Introduction to Ethical Hacking

Kanav Jindal

Computer Science and Engineering Department

ABES Institute of Technology Ghaziabad, India

Abstract: - As nowadays all the information is available online, a large number of users are accessing it some of them use this information for knowledge and some use it to know how to use this information to destroy or steal the data of websites or databases without the permission of the owner. The purpose of this paper is tell what is ethical hacking, difference between ethical hacker and cracker, job role for ethical hacker, what does ethical hackers does, phase of ethical hacking, job profile for ethical hacker, demand for ethical hackers, job trends in India, advantages and disadvantages of ethical hacking is covered in this paper.

Keywords: - Hackers, Ethical Hacker, Job trends.

Introduction

Hacking is breaking in to computer networks and systems either for profit or motivated by a challenge. Hacking is not just a word to be handled easily; it has many meaning in different situations. It is a Computer crime but on the other hand it is one of the highly paid jobs in the field of the computer security. Eric Steven *Raymond*, compiler of "**The New Hacker's Dictionary**", defines a hacker as a clever programmer. A "good hack" is a clever solution to a programming problem and "hacking" is the act of actually doing it. *Eric* Steven Raymond lists four possible characteristics that qualify one as a hacker, which we paraphrase here:

- A person who enjoys learning different programming language.
- A person who enjoys actually doing the programming rather than just think about it
- A person who picks up programming quickly.
- A person who is an expert at a particular programming language or different operating system.

ETHICAL HACKING TERMINLOGY

- **Adware** − Adware is software designed to display the pre-chosen ads to display on our system.
- **Attack** − An attack is an is done on a system to get its access and extract sensitive data.

- **Back door** − A back door, or trap door, is a hidden entry to a computing device or software that can bypasses security measures taken in, such as logins and password protections.
- **Bot** − A bot is a program that automates an action so that it can be done repeatedly at a much higher rate for a longer period than a human operator could do it
- **Botnet** − A botnet, also known as zombie army, is a group of computers controlled without the presence of the owner's knowledge. Botnets are used to send spam or used to do denial of service attacks.
- **Brute force attack** − A brute force attack is an automated and the simplest method to gain access to a system or website. It tries different combination of usernames and passwords, again and again, until it successfully able hack into the system.
- **Clone phishing** − Clone phishing is the process of creating replica of an existing, legitimate email with a false link to trick the recipient into providing personal information.
- **Cracker** − A cracker is one who cracks the original software to access all features of the original software which it considered illegal to do cracking of the original software, especially copying the copyright features such as security, access rights and other features of the original software.
- **Denial of service attack (DOS)** − A denial of service (DOS) attack is a malicious attempt to make a server or a network resource inaccessible to users, usually by temporarily suspending the services and making unavailable to those who's accessing the services on the Internet.
- **DDoS** − Distributed denial of service attack..
- **Spoofing** − Spoofing is a process in which a hacker gains an unauthorized access to computers, whereby the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host and to bypass the firewalls.
- **Firewall** − A firewall is a virtual wall that is used is designed to keep unwanted intruders outside a computer system or network while allowing safe communication between systems and users on the inside of the firewall.
- **Keystroke logging** − Keystroke logging is the process of tracking the keys which are pressed on a computer (or on the touch screen of mobile phone). It is used by hackers to record the login IDs and passwords.
- **Malware** − Malware is a vast umbrella term used to refer many other variety of forms of hostile or harmful software, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, scareware, and other malicious programs.
- **Phishing** − Phishing is e-mail fraud method in which the sender sends out legal looking emails, in an attempt to gain personal and financial information from recipients.
- **Rootkit** − A rootkit allows hacker to maintain command and control over a computer without the computer user/owner knowing about it. Once it has been installed, the

hacker is able to take controller of the victim machine and able to remotely execute files and change system configurations on the host machine.

- **SQL Injection** − SQL injection is an SQL code injection technique, used to attack database and modify the data stored in databases .
- **Social engineering** − Social engineering is process of deceiving someone with the purpose of acquiring sensitive and personal information, like credit card details or user names and passwords. Hacker is experts in doing the social engineering attacks and most popular form of attacks.
- **Trojan** − A Trojan, or Trojan Horse, is a malicious program hidden to look like a valid program, making it difficult to distinguish from programs that are supposed to be there designed with an intention to destroy files, alter information, steal passwords or other sensitive information.

