Defence against Different Approaches of Password Hacking In Context to Pakistan

Imran Mazhar*1, Maria Latif*2, Tamoor Wakeel*3, Iqra Amjad*4

Abstract- Technology has flourished and impacted our lives like never before. With the ever-increasing impact of technology the issues related to technology have increased. Specifically, the issues related to the passwords hacking and password breakouts gave rise to a new alarming situation. In this research, we discuss how hackers started hacking passwords in the USA in the beginning. It describes different types of tools and applications i.e. Cain and Abel, John the ripper that uses CPU core to crack the password etc. This research also provides information of how and which type of passwords users select i.e. mnemonics and randomly generated a password and also discuss all the types of passwords i.e. textual, graphical passwords etc. and identify the different methods of attacks for hacking them i.e. dictionary attack, hybrid and brute force approaches. By the study of existing research, we identify which hacking method is most common in history and analyze the appropriate used solution to prevent password hacking.

Keywords-Password, Hacking, Attacks, Brute force, Dictionary, Key Loggers, two-factor Authentication

I. INTRODUCTION

The huge development of internet has brought varied nice things like electronic commerce, email, and straightforward access to tremendous stores of reference material then forth. Associate Degree ever increasing the range of computers gets related to the net, wireless devices and networks square measure blasting. attributable to the propel innovation of the net, the administration, non-public trade and therefore the regular pc shopper have fears of their data or non-public knowledge being contained by a criminal hacker. These forms of hacker's square measure referred to as black hat hackers who can covertly take the association's knowledge and transmit it to the open net. During this approach, to beat from these real problems, another category of hackers appeared and these hackers square measure named as moral hackers or white hat hackers. This paper portrays moral hackers, their techniques and the way they approach serving to their purchasers and fitting up security openings. during this approach, if there ought to be an incident of PC security, neither hurt the target frameworks nor take knowledge.

- *Imran Mazhar is pursuing master's degree program in Information Technology in University of Lahore, Gujrat Pakistan. PH-+92344626360. E-mail:imranmazhar23@yahoo.com*
- *Tamoor Wakeel is pursuing master's degree program in Information Technology in University of Lahore, Gujrat Pakistan. PH-+923016261819. E-mail:tamoor.wakeel72@gmail.com*
- *Iqra Amjad is pursuing master's degree program in Software Engineering in University of Lahore, Gujrat Pakistan. PH-+923328398122. E-mail:iqra.amjad2526@gmail.com*
- *Maria Latif University of Lahore, Gujrat Pakistan, maria.latif@cs.uol.edu.pk*

these tiger teams or moral hackers would utilize similar traps and techniques that hacker utilizes nevertheless in a very legitimate approach and that they would. Rather, they might assess the target framework's security and report back to the proprietors with the vulnerabilities they found and pointers for the way to cure them. This- paper can characterize moral hacking, show some of the usually utilize terms for aggressors, provides a summing up of the quality administrations offered by suggests that of moral hacking to battle assailants, point out problems and their preventions [3].

II. WHAT IS HACKING?

Hacking is not a basic activity or arrangement of charges a constant variety of people suppose. It is selected term; there square measure varied types of hacking. Hacking is unapproved utilization of system assets. Laptop hacking is that the act of fixing laptop instrumentality associated programming to attain an objective outside of the maker's distinctive reason. People who participate

in laptop hacking may be a coder who breaks into another person's laptop or data while not authorization [3].

ETHICAL HACKING:

The art of testing your computers and system for security vulnerabilities and stopping terrible people get a chance to misuse them. Moral hacking and moral hacker area unit terms accustomed to portraying hacking performed by a company or individual to assist acknowledge potential to a laptop or system. To induce a criminal, combat an analogous attitude as a cheat. That is the reason for moral hacking. ...includes similar apparatuses, traps, and systems that hackers utilize, nevertheless with one noteworthy distinction: moral hacking is legitimate. The set of moral hacking is to seek out vulnerabilities from a hacker's perspective. It is a piece of a general information. Probability administration program that takes into consideration progressing security enhancements. Moral hacking will guarantee that sellers' regarding the safety of things area unit legitimate [3].

