RESEARCH ARTICLE OPEN ACCESS

A Study on Hacking and Ethical Hacking

Dr. K. Mohan Kumar [1], K. Kavitha [2]
Research Guide & HOD of Computer Science [1], Research Scholar [2]
PG and Research Department of Computer Science,
Rajah Serfoji Government college, Thanjavur 613 005.
Tamil Nadu - India.

ABSTRACT

The state of security on the internet is very poor. Hacking is an activity in which, a person exploits the weakness in a system for self-profit or gratification. As public and private organizations migrate more of their critical functions or applications such as electronic commerce, marketing and database access to the Internet, then criminals have more opportunity and incentive to gain access to sensitive information through the Web application. Thus the need of protecting the systems from the hacking generated by the hackers is to promote the persons who will punch back the illegal attacks on our computer systems. Ethical hacking is an identical activity which aims to find and rectify the weakness and vulnerabilities in a system. Ethical hacking describes the process of hacking a network in an ethical way, therefore with good intentions. This study describes what is ethical hacking, what are the types of ethical hacking, impact of Hacking on Businesses and Governments. These papers also analyze the past history of hacking done by malicious hackers and give the most affected country and also the solutions to prevent our system from the hackers.

Keywords:- Hacking, Ethical Hacking

I. INDRODUCTION

Hacking has been a part of computing for 40 years. Some of the first hackers were members of the Massachusetts Institute of Technology (MIT) Tech Model Railroading Club (TMRC) in 1950s. Security is the condition of being protected against danger or loss. In general sense, security is a concept similar to safety. In the case of networks the security is also called the information security. Information security means protecting information and information system from unauthorized access, use, disclosure, disruption, modification, or destruction. The intent of hacking is to discover vulnerabilities so system can be better secured. Hackers may be motivated by a multitude of reasons, such as profit, protest, challenge, enjoyment or to evaluate those weaknesses to assist in removing them. Basic purpose of hacker is to know the system internally without any bad intension [1]. Computer hacking means someone alters computer hardware or software such that it can change the original content. The people who hack computers are known as hackers. Hackers are the experts who had learnt about the computer and the working of the computer [2].

Hacking

Hacking is the process of attempting to gain or successfully gaining, unauthorized access to computer resources. Computer hacking is the practice of modifying computer hardware and software to accomplish a goal outside of the creator's original purpose [1]. Hacking refers to gaining access to a computer to obtain information stored on it by means of password cracker software or any other technique to get data. This is done to either point out the loop holes in the security or to cause intentional sabotage of the computer. They are the computer programmers who have knowledge of computer programming and have enough information on the systems they are about to hack [2]. Thus a hacker whether he wants to sabotage the system or check its security will have to have exceptional knowledge of computers. Though they all have one nothing in common; they are trying to uncover a weakness in your system in order to exploit it [3].

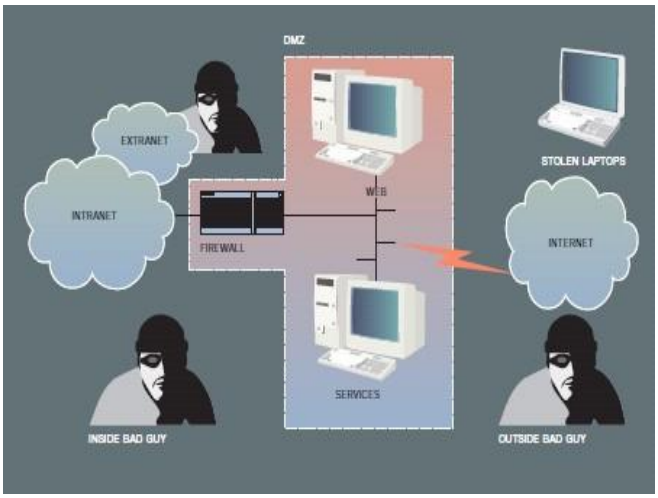


Figure- 1: Different ways to attack computer security

II. TYPES OF HACKING

The different types of hacking as given below

- **Website Hacking** – Website hacking means taking control from the website owner to a person who hacks the website. **Network Hacking** – Network hacking is generally means gathering information about domain by using tools like Telnet, Net stat, etc. over the network.
- **Ethical Hacking** – Ethical hacking is where a person hacks to find weakness in a system and then usually patches them.
- **Email Hacking** – Email hacking is illicit access to an email account or email correspondence.
- **Password Hacking** – Password hacking or password cracking is the process of recovering secret passwords from data that has been stored in or transmitted by a computer system.
- **Online Banking Hacking** – Online banking hacking is unauthorized accessing bank accounts without knowing the password or without permission of account holder.
- **Computer Hacking** – Computer hacking is when files on your computer are viewed, created, or edited without your authorization.

