A Brief Information of Ethical Hacking

Ashwini S K*, K Thippeswamy

Dept. of Studies in CSE, Dept. of PG Studies, VTU Mysuru

DOI: https://doi.org/10.21467/proceedings.1.75

* Corresponding author email: ashwini0621@gmail.com

ABSTRACT

Nowadays Internet technologies are widely adopted. The state of internet security is very poor. Hackers are two types, one is Good hackers and another one is Bad hackers. The Good hackers are the ethical hackers, they works for the good and new issues related to the ethical hacking and the bad hackers are non-ethical hacker, they are concentrating on targeting to destroy the system and thieve the confidential information. This paper gives the brief information on ethical hacking, ethical hacking types, how ethical hacking works, methodology and hacking tools and some needs and limitations of the ethical hacking. The major principal of this article focused to disclose the small idea of the ethical hacking and its affairs.

Keywords: Hacking, Ethical Hacking, Hacking Modes, Hacking Tools and System Security Tools

1 INTRODUCTION

The vast development of the Internet has access to vast commodities of electronic commerce, e-mail, extensively distributed content. Etc. Most of the computer connects to the Internet, wireless devices and networks are growing. As, with the maximum industrial development, there is also one another: Illegal hackers who will secretly steal organization information and move it to the open Internet.

Hacking is an inevitable event in computer hack that can also be applied through the positive implementation of a negative attitude or negative person. Computer and networks are now affected by computer viruses or network viruses. This area is worried about technicians. The intention to put light on hacking, which can be used positively in construction of this area and the behavior of people engaged in this area can be studied. The behavior is related to the psychology of human and its behavior, with respect to the family's family and with respect to society, with respect to self or respect. The human being also influences humanity. No one is good or bad from birth. Different factors are responsible for personal behavior of the person. These factors play an important role in hacking.

Many people hacking think that simple operations or orders are not organized. Hacking is not a special term; there are many types of hacking. Hacking is not a computer and network resource option. Computer hacking is a computer modeling exercise software and software that eliminates a purpose beyond the original creator. People involved in computer hacking activities are also called hackers. "Hacking" is a business that is suspicious and every professional whenever it is heard by clear or someone. It wants to be a hacker of all behavior born in this professional world. Hacker needs a sharp mind to hack any hack. It should be so powerful that no hacker can hack himself.

i. Types of Hackers

Hacking can be divided into three different types:

a. White Hat Hackers:

White hat hackers are ethical hackers with some certificates (Certified Ethical Hackers) .There are good people, ethical hackers who use hacking skills for protective purposes. Their primary purpose is to find the roofs in the network and optimize them. These types of hackers work with famous companies to secure their system and protect them against other hackers.

b. Black Hat Hacker:

A black hat hacker may or may not have any hacking certification but also get good information about hacking. They use their skills for destructive purposes, in which they violate the number of remote machines system or as a result of nurses' intention. After receiving unauthorized access, black hat hackers destroy relevant data, reject the valid user service, and mainly cause problems for their purposes.

c. Gray Hat Hacker:

A gray hat hacker is a combination of black hackers and white hackers. Gray hat hackers can surf the Internet and the skills to inform the administration can hack in a computer system that their system has been hacked. They can offer their system to restart for a small fee.

ii. Types of attacks

a. Nontechnical attacks People who suffer from harassment, consumers and even the means of eliminating themselves, are the biggest weaknesses in any computer or network infrastructure. Humans are trusting on nature, which can lead to social engineering exploitation. Social engineering is described as exploitation of the nature of human confidence to get information for the worst purpose. Other common and effective attacks against information systems are physical. Hackers enter the buildings, computer rooms, or other areas, which contain important information or property. Physical attacks may include dumplant diving (intellectual property, password, network diagrams, and other information through trash cans and dumps).

b. Network-infrastructure attacks Hacker attacks can be made against network infrastructure, as many internet access can reach across the world through the Internet. Here are some examples of the network infrastructure attacks:

- Attach a network through a rogue modem connected to a computer behind a firewall.
- Exploiting of network transmission mechanisms, such as TCP / IP and Networks.