PASSWORD HACKING:

Password hacking is the process of repetition and guessing and try to hack the system. The recovering of passwords from data that are in a computer system is also a password hacking [6]. In history, the first hacker came as an expert programmer to solve any technical problem. The word hacker came from English language word “Russian” that means “the people who chop badly”. They do several disgusting acts to their victims, with their skills to attack and hack the system with computer [4]. Whereas the password is a secret word and string of characters against any system information and resources. It is kept protected and hides for those who are not authentic to use their systems [6].

HACKING CULTURE:

In 1960 and 1970 as the result of intelligent movement: knowing the unknown information and methods and exploring them, and do what others cannot are the beginnings of hacker culture. Many hacker cultures are developed independently and in combination with other hacker culture. After combining these links are able to share any kind of information, their experiences, knowledge, humor, and skills with each other. In this first hacker culture begins [4].

III. CHARACTERISTICS

Password hacking is increases incredibly and an amazing rate every year. The effects of password hacking are disgusting and expensive. Millions of sensitive, amazing and important information are stolen by hackers every year at a higher rate. For the year 2002, from the survey by the Computer Security Institute, Business Company and organizations can afford a loss of more than $70 million by the stolen of proprietary information by the hackers. In 2002, from credit cards.com 55,000 and from UD Universe .com 300,000 credit cards numbers have been stolen by hackers [1].

IV. PROBLEM STATEMENT

By reviewing the previous works of literature on password hacking adaptation from the citizens perceptive. It is concluded the password hacking is broad in their field in all over the world. Our main problem issue is password hacking .the main reason behind password hacking is a weak password. The people mostly select numbers as their password which is easily hacked and don't provide strong protection against password hacking. In this research discuss methods of password hacking and also provide a various solution how to minimize password hacking. Thus we need is to provide strong both in logical and theoretically framework for protection against password hacking.

V. OBJECTIVES OF RESEARCH

The main purpose of our research is to found out all reasons and also all possible different methods of password hacking. For this purpose analyses all the relative previous researches and examine password hacking issue, then suggests the best solution that provides security to users and also provides comfort and the implement our solution.

Identify the reasons and methods of password hacking.

In the aspect of previously all researches, examine the issues.

Suggests and perform our solutions.

VI. LITERATURE REVIEW

Before ten years ago, few famous tools used for password hacking i.e. Cain and Abel and John the Ripper are frequently. For cracking the hashes of a password into a plaintext form CPU core power is used by these password hacking tools. It will take days and years, if the password is complex and strong i.e. include special characters, numeric, alphanumeric etc to bring out the plaintext of passwords from a hash of passwords.

Here are the main TEN best hacking approaches recorded beneath:

NMAP

This is often also alluded to as in light of the fact that the Swiss knife of hacking. This is often to a great utilized in foot printing segment to examine the ports of the targeted workstation ports is open.

WIRESHARK

It catches all networks movement including a network connector. It breaks down for succulent data like usernames and passwords to perform network investigating.

CAIN AND ABEL

It is the speedy method in history created with the aim of hacking the weak UNIX and Windows LM hashes and passwords. This could be wont to split window watchword. It moreover performs man inside the center assaults, catches network passwords and so forth [7].

JOHN THE RIPPER:

It is locally password hacking application developed with network administration and penetration testers in mind. It records VOIP conversation, examine routing protocols by performing as a sniffer in networks, it uses brute force attacks and cryptanalysis attacks to hack passwords [3].

METASPLOIT

It's an expansive data of exploits. It's the last word hacking instrument to "hack" a PC. It's the best utilization in Linux. Burp suite might be a net intermediary instrument that is utilized to check the internet application security. This could savage power any login compose in an extremely program. This apparatus is beneath windows and Linux conditions [3].

AIRCRACK-NG

Air cracking might be an arrangement of apparatuses wont to split wireless constancy passwords. This moreover comes beneath Linux setting.

NESSUS

This is often a thoroughly programmed shortcoming scanner. One should give data preparing address as info and it'll check that deliver to search out the shortcoming in that framework[13].

THC HYDRA

This is a fast saltine instrument. It splits passwords of remote systems in the network. It will split passwords of the numerous protocols and also FTP, HTTP. It comes underneath Linux setting [3].