Hackers

"HACKER" refers to the person try to find the weakness in the computer network for gaining the access. The verb "HACKING" describes modification in the technology for the offensive or the defensive purpose.

TYPES OF HACKERS

Hackers are three types

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

1. White Hat

White hat hackers are those hackers who hack into the system or computer network with the permission of the target to find out the vulnerabilities and security flaws in the present system. They are actually helping the organisation or individual by making them aware about such flaws and bugs. These types of professional's hackers are hired by companies. In the company when there is more than one sneaker then the group of such professionals are called as "tiger team". So we can say that white hat hacker is actually an ethical hacker who is try to report the flaws, ethically.

2. BLACK HAT HACKER

A black hat hacker is a person who works in grey area means again the laws of companies. They exploit the computer system or computer network without the permission from any authorised party. His main goal is to do harm to the system. Basically black hat hacker is a kind of person who uses his knowledge of vulnerabilities exploits the system. He is much more concerned with

his private gain. These persons are not interested to reveal them in the public. They may write their own code or script to destroy the entire system and its security for their private interest and gain.

3. GREY HAT HACKER

A grey hat hacker is a person who has skill to act as a good or bad in both ways. At times grey hat hacker can act both legally and sometimes he may act illegally. These hackers generally do not hack the system for their personal gain. They normally don't have any kind of bad intentions, but they may commit a crime when using technology. A grey hat hacker will not report the flaws in the system to the administrator for any kind of dissemination.

ETHICAL HACKER VERSUS CRACKER

Ethical hackers are usually security professional or network penetration testers who use their hacking skills for defensive and protective purposes. They do their work with the permission of the organization. The work is under the laws of the country. Any computer professional can learn ethical hacking.

Cracker are usually describing as hackers who uses their hacking skills and toolsets for offensive purposes. Some of the popular attacks the cracker does are Denial of Service attack (Dos), virus, Trojan attacks. Their work is against the law of the organization. They do work for their personal gain. Their work is generally in grey area.

THE JOB ROLE FOR ETHICAL HACKER

Ethical hacking also known as penetration testing or white-hat hacking, involves the same tools, tricks, and techniques that hackers use, but with one major difference that Ethical hacking is legal. The person does hacking in order to safe guard the systems and tries to find flaws and bugs in the system. It tries to make system secure and any future attacks.

WHAT DO ETHICAL HACKERS DOES?

The purpose of ethical hacker is usually same as crackers: they're trying to determine what an intruder can see on a targeted network or system and what hackers can do with that information. This process of testing the security of a system or network is known as penetration testing or pen test.

Many ethical hackers detect malicious hacker's activity as part of security team of an organization tasking with defending against the malicious hacking activity. A penetration tester plan can be built around the data that need to be protected and potential risks.

AN ETHICAL HACKER'S SKILL SET

To be an ethical hacker and penetration tester following skill set are needed to become good hacker:

- Strong knowledge of networking, and computer systems.
- Understanding of current different used operating systems like, Linux, Windows, and Mac.
- Ability to hack into network or systems on permission, to assess vulnerabilities.
- Able to perform preventive, corrective and protective countermeasures against malicious attempts.
- Should be proficient in identifying and cracking multiple types of passwords.
- Know the phases and methodologies of ethical hacking.
- Should know how to erase digital evidence of networks and system intrusions.
- Understand encryption techniques and cryptography.
- Adhere to the code of ethics and perform hack under professional conduct.
- Should be aware of common cyberattacks like phishing, social engineering, Trojans, insider attacks, identity thefts, etc., and should know how to undertake appropriate evasion techniques and countermeasures.
- Should have knowledge of cryptography for password decryption.

THE PHASES OF ETHICAL HACKING

The process of ethical hacking is generally divided into six steps:

- Phase 1: Reconnaissance
- Phase 2: Scanning
- Phase 3: Gaining Access
- Phase 4: Maintaining Access
- Phase 5: Clearing Tracks
- Phase 6: Reporting

Figure 1 – Phase of Ethical Hacking

Phase 1 Reconnaissance

This is the first step of Hacking. It is also called as Foot printing 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
- People involved

There are two types of Foot printing:

- **Active:** In Active Reconnaissance, information is gained by directly interacting with the computer system. The information thus gained is accurate and relevant. Due to direct interaction, Active Reconnaissance is associated with high risk of getting detected, if accessed without permission. If detected severe actions are taken and the subsequent activities are trailed.
- **Passive:** In Passive Reconnaissance, the ethical hacker will not be connected to the computer system directly. To gather essential information without interacting with the target system, Passive Reconnaissance is used.

