Password Attacks

MNU-2025

Dr. Ahmed Samy

Lecture 07

Module Contents

In this module, we will cover the below topics:

User Authentication Methods

Types of Password Attacks

Threats of Password Attacks

How to protect your password?

User Authentication Methods

User Authentication

- **User authentication** is the process of verifying the identity of a user who is trying to access a system, application, network, or resource. It's about answering the question: "Are you who you claim to be?"

- for example, User A, has access to only relevant information and is unable to see User B's personal information.

- Authentication is a fundamental security mechanism because it:

1. **Prevents Unauthorized Access:** only legitimate users can access sensitive data.
2. **Establishes Accountability:** systems can track user actions and hold individuals accountable for their activities.
3. **Maintains Data Integrity and Confidentiality:** protect data from being viewed, modified, or deleted by unauthorized individuals.
4. **Builds Trust:** Users are more likely to trust systems that have robust authentication processes in place.

User Authentication Methods

- There are different types of user authentication methods include:

1. **Password Based Login:** The most utilized regular login authentication system that you will employ daily

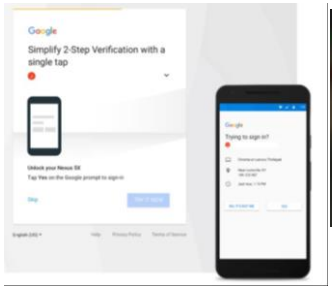
- While utilizing an online service is password-based login, You need to input a combination of your username/mobile number and a password when using the Password-Based Authentication technique.
- The individual is authorized only when both elements have been verified.

- However, because today's users use multiple online services (apps and websites), it's tough to keep track of all their usernames and passwords.
- Users may forget passwords, using the same password for several services, and so on. Cybercriminals begin actions such as phishing, data breaches, and so on.

User Authentication Methods

2. **Multi-Factor Authentication (MFA):** is an authentication method in which an individual must pass multiple factors to gain access to a service or network.

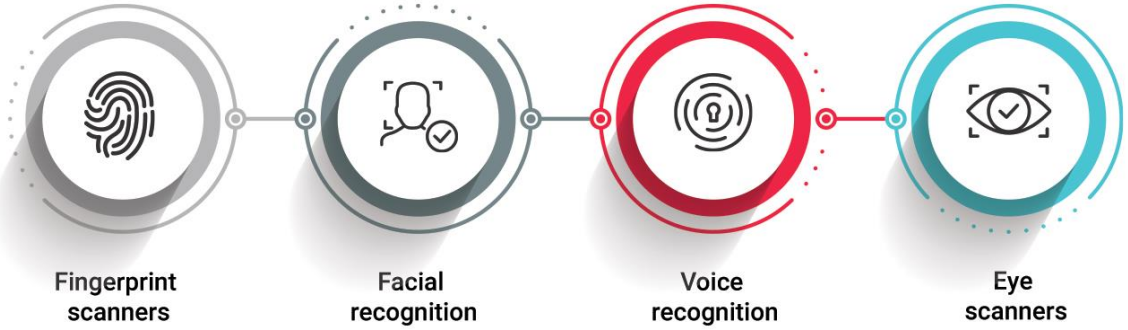
- Users must also submit a second factor in the form of a one-time code that they will receive through phone or email in addition to their Username and Password.



- You may configure several Multi-Factor Authentication (MFA) methods to give an extra layer of security to your resources. OTP/TOTP via SMS, OTP/TOTP over Email, Push notification, Hardware Token, and Mobile Authenticator are all examples of MFA methods (Google, Microsoft, etc.).

User Authentication Methods

3. Biometric Authentication: uses distinctive physiological (related to the body's physical structure) or behavioral (related to patterns in human behavior) traits to identify and verify individuals.

