical hacker
- Uninstalling all the applications

Ethical hackers use the following methods to hide their tracks in ethical hacking:

- Using reverse HTTP shell
- Tunneling with ICMP (Internet Control Message Protocol)