What is Ethical Hacking?

Ethical Hacking is also known as Penetration Testing. This is a performance of penetrating into networks or system to search for the vulnerabilities, and threats from a system which can be easily attacked by a malicious attacker and lead to financial loss, data loss, or various other chief reparations. Nowadays, computers are very obligatory to run a fruitful business. It is not possible to have a secluded computer system and for sure, all the computers are required to be interacted to enable communication with peripheral dealings. While networking and integrations are performed, systems are exposed to the outside world and thus results in hacking. As per the survey conducted by Cyber Security organizations, it is clearly known just because of illegal hackers, Indian companies have lost about $4 billion in the year 2013. Hope you all are aware that hacking is unlawful and such actions can end up in dangerous penalties if caught. Many people are sentenced to imprisonment just because of hacking. To progress the system or network security, Ethical Hacking takes place for setting the susceptibilities hunted at the time of testing. There are few tools and approaches used by malicious hackers and similar processes are used by Ethical hackers too but with the authorization of the sanctioned person to enhance the security system and protect the systems from various malicious users. Few examples of ethical hacking are penetrating networks, creating procedures to crack passwords, or dislocating network services.

Below are the chief points to take care of Ethical Hacking:

- Written permissions to examine the network and try to modify the security settings
- Esteem the individual or business's privacy
- Gain faith of the customers by guaranteeing the security of data and security

Why Ethical Hacking?

Now we have a question "why use Ethical Hacking? So, let us see the reasons for using Ethical Hacking.

1. Preparation for a cyberattack: It is very simple for cyberattacks can abolish an occupation, particularly when coming to a small-sized business. There are many companies that are not well prepared for cyberattacks. Ethical hackers are good at finding the threat operation and understand the process of using new information and procedures to attack the business. Security specialists working with ethical hackers can easily prepare and handle future attacks. This process is useful in reacting to the continuously altering nature of operational threats.
2. Hunting the Susceptibilities: To determine the effectiveness of security measures, update the security system, identify the vulnerabilities, Ethical Hacking is necessary. Once the ethical hackers complete the evaluation part of an organization, a report is sent to the company heads regarding the vulnerable areas. For example, uncertain applications, password encryption under insufficient state, and unprotected systems that are running with unpatched software. Based on this report and data, organizations can perform a few tests to make end up in a few decisions on how and where to progress their security attitude to avoid cyberattacks.
3. Cybercriminals are using different demonstrating approaches**.** These demonstrations provide various techniques of hacking handled by executives used to attack their systems and cause chaos with businesses.

Techniques of Ethical Hacking

There are few ethical hacking techniques that are generally used by hackers to attack businesses and enterprises. Few are discussed below:

1. To find vulnerabilities, we need to scan ports. Few port scanning tools like Nessus, Nmap, or Wireshark are helpful for Ethical hackers to scan an organization's system, recognize the entire open ports, get to know the vulnerabilities available on each port and take corrective steps and act accordingly.
2. Analyzing patch installation procedures is the next technique used by the Ethical Hackers. This is to ensure that we don't introduce any new susceptibilities in the updated software that can be oppressed.
3. Accomplish Sniffing and networking traffic examination using the suitable tools is one the best technique.

Ethical Hackers

Specific computer specialists are frequently appointed in most of the companies to find the weak points and vulnerabilities and fix them. People who can hack into the system with complete permission are known as ethical hackers. Same skills, similar methods, and techniques are used by all the Ethical Hackers for analysis and avoid organization. Ethical hackers use their skills and many of the same methods and techniques to test and sidestep the company's IT security which is said to be immoral counterparts. Ethical hackers are used to document the found out key points and afford suggestions on how to overcome those security issues in order to strengthen the overall organization security. The companies whose networks are connected to the Internet or delivers an online service must always target the penetration testing which is effectively handled and performed by Ethical Hackers.

Based on the intention of the hacking process, we have three (3) types of hackers, White Hat Hacker, Black Hat Hacker, and Grey Hat Hacker. As the name clearly defines, white hat hackers are used for a good purpose, whereas black hat hackers are meant for wrong activities.

1. White Hat Hackers

Hackers who are working for any good purpose with complete proper access and permissions are called White Hat Hackers. Their intention is not to damage a system, but they ensure to hunt for the computer weaknesses and perform penetration testing and vulnerability analysis. Ethical hacking is one of the top demanding jobs available in the software industry and White Hat Hackers is completely legal. Plentiful companies are hiring ethical hackers to have a wonderful security system. White Hat hackers are sure to hold a UG or PG degree in Computer Science or IT. For a better scope and best job, certification on hacking is an advantage.