HPING3

Hping3 sends ICMP, UDP or correspondences parcels so shows answers. This apparatus is a great degree supportive once endeavoring to follow course/ping/test that has firewalls blocked normal pings. This comes beneath windows and Linux [13].

PUTTY

It is a horrendously incredible instrument for the hacker. SSH and telnet, which might be won't interface with remote computers. The utilization putty after you need to join your arrival machine from your PC. It might likewise to perform SSH burrowing sidestep firewalls [3].

VII. TYPES OF PASSWORD'S HACKING:

The different types of password and their methods of hacking them are as follow:

1. TEXTUAL PASSWORD:

In this password is in the form of text form and in graphical form. It is the easiest password type to use. But this method is hacked very easily. The methods by which textual passwords are hackers are as follow: The textual password in lengthen is short which is hacked by hackers by guessing in two or three attempts. It is easily guessed by shoulder surfing of users. The suddenly break down of a user does not shut down the site that user open, by restarting, the hacker easily guessed a password [14].

2. GRAPHICAL PASSWORD:

A Textual password is based on graphical password. These images are set as a password. It is performed or constructed in the grid format. It is also be guessed by shoulder surfing [2]. The hackers select the following two types of passwords most commonly for hacking.

- **MNEMONIC PASSWORDS:**

The 20% hackers hack mnemonic passwords because this includes phrases which are easy to memorize.

- **RANDOM PASSWORDS:**

This type of password includes both upper case and lower case letters. It is created from the internet by using the random generator. It is difficult to hack [5].

VIII. METHODS OF PASSWORD HACKING:

There are many methods of hacking password discussed here.

- **DICTIONARY:** This is simply a collection of words. If your password is simple word it is easily hacked.

- **HYBRID:** This includes text as well as numbers and it is similar to dictionary attack but hacker inserts numbers at the end.

- **BRUTE FORCE:** forcefully select each and every number in every attempt and don't give up until a password is cracked. The most common variation of password hacking is to select user names. The user simply used password as a word with their name first and then any other characters. e.g.: aishanthna. In this Aisha is simply a password. It is viewed that it's simply be cracked in just 8 attempts [6].

- **KEY LOGGER ATTACK**: A hacker uses a program to track all of a user's keystrokes. So at the end of the day, everything the user has typed—including their login IDs and passwords—have been recorded. A key logger attack is different than a brute force or dictionary attack in many ways. Not the least of which, the key logging program used is malware (or a full-blown virus) that must first make it onto the user's device (often the user is tricked into downloading it by clicking on a link in an email). Keylogger attacks are also different because stronger passwords don't provide much protection against them, which is one reason that multi-factor authentication (MFA) is becoming a must-have for all businesses and organizations [1].

- **TWO-FACTOR AUTHENTICATION:** With two-factor authentication (also called multi-factor authentication, 2FA, and advanced authentication), a user is required to not only provide a password to gain access to the system, but also a another security "factor," like a unique one-time access code generated from a token device or secure mobile app on their Smartphone. A network protected by MFA is nearly impenetrable to an outside attack; even if a hacker is able to attain a system password, he won't be able to provide the needed second security factor. [1].

- **RAINBOW TABLE ATTACK**: Rainbow tables aren't as colorful as their name may imply but, for a hacker, your password could well be at the end of it. Rainbow tables are attractive as it reduces the time needed to crack a password hash to simply just looking something up in a list. However, rainbow tables are huge, unwieldy things. They require serious computing power to run and a table becomes useless if the hash it's trying to find has been "salted" by the addition of random characters to its password ahead of hashing the algorithm. They would likely only work with a predefined "random character" set and password strings below 12 characters as the size of the table would be prohibitive to even state-level hackers otherwise[2].

- **PHISHING:** There's an easy way to hack: ask the user for his or her password. A phishing email leads the unsuspecting reader to a faked log in the page associated with whatever service it is the hacker wants to access, requesting the user to put right some terrible problem with their security. That page then skims their password and the hacker can go use it for their own purpose [2].

- **SOCIAL ENGINEERING**: Social engineering takes the whole "ask the user" concept outside of the inbox that phishing tends to stick with and into the real world. A favorite of the social engineer is to call an officer posing as an IT security tech guy and simply ask for the network access password. You'd be amazed at how often this works. Some even have the necessary gonads to don a suit and name badge before walking into a business to ask the receptionist the same question face to face [2].