The following figure - 2 to shows the different types of hacking.

Figure- 2: Different types of hacking

Purpose of Hacking

There could be various positive and negative intentions behind performing hacking activities. Here is a list of some probable reasons why people indulge in hacking activities

- Just for fun
- Show-off
- Steal important information
- Damaging the system
- Hampering privacy
- Money extortion
- System security testing
- To break policy compliance [4].

Ethical Hacking

Ethical hacking is the process which is focuses on securing & protecting computer system. Independent computer security professional breaks into the computer system and neither neither damaged the target system nor steal the information, hacker evaluate target system security and report back to the owner about the threats found. Ethical hacking refers to the act of locating weaknesses and vulnerabilities of computer and information systems by duplicating the intent and actions of malicious hackers [5]. Ethical hacking, also known as

penetration tests, intrusion testing, or red teaming, is the controversial act of locating weaknesses and vulnerabilities of computer and information systems by duplicating the intent and actions of malicious hackers. The following figure - 3 to shows the ethical hacking.

Figure - 3 : Ethical hacking.

Ethical hacking is a way of doing a security assessment. Like all other assessments an ethical hack is a random sample and passing an ethical hack doesn't mean there are no security issues. An ethical hack's results is a detailed report of the findings as well as a testimony that a hacker with a certain amount of time and skills is or isn't able to successfully attack a system or get access to certain information. Ethical hacking can be categorized as a security assessment, a kind of training, a test for the security of an information technology environment. An ethical hack shows the risks an information technology environment is facing and actions can be taken to reduce certain risks or to accept them. The hacker can easily say that Ethical hacking does perfectly fit into the security life cycle shown in the below figure [3].

Figure- 4: Security Life Cycle

Ethical Hacking Process

Ethical hackers must follow a strict scientific process in order to obtain useable and legal results. The following figure -5 to shows the ethical hacking process.

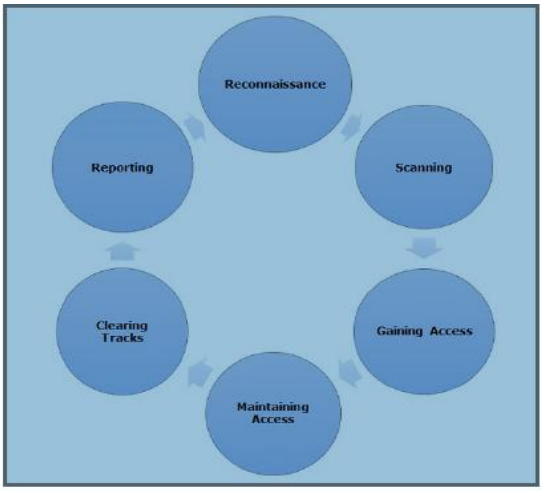


Figure- 5: Ethical Hacking process

Planning

- Planning is essential for having a successful project. It provides an opportunity to give critical thought to what needs to be done, allows for goals to be set, and allows for a risk assessment to evaluate how a project should be carried out.

- The planning phase will describe many of the details of a controlled attack. It will attempt to answer questions regarding how the attack is going to be supported and controlled, what the underlying actions that must be performed and who does what, when, where, and for how long.

Reconnaissance

- Reconnaissance (http://en.wikipedia.org/wiki/Vulnerability_scanner) is the search for freely available information to assist in an attack. This can be as simple as a ping or browsing newsgroups on the Internet in search of disgruntled employees divulging secret
- The reconnaissance phase introduces the relationship between the tasks that must be completed and the methods that will need to be used in order to protect the organization's assets and information.

Enumeration

- Enumeration is also known as network or vulnerability discovery. It is the act of obtaining information that is readily available from the target's system, applications and networks. It is important to note that the enumeration phase is often the point where the line between an ethical hack and a malicious attack can become blurred as it is often easy to go outside of the boundaries outlined in the original attack plan.
- At first glance, enumeration is simple: take the collected data and evaluate it collectively to establish a plan for more reconnaissance or building a matrix for the vulnerability analysis phase. However, the enumeration phase is where the ethical hacker's ability to make logical deductions plays an enormous role.