2. Black Hat Hackers

A black-hat hacker is an illegal actor who enters into the system or network without any legal permissions. Black box ethical hacker is the one who does not know anything about the organization on which they perform the attack. These hackers simply try to impose harm by conceding error-filled website functions, unsecured security systems or closing systems. This process is very for stealing, or gaining access to the most important financial data, passwords, and a few other crucial personal data. The astonishing fact of this type of hacker is they frequently utilize a set of common hacking activities.

3. Grey Hat Hackers

A Grey Hat Hacker is a combination of black box hacking and white box hacking. We cannot expect any intention for this kind of hacking, but their attacking activities are for fun purposes. Just like that, they try to adventure the security within various networks or computer systems without the possessor's knowledge or permission. Their only intention is to acquire the attention of the system owners and be praised for the so-called wonderful hacking work. Grey Hat hackers will not run behind the data or money or information while hacking, neither they work for a good purpose. We can see more Grey Hat Hackers all over the world when compared to the other two hacker types.

Apart from the above-mentioned three (3) major Hackers, there are few other hacker types too which are Red Hat, Blue Hat, Green Hat, and Script Kiddie.

Hacking tools used in common

Hackers are using a variety of tools to achieve a faultless hack and they are listed below:

1. Keyloggers: Keyloggers is an expressly intended tool used to record or log each key pressed on a computer. The documented file is later saved, which contains website details, usernames, accessed applications, and snapshots. You can retrieve the personal messages, credit card numbers, passwords, contact numbers, passwords, and a few other data that are typed on the system.
2. Rootkits: There are few hackers who take remote access to a computer system interacting with the internet and that's where rootkit software tool takes place. The original use of a rootkit is to open a system's backdoor to resolve a few software problems. Inappropriately, hackers are now using this program to threaten an operating system from its users. To install the tool rootkits in a target's computer, Phishing attacks, and social engineering are the most important methods. On successful installation completion, hackers can access and govern the system in a secret manner. This process provides them a chance to steal vital data or shut down the system.
3. Vulnerability Scanner: To categorize and perceive various system weaknesses available in communication systems, networks, networks, etc, a vulnerability scanner is used. Ethical Hackers are utilizing this most common procedure to find all the probable ambiguities and fix those issues instantly.

Different Phases of Ethical Hacking

While performing penetration testing, we need to perform proper steps and they are discussed below:

Step 1 - Planning and Investigation: The initial step for Ethical Hacking is to describe the possibility and mission of a test along with the testing methods which are mandatory to be performed. This step will also discourse the aptitude to comprehend the budding vulnerabilities and the way that target works. With the help of foot-printing tools, the potential foot-printing is done through various email, web services, search engines, web services, social network sites, network, DNS, etc.

Step 2 – Scanning: Next to the planning and investigation phase, we do have a scanning process. This step is to recognize the numerous intrusion efforts performed by the target in two methods. Scanning is done when the application code is operative and the other one is when the

application code is motionless. The most practical method to appreciate the performance of an application in real-time is scanning at the time of functioning.

Step 3 – Acquiring Access: Gaining Access is the step where the web application is criticized with the help of backdoors, SQL injections, and cross-site scripting. Through this phase, it is easy to retrieve the vulnerabilities and later data can be stolen, stop the traffic, and affect the rights to realize the damage volume that can arise.

Step 4 – Preserving Access: To steal the entire valuable data and financial information, this step wakes up. The vulnerability is utilized as a determined presence in the infested system for an extended duration. You can also spread vulnerability within the network by maintaining access for a longer time.

Ste 5 – Analysis: On completing the penetration test, result compilation happens. This result is finalized by analyzing and remarking the vulnerabilities broken, data access, and the duration that a tester can stay unobserved in the system.