- **MALWARE:** A key logger, or screen scraper, can be installed by malware which records everything you type or takes screenshots during a login process, and then forwards a copy of this file to hacker central. Some malware will look for the existence of a web browser client password file and copy this which, unless properly encrypted, will contain easily accessible saved passwords from the user's browsing history [2].

- **OFFLINE CRACKING:** It's easy to imagine that passwords are safe when the systems they protect lock out users after three or four wrong guesses, blocking automated guessing applications. Well, that would be true if it were not for the fact that most password hacking takes place offline, using a set of hashes in a password file that has been 'obtained' from a compromised system.

- **SHOULDER SURFING:** The most confident of hackers will take the guise of a parcel courier, aircon service technician or anything else that gets them access to an office building. Once they are in, the service personnel "uniform" provides a kind of free pass to wander around unhindered, and make note of passwords being entered by genuine members of staff. It also provides an excellent opportunity to eyeball all those post-it notes stuck to the front of LCD screens with logins scribbled upon them [2].

- **SPIDERING:** Savvy hackers have realized that many corporate passwords are made up of words that are connected to the business itself. Studying corporate literature, website sales material and even the websites of competitors and listed customers can provide the ammunition to build a custom word list to use in a brute force attack [2].

- **GUESS:** The password crackers best friend, of course, is the predictability of the user. Unless a truly random password has been created using software dedicated to the task, a user-generated 'random' password is unlikely to be anything of the sort. Instead, thanks to our brains' emotional attachment to things we like, the chances are those random passwords are based upon our interests, hobbies, and pets, family and so on. Password crackers are very likely to look at this information and make a few - often correct - educated guesses when attempting to crack a consumer-level password without resorting to dictionary or brute force attacks [2].

Password-based on text is easier to hack. Hacker commonly hacked passwords of servers of a large organization and the use it again and again for all these computers who use this password [7].

IX. HACKING PROTECTION TECHNIQUES

In the importance of various hacking exercises, some of the recommended insurance systems zone unit

SECURITY INFRASTRUCTURE

One among the principal basic frameworks for forcing information security is the firewall that goes for forbidding access of approaching and leaving movement through the setup of control sets [2].

INTRUSION DETECTION SYSTEM

It is a shields network by gathering info from diffusion of the framework and network offer, therefore examining the knowledge for security problems. It provides day and age perception and examination of shopper and framework action. once all is claimed in done, there is a unit a pair of types of IDS, significantly Network Intrusion Detection System (NIDS) screens varied has by viewing network activity at the network limits and Host Intrusion Detection System (HIDS) can screen application logs, recording framework adjustments like Microsoft word document and administration records[4].

X. DEFENSE AGAINST PASSWORD HACKING:

The users must follow the following instructions to protect their password against hacking:

Passwords can be cracked quickly if has the only consisted of numbers. So, never use only numbers. Special numbers and characters, upper and lower case letters are used for passwords.

Produce acronyms from a recipe or a term or misspell words and use it as a password. E.g. American Standard Code for Information Interchange is an abbreviation of ASCII code, so as a part of password they can be used for password security [4].

If they're suspected of being compromised on password hacking, instantly alter passwords every 7 to 13 months.

For mesh or webbing framework hosts, i.e. firewalls, servers, and routers Linux systems Use different passwords for each system. So, they cannot be hacked easily [8].

If user's hard drives are encrypted, unlocked screens are a great way for systems to be compromised or be protected. So, Use password-protected screensavers for password security. [9].

Password Managers:

In this research use randomly generated alphanumeric characters of at least 20 in lengthen. Last Pass, Dash lane, Robo Form, 1 Password or Secure are rood stage favors that moreover to native apps work via the mobile Web.

Two-Factor Authentication:

Apple, Twitter, Dropbox etc all use two-factor authentication, when new device login into the site or service. Within a temporary password, it sends you a text message when the user tries to log in to the site. Even if a hacker has your account password, it alerts you that someone tries to hack your password. Thus without your temporary password send to you and mobile, you are not login into your own account [1].

