INFORMATION SECURITY PROJECT

Submitted to: Ma'am Mukhtair Bano

Submitted by: Aqsa Tabasum (002)
Shamsa Kanwal (028)

Title: Password Attack

PASSWORD ATTACK

PASSWORD ATTACKS:

In our daily life, passwords play an important role as almost every computing application requires password like ATM machines, Windows login and internet services etc. The purpose of password is to restrict the unauthorized access to information. Although passwords are used for security purpose but they do not provide much protection since there are flaws in the conventional password systems. When an attacker wants to steal our password, it is referred to as password attack.

BACKGROUND:

Since the beginning of time, people have used passwords. Entrances would ask people who wanted to get into a certain area for a password or watchword and would only let a person or group through if they knew the password.

In the military, passwords grew to include both a password and a counter password. For example, in the first days of the Battle of Normandy, paratroopers of the U.S. 101st Airborne Division used the password "flash," which was given as a challenge and answered with the correct answer, "thunder." Every three days, the challenge and the way to answer it changed. On D-Day, American paratroopers were known to use a device called a "cricket" instead of a password system as a temporary way to identify themselves. When the "cricket" gave a metallic click as a password, the responder had to give two clicks in return.

The standard explanation for why passwords don't work is that they are both too long for people to remember and too short to be secure. It's easy to see how this conclusion could be reached. If we only use letters and numbers, there are about 26 passwords with one character, 212 passwords with two characters, etc. The fastest systems for cracking passwords can check about 236 passwords per second. If you want a password that takes a year to crack, it needs to be at least 10 characters long.

The UNIX operating system, which was made in the 1970s, was the first to have a password system. Before personal computers, most computers were shared by multiple people. Each person had their own account, and the operating system kept each user's data safe from the other users. Someone else couldn't get into your account if they didn't know your password.

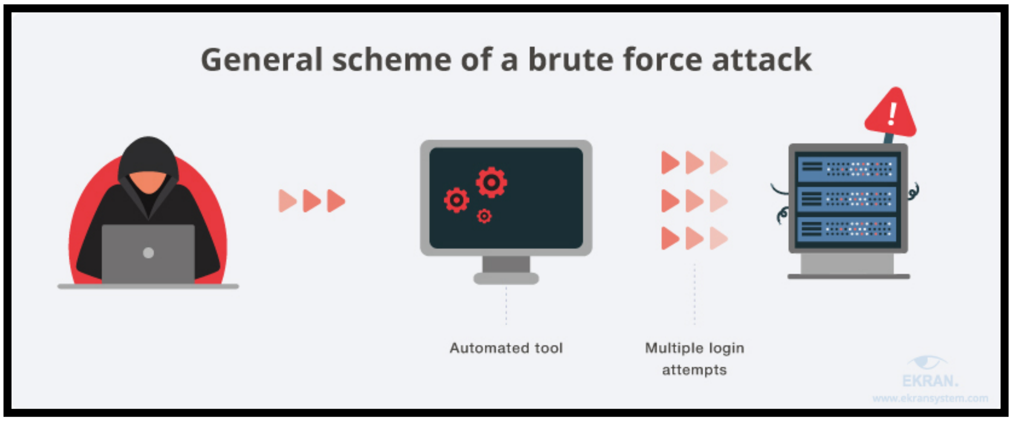
The people who made UNIX figured out that it would be better to use what is now called "password hashing." Instead of storing the actual password, you store what is called a "one-way function" of the password. A one-way function is just a function H that is easy to compute in one direction but not in the other. 1 This is usually done with something called a "hash function." The process of doing this is called "password hashing," and the values that are stored are called "password hashes."

In this case, that means you store the pair (Username, H (Password)). When the user tries to log in, you take the password they enter, P, and figure out H. (P). If H (P) is the same as the stored password, you know for sure that their password is correct, so you let them log in. If H (P) is not the same as the stored password, you return an error. The cool thing about this design is that even if the password file is leaked, the attacker only learns the hashes of the passwords.

