International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 4 Apr. 2021, pp: 483-486 www.ijaem.net ISSN: 2395-5252

Ethical Hacking

Surya Prakash. SManimozhi.p

Student, Assistant professor Master of Computer Applications,Department of Computer Applications, PSG College of Arts & Science, Coimbatore

Submitted: 15-04-2021 Revised: 28-04-2021 Accepted: 30-04-2021

ABSTRACT: The explosive growth of the Internet has brought Many good things such as E-commerce-banking, E-mail, Cloud computing, but there is also a Dark side such as Hacking, Backdoors etc. Hacking is the first big problem Faced by Governments, companies, and private citizens Around the world , Hacking includes reading others e-mail, Steal their credit card number from an on-line shopping site, Secretly transmitting secrets to the open Internet. An Ethical Hacker can help the people who are suffered by this Hackings. This Paper Describes about Ethical Hackers, Their Skills, Their Attitudes, and How They Go About Helping TheirCustomers Find and Plug up Security Holes.

I. INTRODUCTION

Ethical hacking technology is spreading to diversified fields of the life and especially to all walks of computer industry; the need to protect the important data of the same should be addressed with right technology. Ethical Hacking emerged as the latest and futuristic technology of the computers, because of the smartness of hackers. Every small or big company is adopting this as the front layer of security for protecting their data. Understanding the true intentions of the general public is quite a hard task in these days, and it is even harder so, to understand the intentions of every single ethical hacker getting into vulnerable systems or networks. Technology is ever growing and people are encountering tools that are beneficial to them. If these tools falls into the wrong hands they can create great controversy, breaching our basic right to privacy, respect and freewill. The constant issues

Highlighted by the media always reporting some type of cyber crime, a study showing that nearly 93% of attacks happened inside of the organization raising concerns of how easy it is to be working inside to be able to infiltrate attacks.

TYPE OF ETHICAL HACKERS

Hackers can be divided into three groups:

White-Hats Good guys, include ethical hackers
Black-Hats Bad guys, include malicious hackers
Gray-Hats Good or bad hacker; depends on the situation

Ethical hackers usually fall into the white-hat category, butSometimes they're former gray hats who have becomeSecurity professionals and who now use their skills in anEthical manner.

White-Hats

White hats are the good guys, the ethical hackers who useTheir hacking skills for defensive purposes. White-hatHackers are usually security professionals with knowledgeOf hacking and the hacker toolset and who use thisKnowledge to locate weaknesses and implementCountermeasures. White-hat hackers are prime candidatesFor the exam. White hats are those who hack withPermission from the data owner. It is critical to get permission prior to beginning any hacking activity. This isWhat makes a security professional a white hat versus aMalicious hacker who cannot be trusted.

Black-Hats

Black hats are the bad guys: the malicious hackers or Crackers who use their skills for illegal or malicious Purposes. They break into or otherwise violate the systemIntegrity of remote systems, with malicious intent. HavingGained unauthorized access, black-hat hackers destroy vitalData, deny legitimate users service, and just cause problemsFor their targets. Black-hat hackers and crackers can easily

Be differentiated from white-hat hackers because theirActions are malicious. This is the traditional definition of aHacker and what most people consider a hacker to be.

Gray-Hats

Gray hats are hackers who may work offensively or Defensively, depending on the situation.

WORKING OF AN ETHICAL HACKER

The working of an ethical hacker involves the under mentioned steps: obeying the Ethical Hacking Commandments: Every Ethical Hacker must follow few basic principles. If he Does not follow, bad things can happen. Most of the time these principles get ignored or forgotten when Planning or executing ethical hacking tests. The results are even very dangerous.

2. Working ethically: The word ethical can be defined as working with high professional morals and principles. Whether you're performing ethical hacking tests against your own systems or for someone who has hired you, Everything you do as an ethical Hacker must be approved and must support the company's goals. No hidden Agendas are allowed. Trustworthiness is the ultimate objective. The misuse of information is absolutely not Allowed. Respecting Privacy: Treat the information you gather with complete respect. All information you obtain during
Your testing from Web application log files to clear-text passwords — must be kept private.

4. Not crashing your systems: One of the biggest mistakes is when people try to hack their own systems; they Come up with crashing their systems. The main reason for this is poor planning. These testers have not read the Documentation or misunderstand the usage and power of the security tools and techniques. You can easily create Miserable conditions on your systems when testing. Running too many tests too quickly on a system causes Many system lockups. Many security assessment tools can control how many tests are performed on a system at
The same time. These tools are especially handy if you need to run the tests on production systems during regular Business hours.

Executing the plan: In Ethical hacking, Time and patience are important. Be careful when performing.

Types of Attacks performed by Attacker:

1.Keylogger: Keylogger is an attack in which the attacker tries to capture the key strokes of keyboard and maintains a log file for it. The attacker may use it to gain access to the passwords or some login information.

2.Waterhole Attacks: This attack is basically done by making a clone for the website or wifi. This is being done by judging the people's schedule so that they can be attacked at that time. When the user logs in to the wifi and accesses the site, the attacker captures its information.

3.Dos (Denial of Service): In Denial of Service attack, the intruder sends multiple requests to the particular system, the requests are sent by the zombie computer whose task is nothing but to send fake requests just to make the actual systemslow down. It creates a lot of traffic through requests that the actual functioning of system gets slow.

4.Phishing Attack: In Phishing attack, the attacker sendsspam messages or emails to gain information about logins or credit card credentials.It may send messages which may seem to be from an authenticated source but actually it is not.

5.Cookie Theft: In this the attacker finds the information about the login of the user from the values that cookies store in the browser. For example,they may use cookie information to get your social media accounts hacked.6.Sql Injection: Sql Injection is placing of some code as a sql query at the time of authentication to get access to the application. By this they can also get access to the database,they can modify, delete or edit the entries in the database.

Advantages of ethical hacking:

This prevents identity theft and the leaking of vitalInformation.

□ It allows them to implement strongersecurity
Measures.

□ It is also beneficial to help government entities toProtect major computer system from being
Compromised in a way that national security
Would be an issue.

Preventing Security breaches of the system.□ You can have a computer system which is all secured from the malicious users.

Disadvantages of Hacking are−

□ Private informationcan be accessed by the hackers
Corrupting System operations
.□ Denial of service attacks□ Databases accessing
by malicious users.

ETHICAL HACKING MODES

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.

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.

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 of 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.

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.

II. 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.

III. 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.

REFERENCES

[1]. 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.

[2]. H.M David, "Three Different Shades of Ethical Hacking: Black, White and Gray," in GSEC Practical Assignment, Version 1.4b, Option 1, Feb 23, 2004.

[3]. Sanctum Inc, "Ethical Hacking techniques to audit and secure web enabled applications", 2002.

[4]. Smith B., Yurcik W., Doss D., "Ethical Hacking: the security justification redux", IEEE Transactions, pp. 375-379, 2002.