Phase 2 Scanning

Scanning is the second phase in the hacking methodology in which the hacker tries to make a blue print of the target network. It is similar to a thief going through your neighbourhood and checking every door and window on each house to see which ones are open and which ones are locked. The blue print includes the ip addresses of the target network which are live, the services which are running on those systems and so on. Usually the services run on predetermined ports. There are different tools used for scanning war dialing and pingers were used earlier but now a day's both could be detected easily and hence are not in much use. Modern port scanning uses TCP protocol to do scanning and they could even detect the operating systems running on the particular hosts.

Scanning can be done in three ways:

1. Port Scanning

Port Scanning is the process of identifying open and available TCP/IP port on a system. Scanning tools enable a hacker to learn about the services available on a given system. Port Number are divided into three ranges:

Well-Known Ports: 0-1023

Registered Ports: 1024-49151

Dynamic Ports: 491251-65535

2. Network Scanning

Network scanning is a procedure for identifying active host on the network, either to attack them or as a network security assessment. Hosts are identified by their individual IP addresses. Network-scanning tools attempt to identify all the live or responding hosts on the network and their corresponding IP addresses

3. Vulnerability Scanning

Vulnerability scanning is the procedure for identifying the vulnerabilities of computer systems on a network. Generally, a vulnerability scanner first identifies the operating system on a network, include service packs that may be installed. Then the scanner identifies weakness or vulnerabilities in the operating system. After that hacker tell about the weakness in system.

Phase 3 Gaining Access

Phase 3 is when the real hacking takes place. This is the actual hacking phase in which the hacker gains access to the system. The hacker will make use of all the information he collected in the pre-attacking phases. Usually the main hindrance to gaining access to a system is the passwords. System hacking can be considered as many steps. First the hacker will try to get in to the system. Once he gets in to the system the next thing he want will be to increase his privileges so that he can have more control over the system. As a normal user the hacker may not be able to see the confidential details or cannot upload or run the different hack tools for his own personal interest. Another way to crack in to a system is by the attacks like man in the middle attack.

- **Password Cracking:**

There are many methods for cracking the password and then get in to the system. The simplest method is to guess the password. But this is a tedious work. But in order to make this work easier there are many automated tools for password guessing like legion. Legion actually has an inbuilt dictionary in it and the software will automatically. That is the software itself generates the password using the dictionary and will check the responses.

Techniques used in password cracking are:

- Dictionary cracking
- Brute force cracking
- Hybrid cracking
- Social engineering

- **Privilege escalation:**

  Privilege escalation is the process of raising the privileges once the hacker gets in to the system. That is the hacker may get in as an ordinary user. And now he tries to increase his privileges to that of an administrator who can do many things. There are many types of tools available for this. There are some tools like get admin attaches the user to some kernel routine so that the services run by the user look like a system routine rather than user initiated program. The privilege escalation process usually uses the vulnerabilities present in the host operating system or the software. There are many tools like hk.exe, metasploit etc. One such community of hackers is the metasploit.

Phase 4 Maintaining Access

Now the hacker is inside the system by some means by password guessing or exploiting some of its vulnerabilities. This means that he is now in a position to upload some files and download some of them. The next aim will be to make an easier path to get in when he comes the next time. This is analogous to making a small hidden door in the building so that he can directly enter in to the building through the door easily. In the network scenario the hacker will do it by uploading some software's like Trojan horses, sniffers, key stroke loggers etc.

Phase 5 Clearing Tracks

Now we come to the final step in the hacking. There is a saying that "everybody knows a good hacker but nobody knows a great hacker". This means that a good hacker can always clear tracks or any record that they may be present in the network to prove that he was here. Whenever a hacker downloads some file or installs some software, its log will be stored in the server logs. So in order to erase that hacker uses man tools. One such tool is windows resource kit's auditpol.exe. This is a command line tool with which the intruder can easily disable auditing. Another tool which eliminates any physical evidence is the evidence eliminator. Sometimes apart from the server logs some other in formations may be stored temporarily. The Evidence Eliminator deletes all such evidences.