Vulnerability Analysis

- In order to effectively analyze data, an ethical hacker must employ a logical and pragmatic approach. In the vulnerability analysis phase, the collected information is compared with known vulnerabilities in a practical process.
- Information is useful no matter what the source. Any little bit can help in discovering options for exploitation and may possibly lead to discoveries that may not have been found otherwise. Known vulnerabilities, incidents, service packs, updates, and even available hacker tools help in identifying a point of attack. The Internet provides a vast amount of information that can easily be associated with the architecture and strong and weak points of a system.

Exploitation

- A significant amount of time is spent planning and evaluated an ethical hack. Of course, all this planning must eventually lead to some form of attack. The exploitation (http://en.wikipedia.org/wiki/Exploit_(computer_security)) of a system can be as easy as running a small tool or as intricate as a series of complex steps that must be executed in a particular way in order to gain access.
- The exploitation process is broken down into a set of subtasks which can be many steps or a single step in performing the attack. As each step is performed, an evaluation takes place to ensure that the expected outcome is being met.

Final Analysis

- Although the exploitation phase has a number of checks and validations to ensure success, a final analysis is required to categorize the vulnerabilities of the system in terms of their level of exposure and to assist in the derivation of a mitigation plan. The final analysis phase provides a link between the exploitation phase and the creation of a deliverable.
- A comprehensive view of the entire attack must exist in order to construct a bigger picture of the security posture of the environment and express the vulnerabilities in a clear and useful manner. The final

analysis is part interpretation and part empirical results.

Deliverables

- Deliverables communicate the results of tests in numerous ways. Some deliverables are short and concise, only providing a list of vulnerabilities and how to fix them, while others are long and detailed, providing a list of vulnerabilities with detailed descriptions regarding how they were found, how to exploit them, the implications of having such as a vulnerability and how to remedy the situation.
- The deliverable phase is a way for an ethical hacker to convey the results of their tests. Recently, ethical hacking has become so commoditized that if a deliverable does not instill fear into the hearts of executives, it could be considered a failure.

Integration

- Finally, it essential that there is some means of using the test results for something productive. Often, the deliverable is combined with existing materials, such as a risk analysis, security policy, previous test results, and information associated with a security program to enhance mitigation and develop remedies and patches for vulnerabilities [6].

Benefits of ethical hacking

- This type of "test" can provide convincing evidence of real system or network level threat exposures through proof of access. Even though these findings may be somewhat negative, by identifying any exposure you can be proactive in improving the overall security of your systems.
- An ethical hack, which tests beyond operating system and network vulnerabilities, provides a example, should your ethical hack prove that your firewalls could withstand an attack because there was no breach, but no one noticed the attacks, you may be better prepared to make a case for improving intrusion detection broader view of an organization's security. The results should provide a clear picture of how well your detection processes works as well as the response mechanisms that should be in place."Tests" of this sort could also identify weakness such as the fact that many systems security administrators may not be as aware of hacking techniques as are the hackers they are trying to protect against. These findings could help promote a need for better communication between system administrators and technical support staff, or identify training needs.
- Quite often, security awareness among senior management is seriously lacking.[3]

