**Dated: 31/08/2022 bwl#2**

.

*What is Ethical Hacking?*

Ethical hacking is an authorized practice of detecting vulnerabilities in an application, system, or organization’s infrastructure and bypassing system security to identify potential data breaches and threats in a network. 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.

“It takes a thief to catch a thief.”

They check for key vulnerabilities including but are not limited to:

· Injection attacks

· Changes in security settings

· Exposure of sensitive data

· Breach in authentication protocols

· Components used in the system or network that may be used as access points

Now, as you have an idea of what is ethical hacking, it's time to learn the type of hackers.

*What are the Different Types of Hackers?*

The practice of ethical hacking is called “White Hat” hacking and those who perform it are called White Hat hackers. In contrast to Ethical Hacking, “Black Hat” hacking describes practices involving security violations. The black hat hacker uses illegal techniques to compromise the system or destroy information. Unlike White Hat hackers, “Grey Hat” hackers don’t ask for permission before getting into your system. But Grey Hats are also

different from Black Hats because they don’t perform hacking for any personal

or third-party benefit. These hackers do not have any malicious intention and

hack systems for fun or various other reasons, usually informing the owner

about any threats they find. Grey Hat and Black Hat hacking are both illegal as

they both constitute an unauthorized system breach, even though the intentions

of both types of hackers differ.

White Hat Hacker vs Black Hat Hacker

The best way to differentiate between White Hat and Black

Hat hackers are by taking a look at their motives. Black Hat hackers are

motivated by malicious intent, manifested by personal gains, profit, or

harassment; whereas White Hat hackers seek out and remedy vulnerabilities, to

prevent Black Hats from taking advantage.

The other ways to distinguish between White Hat and Black

Hat hackers include:

**Techniques Used**

White Hat hackers duplicate the techniques and methods followed by malicious hackers to find out the system discrepancies, replicating all the latter’s steps to find out how a

system attack occurred or may occur. If they find a weak point in the system or

network, they report it immediately and fix the flaw.

* **Legality**

Even though White Hat hacking follows the same techniques

and methods as Black Hat hacking, only one is legally acceptable. Black Hat

hackers break the law by penetrating systems without consent.

* **Ownership**

White Hat hackers are employed by organizations to

penetrate their systems and detect security issues. Black hat hackers neither

own the system nor work for someone who owns it.

After understanding what is ethical hacking, the types of

ethical hackers, and knowing the difference between white-hat and black-hat

hackers, let's have a look at the ethical hacker roles and responsibilities.

What are the Roles and

Responsibilities of an Ethical Hacker?

Ethical Hackers must follow certain guidelines to perform

hacking legally. A good hacker knows his or her responsibility and adheres to

all of the ethical guidelines. Here are the most important rules of Ethical

Hacking:

· An ethical hacker must seek authorization from the

organization that owns the system. Hackers should obtain complete approval

before performing any security assessment on the system or network.

· Determine the scope of their assessment and make known

their plan to the organization.

· Report any security breaches and vulnerabilities found

in the system or network.

· Keep their discoveries confidential. As their purpose

is to secure the system or network, ethical hackers should agree to and respect

their non-disclosure agreement.

· Erase all traces of the hack after checking the system for any vulnerability. It prevents malicious hackers from entering the system through the identified loopholes.

Skills Required to Become an Ethical Hacker

· Knowledge of programming

· Scripting knowledge

· Networking skills

· Understanding of databases

· Knowledge of multiple platforms like Windows, Linux, Unix, etc.

· The ability to work with different hacking tools

available in the market.

· Knowledge of search engines and servers.