- Overflowing a network with the too many requests and creating a denial of service (DoS) for legitimate requests.
- To install a network analysis on a network and capture on each packet, clear information in the secret text, display Piggybacking on a network through a secure 802.11b wireless configuration.

c. Operating-system attacks Hacking Operating System (OS) is a favorite way of bad guys. There is also a major part of OSs Hacker attacks because each computer is one and many leading exploits can be used against them. Occasionally, some operating systems that are more secure than the box, such as novel networks and BSD Unique flaws are attacked, and increase risk. But hackers attack windows and Linux such as operating systems because they use mass and are known better than their threats. Here are a variety of examples of attacks on operating systems:

- Exploiting exact protocol implementations
- Authentication systems is built in attacking
- Flouting file-system safety.
- Passwords are cracking and encryption system.

d. Application and other specialized attacks Apps take lots of hackers. Programs such as email server software and web applications are often hit:

- Hyper Text Transfer Protocol (HTTP) and Simple Mail Transfer Protocol (SMPP) applications are often attacking, since setting up maximum firewall and other security mechanisms to allow full access to the Internet from these programs.
- Malicious software (malware) contains viruses, insects, Trojan horses, and spyware. Malware prevent networks and reduces the system.
- Spam (junk email) system availability and destruction at the storage space is spreading. And this may take malware. Ethical hacking helps such attacks against your computer system.

2 ETHICAL HACKING MODES

1. **Insider attack:** This type of attacks and the performance of this ethical hack model that can be done by a legitimate person with a valid connection to the organization's network.
2. **Outsider attack:** This ethical hack tries to imagine the types of attacks that can be started across the Internet. This can be used by Hyper Text Transfer Protocol, Simple Mail Transfer Protocol (SMPP), Configured Question Language, or all other available services.
3. **Stolen equipment attack**: This simulation is closely related to a physical attack as it targets the organization's equipment. It could seek to target the CEO's laptop or the

quality being organised backup tapes. No matter what the target, the goal is to extract critical information, usernames, and passwords.

4. **Physical entry:** This simulation organization wants to examine the physical controls of the organization. Such doors, gates, locks, guards, closed circuit television (CCTV), and alarms are checked to see if they are outstanding.
5. **Bypassed authentication attack**: This simulation works with the search of wireless access points (WAP) and modems. The goal is to see that these systems are safe and provide sufficient control over control. If control rotation can occur, the ethical hacker can investigate which surface system control can be controlled.
6. **Social engineering attack:** This is not the purpose of simulation technological system or physical accessibility. Social engineering attacks targeted the organization's employees and tried to arrange them to get information about stability. A long way can be overcome by eliminating proper control, policies and such type of attack.

3 ETHICAL HACKER WORKING

The work of ethical hacker is included in the following steps:

1. **Obeying the Ethical Hacking Commandments:**
   Every ethical hacker should follow some basic principles. If they do not work, there may be bad things. During the planning or implementation of ethical hacking testing, most of these principles have been ignored or forgotten. Results are also very dangerous.
2. **Working ethically:**
   Ethical ethics can be described as working with high professional ethics and principles. Whether you are conducting ethical hacking tests against your own system or for someone who gets a job, you can do whatever you do as a ethical hacker and support the company's goals. Is. Hidden ages are not allowed. The ultimate goal of trust is. Incorrect information is not allowed.
3. **Respecting Privacy:**
   Treat the information collected with full respect. Log files should be kept private to clear all the information they receive during the web application files.
4. **Not crashing your systems:**
   One of the biggest mistakes is that when people try to hack their system; they come to destroy their system. Its main reason is poor planning. The exam did not read the documents or misuse the use and security of the security tools and techniques. When you are testing, you can easily create an incorrect situation on your system. There is a lot of tests going on a system too soon, locking lots of systems. Many security diagnostic tools can control how many tests are performed at the same time. If you do not have an account yet, register now! I'm sorry to hear from you. Please try again. If you do not have an account yet, register now!

5. **Executing the plan**:

In ethical hacking, time and patience is very important. Be careful when you are conducting your ethical hacking test

4 PROCESS OF ETHICAL HACKING

Planning is needed prior to the ethical hacking process. All technical, administrative and imperial issues should be considered. Planning is important for any testing test - an easy password test for a complete test on a web application. Data backups need to be closed; otherwise the investigation can be called unexpectedly if someone claims they are never eligible for the test.