Phase 6 Reporting

It is final phase of hacking in this reporting here the Ethical Hacker compiles a report with his findings and the job that was done such as the tools used, the success rate, vulnerabilities found, and the exploit processes.

ETHICAL HACKING: JOB PROFILES

There are various job roles in which ethical hackers can get jobs some of them are listed below:

- Information Security Analyst
- Security Analyst
- Certified Ethical Hacker (CEH)
- Ethical Hacker

- Security Consultant, (Computing / Networking / Information Technology)
- Information Security Manager
- Penetration Tester

JOB DEMAND IN ETHICAL HACKING

Ethical hacking careers are flourishing. Certified ethical hackers are in huge demand as their work entails finding the flaws in an enterprise's systems and network. If you are a certified ethical hacker, you can join the government or a private organization as a cyber-security expert/specialist. The profiles that are on offer include Security Executive, Web Security Manager/Administrator, Network Security Administrator, Network Security Systems Manager and much more. However, an ethical hacking career is not limited to IT companies. Retail chains, airlines, BFSI industries, hospitality chains, and several other industries also recruit cyber security experts. A qualified ethical hacker can also start their own business to provide ethical hacking training and services.

At present, IT companies are the main recruiters of ethical hackers. The much sought-after companies such as:

- Infosys
- Wipro
- TCS
- Tech Mahindra
- IBM
- CIA
- Mossad
- National Security Agency(NSA)
- Accenture
- DXC
- Central Bureau of Investigation(CBI)
- National Security Agency (NSA)
- National Investigative Agency (NIA)
- Federal Bureau of Information (FBI)

- Global Logic and many more

JOB TRENDS IN INDIA

5-10 years ago, there wasn't much scope in the field of ethical hacking but the landscape has changed today. As cybercrime has increased, every company is in need of ethical hackers to check their system. As per a **Nasscom** survey, we need **5 lakh cyber security professionals, but we have only 50,000."**

The pay-scale is in the field of ethical hacking, Mr. Sengupta says, "While freshers earn a starting salary of Rs.6 lac per annum, there are people who earn upto Rs.60 lacs per annum too. The sky is the limit for experienced professionals in this field.".

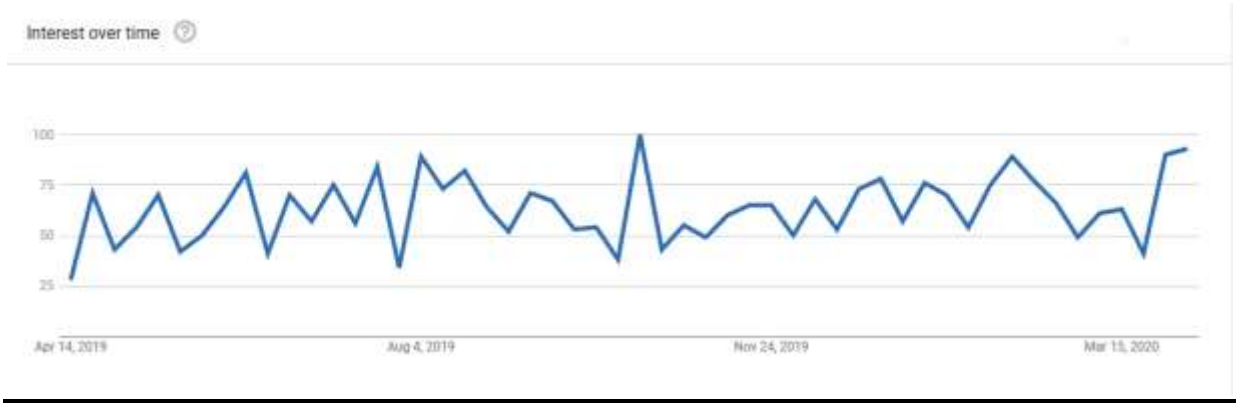

Figure 2: Google trend show demand of Ethical Hacker in India

Growing at a rate that is outpacing all other areas of IT, cyber security has emerged as a high-growth-field of 2019, and possibly of the entire decade. During the 5 years between 2015 and 2020, listings for cybersecurity jobs increased by a whopping 85% according to the analysis made by the Bureau of Labor Statistics. This has led to a lot of unfilled positions so jobs are plenty and they pay well too.