XI. Application and other particular assaults:

Applications take an excellent deal of hits by hackers. Projects, as an example, the email server software system and internet applications usually area unit pummeled: machine-readable text Transfer Protocol (HTTP) and straightforward

- Mail Transfer Protocol (SMTP) applications area unit often ill-treated on the grounds that almost all firewalls and alternative security systems area unit organized to modify full access to those comes from the web. Malicious software system (malware) incorporates [6].

- Infections, worms, Trojan steeds, and spyware. Malware obstructs networks and brings down systems. Spam (garbage email) is wreaking ruin on the framework

- Accessibility and storeroom. And it will convey malware. Moral hacking uncovers such assaults against your laptop systems [7].

XIV. METHODOLOGY

The purpose of this paper is to understand the password hacking and methods i.e. how we do password hacking. For this purpose i.e. understand this issue collect data from all relative research paper, relative books, magazines, articles, and reports of all the previous researchers. So, in this research collect the secondary data and then implement our solution to avoid the issue of password hacking and provide comfort to users to use their accounts. Examine and evaluate the all previous researches to understand which methods mostly hackers used to perform password hacking and which solution is widely and commonly provided by the previous researches to solve this issue and that provide comfort to the user [8]. To achieve our purpose of reducing the password hacking, first, see the previous research on password hacking methods and how they affect the users and then focus on the solutions of these issues. So, in this research collect data and perform an action on it. So, Experimental methodology is used in this research [9].

XV. SCOPE & LIMITATIONS:

The research main purpose is to solve password hacking issue with respect to Pakistan. But besides discussing the methods and providing solutions to this problem, define the scope and also limitation of our research [9].

SCOPE:

The methods and solutions that we provide to solve the password hacking issue are only applicable inside Pakistan, so it is not generalize.

The solution that suggests solving the password hacking issue is only within the computer hacking domain. So it is not generalized.

First study all the previous researches of different researchers of different countries on password hacking problem then analyses all the possible solutions that they provide to avoid password hacking.

Our research provides a base for future work, as very little effort has been made in Pakistan to solve the issue. In this way, the next researcher can work on it more deeply and provide a much more effective solution to eliminate this issue [6].

LIMITATIONS:

The solution that suggests after a thorough analysis of previous researches of different researchers may not solve all issues of password hacking. As new technology introduces every day, at that time the outcomes of our research may not be so effective.

The solutions that provided is not generalized, it only is applicable in Pakistan.

The solutions may be applicable only according to the time, as time changes new technology is introduced and that time our research may not be useful for the users and its outcomes may not be very affected [9].

XVI. CONCLUSION:

Nowadays password hacking is a great issue in Pakistan. The feel hesitation for creating accounts online due to fear of password hacking. The main objective of this research is to identify the various passwords types and define different methods, how to hack them and which resources are used for the hacking by hackers and to identify the solutions of these problems by studying the researcher’s previous papers and discuss which method is most commonly is used to reduce the password hacking issue. The most effective solution to solving this problem is to use two-factor authentication. In this for login into your own account, your mobile and temporary password which is provided by the system admin is required. When some other people who have your correct password try to use your password and attempt to hack it, the system automatically alerts the users. As technology gets vast in its field from time to time, password hacking is also increasing incredibly. As the government gives permission to legally hack the passwords, but the ratio of illegal password hacking is very high. The Government takes strict reaction on this type of action.

XVII. REFERENCES:

[1] V. C Jason. Computer Hacking: Making the Case for a National Reporting Requirement: No. 2004-07 ,4/2004.

[2] C. Banita & Dr G. Puneet .3d Password –A Secure Tool: January 2014, Volume 4, Issue 1.

[3] John A. Chester, "Analysis of Password Cracking Methods & Applications", 2015.

[4] History & Impact of Hacking: final paper from history of computing.

[5] B. Jorgen , W. N Rune ,Martin J. Gilje . All in a day's work: Password cracking for the rest of us.

[6] T. Predrag .Passwords attacks and generation strategies.

[7] O.Jim and M. Jeanna . A Study of Passwords and Methods Used in Brute-Force SSH Attacks .

[8] Q. Sahar . Using SMS Authentication to Diminish Privacy Issues in E Services.

[9] Harold Tipton and Micki Krause. Information Security Management Handbook 4 th Edition, Volume 3. Boca Raton: Auer Bach Publications, 2002.