TYPES OF PASSWORD ATTACK:

1. BRUTE FORCE:

In this form of attack, every known password combination is used to crack the password. The brute force approach is commonly used to crack encrypted passwords that are maintained as encrypted text. MD5 hashing scheme is used for the purpose of storing the passwords in early Linux systems. User names and their passwords are stored in the password file which is available in operating system. If an attacker gets access to this file then the passwords can be guess. Passwords are encrypted in the form of MD5 hash, in order to get the password the attacker extract MD5 hash from the password file which is available on the target system. One by one all MD5 hashes are matched with the hash. Password got selected when the hashes matched. Brute force attacks are considered as time consuming because they required searching the hash from all the options.



PREVENTIVE MEASURES FROM BRUTE FORCE ATTACK:

- Increase password length
- Increase password complexity
- Use multi-factor authentication
- Limit login attempts

REAL TIME EXMAPLES:

Attack:

- In 2016, a brute force assault on the popular ecommerce site Alibaba compromised the credentials of approximately 21 million customers. During the incident, which occurred between October and November of that year, the attackers accessed the usernames and passwords of 99 million individuals without authorization.

Reason:

- The fundamental source of the assault, according to experts, was the duplication of passwords by users. It was observed that the majority of platform users shared their passwords with their other accounts. Weak passwords were a contributor to the assault. Some of the users had passwords that were simple to crack.

Attack:

- In August 2020, the Canadian Revenue Agency (CRA) was infiltrated by a brute force assault that compromised around 11,000 CRA and other government-related accounts.

Reason:

Experts found out that the hackers used stolen login information, such as usernames and passwords, to get into the affected systems. The attack showed again that you shouldn't use the same password for more than one website or account. You can stop brute-force attacks by giving yourself strong passwords.

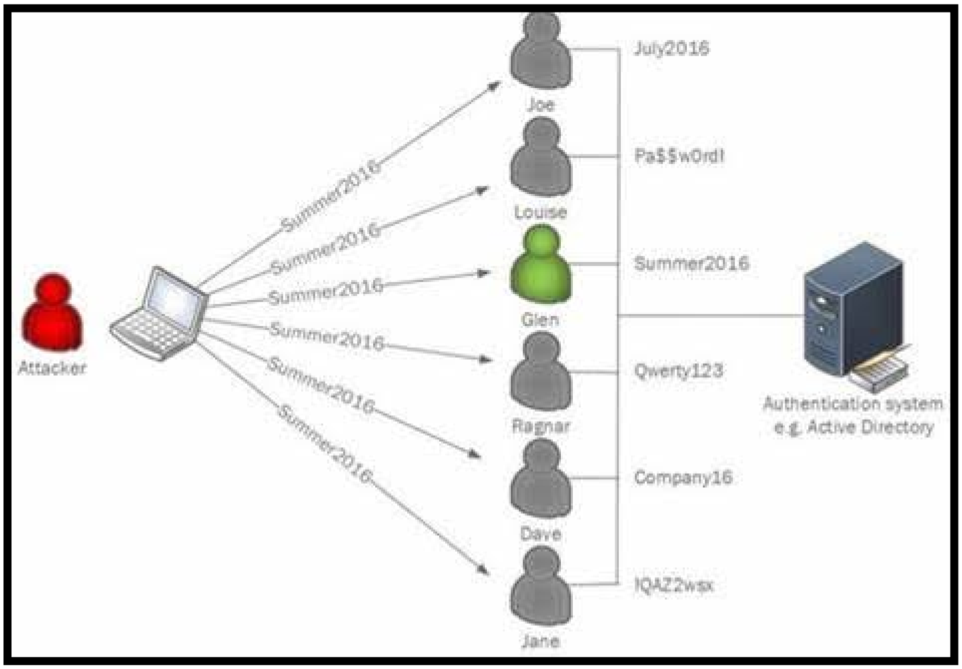
Attack:

- In 2018, the Northern Irish Parliament was the subject of a brute force attack that compromised some of its members' accounts. Investigations into the attack indicated that it was launched from outside sources. The attackers gained access to assembly members' mails by attempting several passwords. The compromised accounts were terminated, and lawmakers were asked to reset their passwords to something more secure. They were instructed to utilize passphrases instead of single words.