A well-defined scope is included in the following information:

1. Specific systems to test.
2. Threats are involved.
3. Planning schedule time to take test and on the whole timeline.
4. Collect and discover information of the systems before testing.
5. What is made while a main vulnerability is exposed?
6. The specific deliverables

5 METHODOLOGY

The overall hacking method includes the following steps, as follows:

1. Reconnaissance:

The literal meaning of the Word reconnaissance is a preliminary survey to gain the information. This is also known as foot-printing. The hacker collects information about the company which the person is going to hack. Information as DNS servers, administrator contacts and IP ranges can be collected. During the reconnaissance phase different kind of tools can be used – network mapping, network and vulnerability scanning tools etc can be commonly used. Cheops for example is a very good network mapping tool which is able to generate networking graphs. They can be of great help later on during the attack phase or to get an overview about the network. A network mapping tool is very helpful when doing an internal ethical hack.

2. Scanning:

The hacker tries to make a blue print of the target network. 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. Modern port scanning uses TCP protocol to do scanning and they could even detect the operating systems running on the particular hosts.

3. Enumeration:

Some servers to calculate the hacker's involvement to provide information to them that they are required to attack. By doing this, hacker wants to know which resources and shares can be found in this system, which user accounts and user groups are present in the network, which applications are there.

4. Gaining Access:

This is a real hacking step that has access to the hacker system. Hacker will already use all the information collected in the attack period. The basic barrier password is usually to access a system. In system hacking, the first hacker will try to get into the system.

5. Maintaining Access:

Now the hacker is inside the system. This means that now they have the status of uploading some files and downloading some of them. Next time he'll make an easy way to get in the next time. It is suitable for building a small printed door in the building, so they can easily enter the building through the door.

6. **Clearing Tracks**:

Hacker ends here the physical evidence of its hacking system. Whenever the hacker downloads a file or installs some software, its login will be stored in the login log. So hacker to eliminate using human tools. Windows Device Kit is an instrument of auditpol.exe. Another tool that eliminates any physical identity is to destroy the proof. Destroy all the identifying destinations.

6 HACKERS USED TOOLS

There are several common tools used by network criminals:

- **Trojan horse**- These are malicious programs or can be used to establish backup software in a computer system so that the offense is accessible.
- **Virus-** A virus is an automatic program that spreads itself by copying captions into another valid code or document.
- **Worm** - Bugs are an ideal virus and have an automatic program. The difference between the virus and a worm is that a worm does not connect itself to another code.
- **Vulnerability scanner** –This device can be used by hackers and interviewers to check computers on the network for instantly known weaknesses. Hackers also use port scanners. To see the check that ports on a specific computer are "open" or available to access the computer.
- **Sniffer** – This is an application that either passes passwords and other data in transit or in the network inside the network.
- **Exploit** – This is to take advantage of a leading weakness.
- **Social engineering –** To get some form of information.
- **Root kit** - This device is to hide the fact that computer security is considered.

ISBN: 978-81-936820-0-5

Proceedings DOI: 10.21467/proceedings.1

7 ETHICAL HACKING BENEFITS AND LIMITATIONS

i. Benefits

Today, the security of the ethical hacking network is backbone. Every day its relevance is increasing.

1. You have to think like a thief to catch the thief.
2. Help open the open hole in the network.
3. Provides security to banking and financial organization.
4. Prevents website expenses.
5. A modern technology

ii. Limitations

As with all types of activities which are in the dark, there will be many problems. There is a possible reduction in ethical hacking

1. Using the ethical hacker information that has benefited corruption hacking activities
2. The company's financial and bank details can be allowed to view
3. The probability is that the ethical hackers will send and / or send abusive codes, viruses, malware, and other destructive and dangerous things to the computer system.
4. Massively violate the security.

8 SYSTEM SECURITY

- **Make it difficult to hack your password**

Hard password includes upper and lower case numbers, numbers and special characters. They should have at least eight characters in length. It should not be easy for them to find hackers, such as your pet's name or a member of the family member.

- **Regularly change your password**

A common mistake made by the consumer is to make a difficult password, but it should never change. It may be difficult to remember a long list of complicated passwords. But no password failed. Hackers have more than one account if they have the same account accounts. Password management services, such as a presentation or password box, can help you track difficult passwords. This service allows users to easily store and save their password.

- **Clear your browser's history**

It goes for all devices used in your home computer, your work computer, or your friend's member one day. Keep track of Internet browsers like Firefox or Chrome where you've done and what you've done online. They see the records of each of your site. Information about sending or saving to your computer can be kept for days or weeks. It is very easy for those who steal the detailed record of your online activities.

- **Do not use free WiFi**

The growing number of people now offers free wireless access to the Internet. Often, a user does not need a password to connect to the wireless network. These services may be useful, but it is also an easy way for hackers to access everything on your device. Unless you really need it, it's not the best to use it.