This is condition is same many other countries like USA, Europe, United Kingdom, Japan, Russia and many more.

Demand of Ethical Hacker in India Region wise:

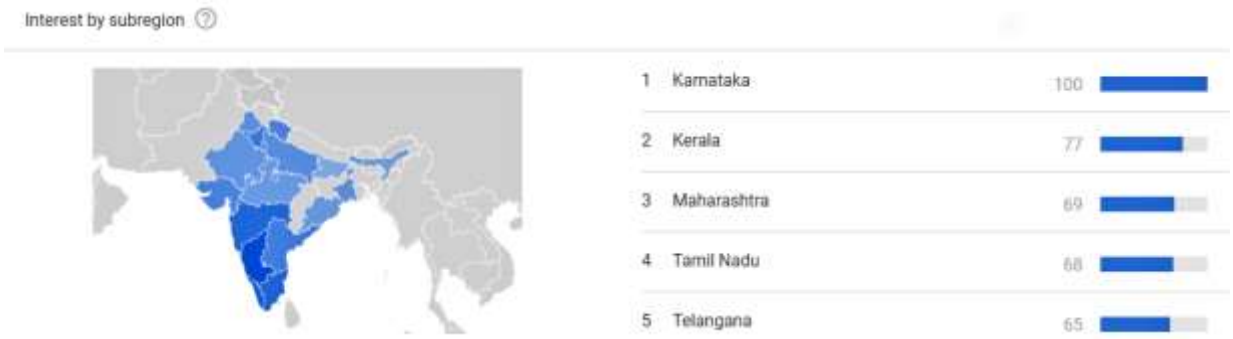

Figure 3: Ethical Hacker Demand in India Region wise:

As the region wise of India shows that each and every part of India is looking for ethical hacker. Most demand of it is in Karnataka then Kerala then Maharashtra so on. With its increasing boom the pay scale is also high in every part of India.

ADVANTAGES OF ETHICAL HACKER:

1. Fighting against terrorism and national security breaches.
2. Having a computer system that prevents malicious hackers from gaining access.
3. Having adequate preventative measures in place to prevent security breaches
4. Helps in closing the open holes in the system network
5. Provides security to banking and financial establishments
6. Prevents website defacements
7. An evolving technique

DISADVANTAGES OF ETHICAL HACKER:

1. All depends upon the trustworthiness of the ethical hacker
2. Hiring professionals is expensive.
3. The ethical hacker using the knowledge they gain to do malicious hacking activities.
4. Allowing the company's financial and banking details to be seen.

5. The possibility that the ethical hacker will send and/or place malicious code, viruses, malware and other destructive and harmful things on a computer system.

6. Massive security breach.

FINAL CONCLUSION

1. As it an evolving branch the scope of enhancement in technology is immense. No ethical hacker can ensure the system security by using the same technique repeatedly. He would have to improve, develop and explore new avenues repeatedly.
2. More enhanced software's should be used for optimum protection. Tools used, need to be updated regularly and more efficient ones need to be developed.
3. Ethical hacking is not a criminal activity and should never be considered as such.
4. While it is true that malicious hacking is a computer crime and criminal activity, ethical hacking is never a crime.
5. Ethical hacking is one of the most emerging fields with industry regulation and organizational IT policies.
6. Malicious hacking should be prevented while ethical hacking which promotes research, innovation, and technological breakthroughs should be encouraged and allowed.

REFERENCES

1. https://www.edureka.co/blog/ethical-hacking-tutorial/
2. CEH v10 Certified Ethical Hacker Study Guide by Ric Messier
3. "Ethical Hacking and Hacking Attacks"International.pdf" by Abhineet Anand
4. Certified Ethical Guide by Sagar Ajay Rahalkar
5. Ethical Hacking Ethical Hacking Procedure Certified Ethical Hacking Ethical Hacking: Future 15 by Ajinkya A. Farsole, Amruta G. KAshikar, Apurva Zunzunwala.
6. Sec council blogs by EC Council