Certifications on Ethical Hacking

Below are the certifications available for Ethical Hacking concepts:

S. No	Category	Certification Name	About Certification
1.	Core	Certified Network Defender (CND)	The major focus of CND certification is about creating network admins who are well qualified in detecting, shielding, and retorting to the network threats. You can get hands-on experience on all the chief tools of network security and methods. Through this certification, you will get strong knowledge of network security operations and technologies. The exam duration is approximately 4 hours and a number of questions is 100.
2.		Certified Ethical Hacker (CEH)	CEH is the world's top unconventional certification containing the most used 20 security domains that are used in the current days to enhance the organization's information security position. The exam duration is 4 hours and 125 questions are posted in the exam.
3.		Certified Ethical Hacker (CEH- Practical)	In this certification exam, you will need to demonstrate the application of Ethical Hacking methods like Detection of Operation Systems, networking scanning, vulnerability analysis, identification of threat vector, web app & system hacking, and so on. The duration of this exam would be around 6 hours.
4.		Certified Ethical Hacker (CEH- Master)	The world's top performance-based ethical hacking certification is CEH - Master, which is well verified and available through online courses as well. On completing this certification, you will be able to say "Yes, I am clear, I can work all alone". Once you clear the CEH Master

			and CEH Practical certifications, you will get the award from EC-Council.
5.	Advanced Level	Certified Threat Intelligence Analyst (CITA)	The development of the CTIA program was a collaboration with threat intelligence and cybersecurity experts all over the world to aid various companies to recognize and moderate business hazards. All the mysterious internal and external threats can be converted to known threats. An organized method for constructing active threat intelligence is taught from this course.
6.		EC-Council Certified Security Analyst (ECSA)	ECSA provides you a group of wide-ranging methodologies that encloses various pen-testing needs in different categories. The exam duration for this course would be around 4 hours and the number of questions is 150. You need to get 70% to pass this level of certification.
7.		EC-Council Certified Security Analyst (ECSA-Practical)	ECSA-Practical is to test an individual skill to accomplish exploit and threat research, teach to write own exploits, modify payloads, and make perilous choices at various pen-testing phases which can make or disrupt the entire valuation.
8.	Expert Level	Licensed Penetration Tester – Master (LPT)	If you are ready to become a master in pen-testing tools and methodologies, then you need to opt LPT program where you can face the firmest challenges in a scheduled environment. You can easily get knowledge on advanced ideas like pivoting between networks, scanning against defences, deploying proxy chains, and how to use web shells. Live online, Self-study, In-person training, and Master class are the different training options available with the LPT course.

Skills grabbed by Ethical Hackers

On completing the above mentioned Ethical Hacking certifications and leading your career as an Ethical Hacker, then you are expected to have proficiency in networking, database handling, and operating system. For better communication, excellent soft skills are also expected. The chief technical skillsets that an ethical hacker must have are DNS spoofing, SQL Injection, Session hijacking and spoofing, handle numerous network attacks, password predicting and breaking, and network traffic sniffing. Apart from all these mentioned skills, a very common skill expected is creative thinking as they must face all the ingenious ways used by the black hat hackers. The fact is it’s the duty of ethical hackers to foresee and take preventive measures.

Career in Ethical Hacking

If you have completed the Ethical Hacking certifications, you can try for various hacking roles like Security Analyst, Information Security Manager, Information Security Analyst, Security Consultant, Penetration Tester, and Certified Ethical Hacker. You can easily get a chance to work

in the military and for secret intelligence agencies such as NSA, CIA, and Mossad. An average salary for an ethical hacker would approximately $90,000 yearly as per the report shared by PayScale in the year 2019. With few years of experience, you can draw up to $120,000 per year and it keeps on increased based on your experience.

Why choose Ethical Hacking as a Career

1. There are few top companies that offer a very good pay for ethical hackers. Such companies are S.Air Force, S.Army, Booz, Hamilton, Allen, General Dynamics Information Technology Inc, etc.
2. Individuals who are good at hacking can work in different sectors like hotels, financial institutions, airlines, etc.
3. Ethical hacking is a perfect choice to make your entry to different domains.
4. Pre-requisites to become an ethical hacker are not a big list, whereas only a bachelor's degree in computer science is expected.
5. Ethical Hacking is an ever-growing field as it protects various systems that contain all the valuable information.
6. If you are a black hat hacker, it becomes very simple for you to turn out to be a white hat hacker with all your hacking skills.
7. If you are a Grey hat hacker, you can simply have fun without breaking the law.
8. The job title "Ethical Hacker" is a cool title that you can casually and happily mention to other people when asked for your job role.

The other basic concepts that need to concentrate are need to think out of the box, do a few hands-on exercises to perform self-learning, and try to get more information. Use the crucial key called "internet" for all your queries and become a master in your Ethical Hacking career.