- **Use HTTPS**

HTTPS is officially known as "Hyper Text Transmission Protocol". It's like HTTP, which is used to enter Internet addresses. During HTTPS online adds an additional layer of security and encryption. Communication between users and sites that support HTTPS are encrypted. This information is also confirmed. This means that HTTPS can determine if the website is real or not.

- **See what you click**

Hackers is one of the most popular and successful ways your computer is through a technology called phishing. Fishing occurs in fishing when an email opens open that looks real. But the attachment is actually a virus that immediately affects the user's computer. If someone sends you a file or website, you do not ask him, it's better to not click on it.

- **Try not to use a public computer**

For many people, it may be hard to use public computers. People who use the Internet cafe to get online without access to computer or internet. However, more people use a computer, it is possible that a virus has affected it.

- **Use anti-virus protection**

Many anti-virus services are available for consumers. They can offer many different types of computer protection. Some anti-virus services are also free. They are one of the best ways to keep professional help users ahead of one step ahead of hackers.

- **Be careful while using thumb drive**

Thumb drives, which are also known as flash drives, are small and easy storage devices to use in different computers. They are a popular tool that people use to change files and documents. They can easily spread viruses to computers and networks.

9 CONCLUSION

The main objective of this paper is to provide basic information about the types of attacks, types of invaders and their strategy on the Internet. This paper shows hacking, ethical hacking and tools from many perspectives. The current poor security on the Internet can be the most effective way to prevent ethical hacking security holes and prevent interruptions. On the other hand, the ethical hacking tools are also a bad tool for muscles. The main strategy is to keep one step ahead of pastors.

ISBN: 978-81-936820-0-5

Proceedings DOI: 10.21467/proceedings.1

REFERENCES

[1] Gurpreet K. Juneja, “Ethical Hacking: A Technique to Enhance Information Security”, in International Journal of Innovative Research in Science, Engineering and Technology, Vol. 2, Issue 12, December 2013, page no. 7575-7580.

[2] Umar Salihu Barros, Mohammed Salihu Barros, “A Survey of Ethical Hacking process and Security”, in 4th International Conference on System Modeling & Advancement in Research Trends (SMART) College of Computing Sciences and Information Technology (CCSIT) , Teerthanker Mahaveer University , Moradabad, 2015, page no. 406-410.

[3] Abhishek Gupta, Dr. Jatinder Singh Mahnas, “Study on Ethical Hacking and Penetration Testing”, in International Journal of Scientific Research in Computer Science, Engineering and Information Technology © 2017 IJSRCSEIT | Volume 2 | Issue 4 | ISSN : 2456-3307, page no. 466-470

[4] Bhawana Sahare, Ankit Naik, Shashikala Khandey, “Study on Ethical Hacking”, in international Journal of Computer Science Trends and Technology (IJCST) – Volume 2 Issue 4, Nov-Dec 2014, page no. 6-10.

[5] Sumit Sharma, Anurekh Kumar, Shobha Bhatt, “A Literature Survey: Why Attacks are Successful on Information System”, in International Journal of Science, Engineering and Technology Research (IJSETR), Volume 4, Issue 7, July 2015, page no. 2617 - 2624

[6] Aishwarya S. Patil1, Ankush D. Patil, “Review on Ethical Hacking: A Security Assessment Tool to Audit and Secure Web Enabled Applications”, in International Journal of Research in Science & Engineering, Special Issue: Techno-Xtreme 16, e-ISSN: 2394-8299, p-ISSN: 2394-8280, page no. 524-530

[7] Sonal Beniwal, Sneha, “Ethical Hacking: A Security Technique”, in International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 4, 2015 ISSN: 2277 128X, page no. 325-329

[8] Er. Anjali Passi, Er. Priyanka Sharma, “Compressive Study on Ethical Hacking”, in International Journal of Emerging Research in Management &Technology, ISSN: 2278-9359 (Volume-4, Issue-1), January 2015, page no. 30-32.

[9] R. Edward Andrews, S. Sridhar, “Survey on Ethical Hacking and System Security”, in Special Issue of Engineering and Scientific International Journal (ESIJ) Technical Seminar & Report Writing - Master of Computer Applications - S. A. Engineering College (TSRW-MCA-SAEC) - May 2016, ISSN 2394-187(Online), ISSN 2394-7179 (Print), page no. 39-41.