2. **PASSWORD SPRAYING:**
   By the use of few commonly used passwords, the attacker attempts to access large number of accounts, known as password spraying. The target of password spraying attack is on large number of account while the brute force attack targets a single account and guesses the password of it. Password spraying attack is also known as “low and slow” method because the attacker first tries a single password such as password123 or summer2022 to all

targeted accounts before moving to the second attempt of password. The targeted applications of password spraying include:

- Cloud based applications
- Email applications
- Single sign-on applications



PREVENTIVE MEASURES FROM PASSWORD SPRAYING ATTACK:

- Active Directory password protection should be enabled; it allows the administrators to eliminate the commonly used or easily guessable password.
- Conduction of simulated attack of pen testing, it helps to judge how vulnerable measures you organization password have.
- Password less User access should be implemented; organization is offering biometric verification and excluded the feature of password.

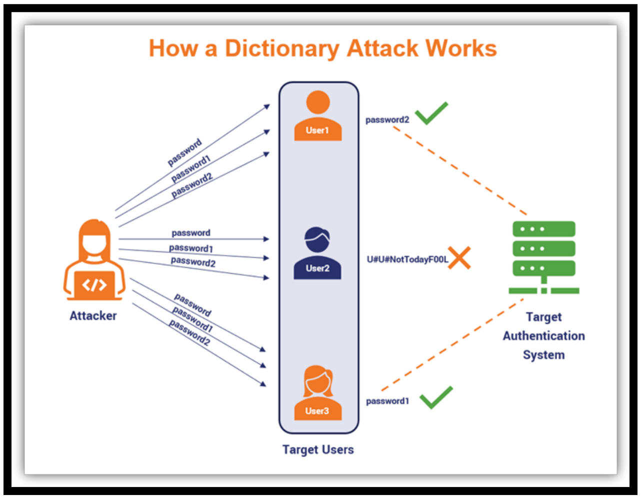
REAL TIME EXAMPLE:

In 2013 a victim of password spraying attack said:

"When my bank was the target of a password spraying attack, I was requested to change my password." It turns out that a hacker tried millions of login and password combinations against the bank's users - and I was one of them."

3. DICTIONARY:

Dictionary attacks are relatively faster the brute force attacks. Instead of checking every possible option for a password as we do in brute force, the dictionary attack uses specific passwords like many users use name of their birds, familiar places or favorite personalities as a password. Passwords of such a type can be guessed by dictionary attack. Attacker first make a dictionary which have all the commonly used words which might be used as a password, then attacker apply these words to break the password. The drawback of dictionary attack is that there might be possibility that password which we crack is not available in the dictionary.



PREVENTIVE MEASURES FROM DICTIONARY ATTACK:

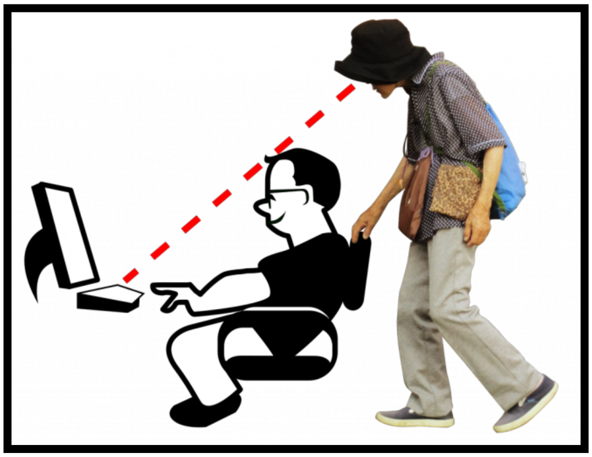
- Strong passwords
- Regularly change password
- Device lockout on failed login attempts
- Do not use common words as password
- Used biometric verification