III. METHODOLOGY

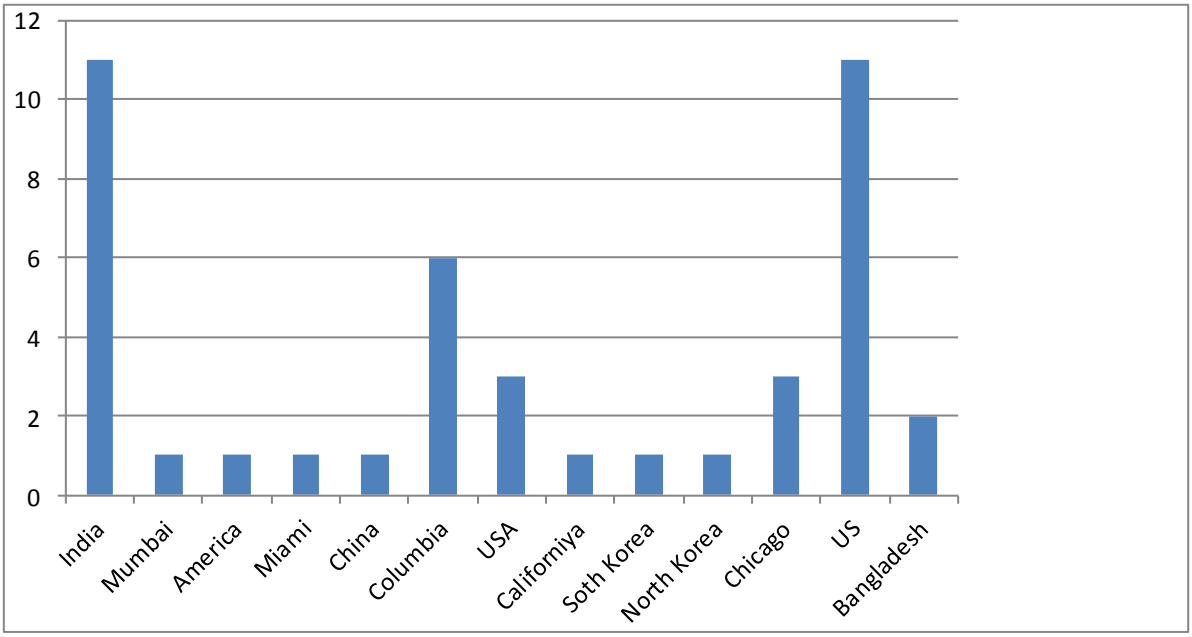
The various attacks happened in different country for this study is collected from various web resources. The consolidated history of attack arrived. Using this detail the most affected country is found and the protection mechanism to avoid the hacking is analyzed.

IV. RESULT AND DISCUSSION

The following table -1 to consolidated history of attacks.

COUNTRY	NO OF ATTACKS
India	11
Bangladesh	02
Russia	03
Mumbai	01
America	01
Miami	01
China	01
Columbia	06
California	01
South Korea	01
North Korea	01
Chicago	03
US	11

Table -1: Consolidated History



The following figure - 8 shows the diagrammatic representation of table -2.

Figure – 8: Attack history

The figure -8 shows India and US is having more attacks compare with other countries. So these countries should increase their security by implementing some new methods to avoid hacking. The following discussion gives an idea for the avoidance of hacking.

Methods to avoid Hacking

- **Create complex passwords.** User passwords to access your accounts on apps or websites should consist of a combination of numbers, upper- and lower-case letters, and special characters that is difficult to guess. Don't use the same password for more than one website or account. This limits the damage to you if a hacker happens to crack one of user passwords.

- **Use a password manager**. Password managers store and auto-fill your credentials for different sites, allowing you to create a complex and unique password for each site without having to worry about entering the password itself more than once. While you should absolutely keep track of you passwords on your own as well, a password manager will help make your device much more secure.

- **Don't give out your password.** This is an obvious piece of advice, but one that bears revisiting: with the exception of some school services, you shouldn't ever have to provide a site administrator with your password for them to access your account. This logic applies to IT workers and Microsoft or Apple representatives. Similarly, don't tell people your phone or tablet's PIN or pass code combination. Even your friends might accidentally tell someone your pass code. If you do have to give someone your password for some reason, change it as soon as they are done with whatever they needed to do on your account.

- **Change user passwords often.** In addition to keeping your password a secret, user should change the passwords on your various accounts and devices at least once every six months. Be sure not to use the same password twice (e.g., your Facebook password should be different than user bank password, etc.). When user do change users password, user should change it substantially. Don't simply replace one letter with a number.

- **Use two-factor authentication.** Two-factor identification requires you to enter a code sent to user in a text message or another service to access your account after you enter your user name and password. This makes it more difficult for a hacker to access your information, even if hacker sare able to crack user password. Most major websites, including popular social media networks, have some form of two-factor authentication available. Check your account settings to learn how to enable this feature. The hacker can set up two-step verification for your Google account. Popular app alternatives to receiving a text message include Google Authenticator and Microsoft Authenticator.

- **Read privacy polices carefully**. Any company that has information from user must have a privacy policy that details how they use that information and the extent to which they share it with others. Most people simply click through the privacy policy without reading it. Although the reading can be cumbersome, it's worth at least skimming it so you know how user data is being used. If hacker see something in the privacy policy that you disagree with, or that makes you uncomfortable, hacker want to reconsider sharing information with that company.

- **Log out of accounts when you're done with them.** Simply closing the browser window isn't always enough, so make sure you click (or tap) on your account name and select Log Out (or Sign Out in some cases) to manually sign out of your account and remove your login credentials from the site.

- **Make sure you're on an official website when entering passwords.** Phishing scams – instances in which a malicious page pretends to be a login page for a social media or bank account – are one of the easiest ways for hacker to get hacked. One way to spot phishing scams is to look at the site's URL: if it closely resembles (but doesn't exactly match) a reputable site's URL (e.g., "Faecbook" instead of "Facebook"), it's a fake site. For example, enter your Twitter login information on Twitter's official page only. Avoid doing so on a page that asks for the login information in order to share an article or something similar. An exception to this rule is when a university uses an existing service (e.g., Gmail) through their home page.

- **Use secured wireless networks.** Generally speaking, secured networks require hacker to enter a password before hacker can connect to them. In some locations (such as airports or coffee shops), hacker can request the password after purchasing an item. If the wireless network isn't secured, your computer will let hacker know before connecting. In some operating systems, there will also be an exclamation mark next to the network's name. If hacker have to use the internet but don't have access to a secure network, change your passwords immediately the next time user log into a secure network. If hacker has a wireless network at home, make sure it's secure and encrypted.

- **Download programs only from reputable sites.** This methodology goes for sites user visit on an unsecured connection as well. If there isn't a padlock icon to the left of the URL address and "HTTPS" in front of the "www" portion of the URL, it's best to avoid the site (and downloading anything from it) entirely if possible. Learn to recognize fake websites. In addition to avoiding sites without "HTTPS" and the padlock icon next to the URL, double-check the website's URL before entering your password on it. Some sites will attempt to steal your login information by posing as another site (this is known as a phishing scam); you can spot these sites by looking for extra (or missing) letters, dashes between words, and extra symbols. For example, a site masquerading as Face book might have faceboook.com as its URL. Sites which display dashes between multiple words in the site name itself (the words in between "www" and ".com") are generally not reliable.

- **Avoid file sharing services.** Not only does file sharing often violate intellectual property laws, but file sharing websites are crawling with hackers. User may think you're downloading the latest hit song or a new movie, but the file actually is a virus or malware in disguise. Many of these files are designed in such a way that the virus or malware hidden within won't be picked up by anti-virus software screenings. The virus won't infect your system until you try to play the file.

- **Shop only on secure sites**. Don't enter account or credit card information on a site that doesn't have "https://" written before the "www" section of the website address. The "s" indicates the site is secure. Sites without that won't encrypt or protect your data.

- **Keep personal information off social media.** User may think you're just sharing with friends, but revealing too much about yourself and your life on social media can make you vulnerable to hackers. Share personal information directly with people who need to know rather than openly posting on social media [10].

V. CONCLUSION

Hacking has its benefits and risks. Hackers are very diverse. They may bankrupt a company or may protect the data, increasing the revenues for the company. The battle between the ethical or white hat hackers and the malicious or black hat hackers is a long war, which has no end. While ethical hackers help to understand the companies security needs, the malicious hackers intrudes illegally and harm the network for their personal benefits. Ethical Hackers help organizations to understand the present hidden problems in their servers and corporate network. Ethical Hacking is a tool, which if properly utilized, can prove useful for understanding the weaknesses of a network and how they might be exploited. This also concludes that ethical hacking is an important aspect of computer world. It deals with both sides of being good and bad. Ethical hacking plays a vital role in maintaining and saving a lot of secret information, whereas malicious hacking can destroy everything. This study analyzes the hacking done by the malicious hackers.

REFERENCES

[1] Sova Pal (Bera) “Overview of Hacking” IOSR Journal of Computer Engineering (IOSR-JCE).

[2] Suriya Begum*, Sujeeth Kumar, Ashhar “A comprehensive study on ethical hacking” international journal of engineering sciences & research technology.

[3] Bhawana Sahare, Ankit Naik, Shashikala Khandey “Study Of Ethical Hacking” International Journal of Computer Science Trends and Technology (IJCST).

[4] https://www.tutorialspoint.com/ethical_hacking/ethical_hacking_overview.htm Copyright © tutorialspoint.com
[5] From Computing and Software Wiki "Ethical Hacking"
[6] https://www.tutorialspoint.com/ethical_hacking/ethical_hacking_process.htm Copyright © tutorialspoint.com