REAL TIME EXAMPLE:

On January 4, 2009, a hacker named GMZ used a tool he made to launch a dictionary attack on the Twitter account of a person named Crystal. Overnight, the programme ran for several hours and tried out different English words on its own. He checked the results around 11 a.m. E.T. on Monday and found himself in Crystal's account. Soon, GMZ found out that Crystal worked for Twitter and had administrative rights. He was able to get into a few high-profile accounts by changing their passwords and giving them to other hackers. Some of these were from President-elect Barack Obama, Britney Spears, CBS News, and Fox News.

4. Shoulder Suffering:

Shoulder suffering is also called as spying in which the attacker notices the movement of the target person in order to get his/her password. The attacker observes the user that how he/she is entering the password, which keys are pressed. After the keen observation the attackers get to know about the length of the password and then use that password. In order to avoid shoulder suffering we should not access our personal information in front of others or especially at that time when some person is observing us.



PREVENTIVE MEASURES FROM SHOULDER SUFFERING ATTACK:

- For public computer or laptops use screen protector
- Try not to verbalize the information which is sensitive in public
- Whenever you leave your devices, lock them
- When entering data on a cellphone in a public place, sit with your back to the wall

REAL TIME EXAMPLES:

Shoulder surfing started in the early 1980s, when scammers would watch as people put their calling card numbers into public payphones. Then, they would either use the numbers to make long-distance calls themselves or sell them for less money.

It is still common practice today for scammers to peer over their victims' shoulders to steal private information.

Most common examples of shoulder surfing are:

- ➢ Shoulder surfers go to places where there are a lot of people so they can mix in and steal data without being caught. For example, let's say you're out with friends at a bar or restaurant and need to move money into your account to pay the bill. Shoulder surfers can see what you type into your mobile banking app and then use that information to steal money or empty your account.

- Few people think twice before using their phones on public transportation. But shoulder surfers can easily attack in this situation. Shoulder surfers can see what you do when you sign in to an app on your phone or enter your passcode. Later, they could steal your phone or wallet and find out private information about you.
- Shoulder surfers sometimes don't listen to what you type but to what you say. Let's say you're on the phone with your child and they ask for your account information so they can buy something online. You read them out loud for everyone to hear without giving it a second thought.
- Just think about all the information you have to give up when you get a new job, like your Social Security number, address, phone number, and banking information for benefits. Your new coworkers might stop by for a chat and see your most private information.

5. Key logger Attack:

A key logger is spyware that logs a user's keystrokes and records their behavior. Key loggers are used by cybercriminals to steal a variety of sensitive data, including passwords and credit card details. A key logger records not only the user name and password, but also the website or app where those details are used, as well as other sensitive information, in a password attack.

PREVENTIVE MEASURES FROM KEY LOGGER ATTACK:

- Use two factor authentication
- Install software updates
- Key encryption should be used
- Avoid to download crack software
- Install anti malware program

REAL TIME EXAMPLES:

- Olympic Vision, a key logger, has been used to target US, Middle Eastern, and Asian businesspeople for business email compromise (BEC) assaults. Olympic Vision infects target systems through spear-phishing and social engineering tactics in order to steal sensitive data and spy on commercial transactions. The key logger is not complex, but it can be purchased on the black market for $25, making it easily accessible to hostile actors.
- DarkHotel, which exploited hotel WIFI to target corporate and political elites, employed a variety of viruses to obtain access to the systems of certain prominent people. After gaining access, the attackers installed key loggers to steal their targets' passwords and other personal information.