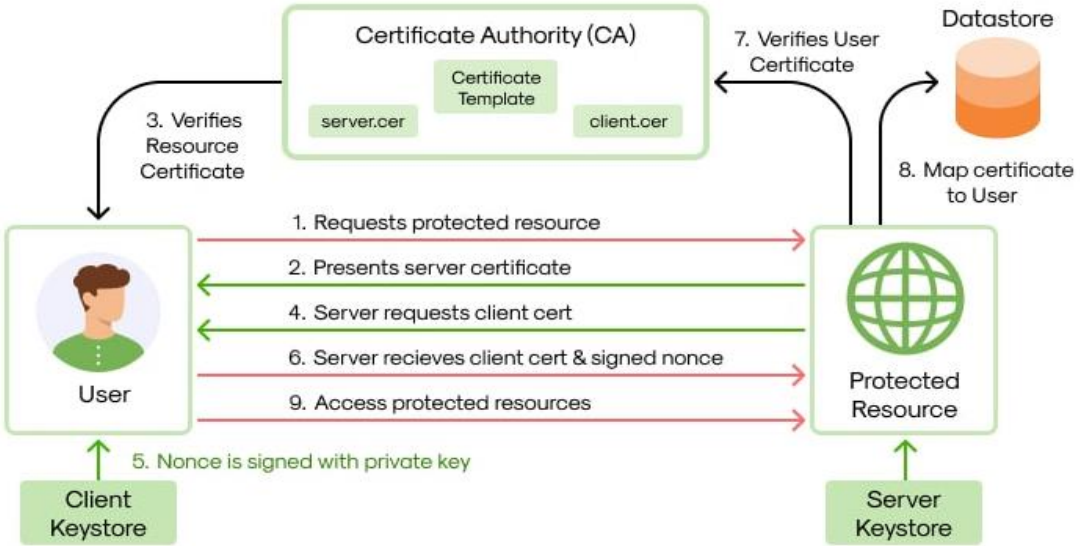


- First, the physical characteristics of individuals are saved in a database. Individuals' physical features are checked against the data contained in the database whenever a user wants to access any device or physically enter any premises (Organization, School, Colleges, Workplace).

User Authentication Methods

4. **Certificate-based authentication:** Certificate-based authentication identifies people, servers, workstations, and devices by using an electronic digital identity.

- Certificate-based authentication is a well-suited for secure communication between devices and servers without human intervention.



User Authentication Methods

5. **Token-Based Authentication:** allows users to enter their credentials only once and obtain a one-of-a-kind encrypted string exchange in return (token).

- After that, you won't have to input your credentials every time you want to log in or acquire access., The digital token ensures that you have already been granted access.

	Token (for Authentication)	OTP (One-Time Password)
Usage	Session/Authorization after login	Strong initial login/transaction verification
Lifespan	Minutes to hours/days	Seconds/Single use
Generation	Server after initial auth	Algorithm (device/server) or Server

Password Attacks

Password Attacks

- Password attack and password cracking are terms that refer to any technique or process used by a malicious actor to recover the original plaintext password from a stored password hash, or to bypass the authentication process without knowing the actual password.

- **Key Goals of a Password Attack:**

1. Recover the Plaintext Password: The attacker wants to obtain the actual password in a readable format (e.g., "P@$$wOrd123"). This allows them to directly log in to the target account or system.

2. Bypass Authentication: In some cases, attackers might not need the plaintext password. They might exploit vulnerabilities in the authentication system to gain access without ever needing to crack the hash (e.g., through session hijacking or exploiting flaws in the login process).

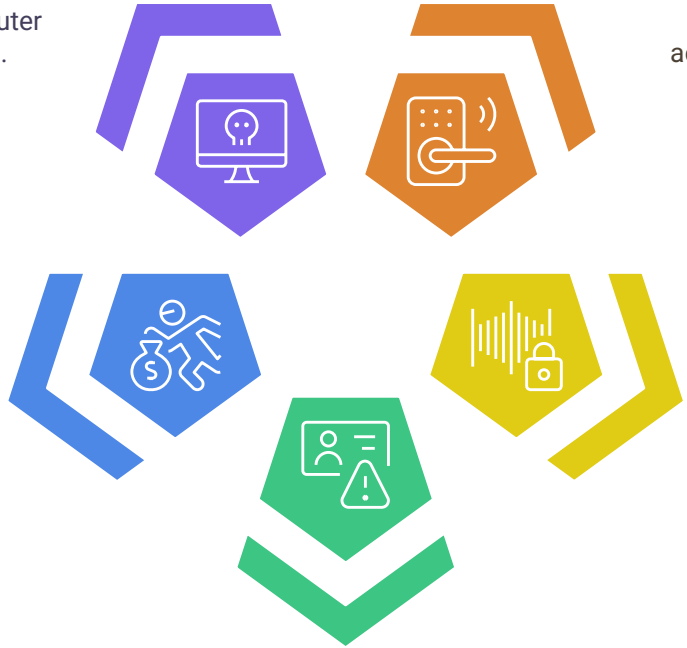
Threats of Password Attacks

System Compromise

Taking control of computer systems or networks.

Unauthorized Access

Gaining entry to personal accounts without permission.



Financial Loss

Suffering monetary damages due to unauthorized transactions.

Data Breaches

Exposure of sensitive information to unauthorized parties.

Identity Theft

Using someone's identity for malicious activities.

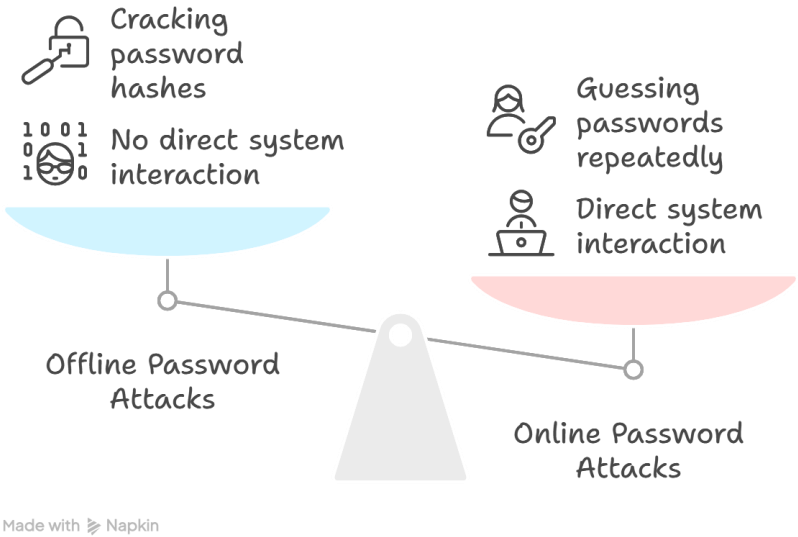
1. Brute Force Attacks

Types of Password Attacks

- Password attack methods divided into two types:

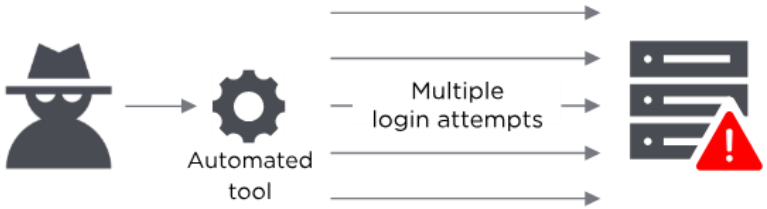
1. **Offline Password Attacks**: the attacker obtaining a password hash (a one-way encrypted representation of the password) and then attempting to crack it without directly interacting with the system.

2. **Online Password Attacks**: These attacks involve direct interaction with the authentication system. Attackers attempt to guess passwords by trying to log in repeatedly.

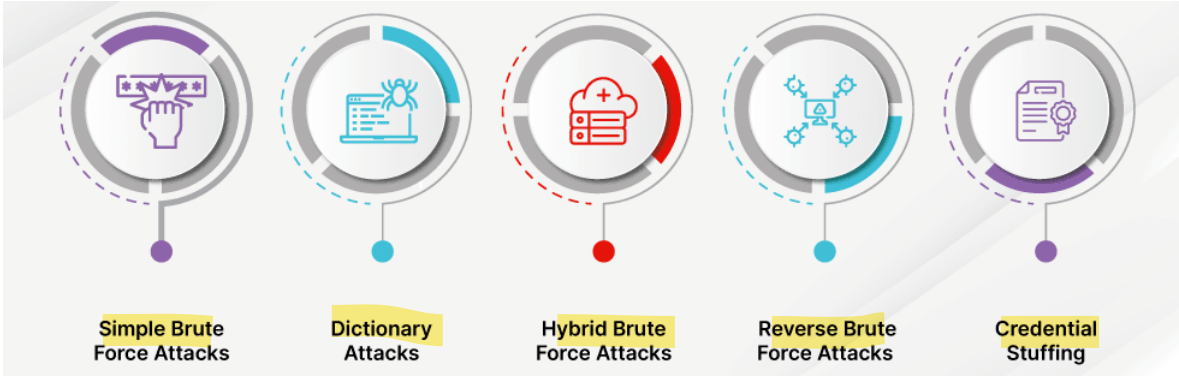


Brute Force Password Attacks

- **A brute force attack** is a hacking method that uses trial and error to crack passwords, login credentials, and encryption keys.
- The hacker tries multiple usernames and passwords, often using a computer to test a wide range of combinations, until they find the correct login information.



- **Types Of Brute Force Attacks:**



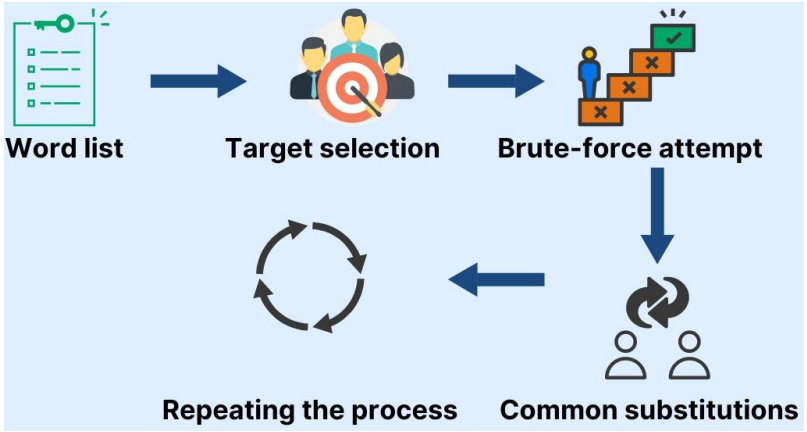
Brute Force Attacks

1. **A simple brute force attack** occurs when a hacker attempts to guess a user's login credentials manually without using any software. This is typically through standard password combinations or personal identification number (PIN) codes.

- These attacks are simple because many people still use weak passwords, such as "password123" or "1234," or practice poor password etiquette, such as using the same password for multiple websites.

2. **Dictionary attacks:** the attacker selects a target, then tests possible passwords against that individual's username.

- The name "dictionary attack" comes from hackers running through dictionaries and amending words with special characters and numbers. This type of attack is typically time-consuming and has a low chance of success compared to newer, more effective attack methods.



Brute Force Attacks

3. **Hybrid brute force attack** combines the principles of dictionary attacks and brute-force attacks. Instead of just using a static list of words, it takes words from a dictionary and then applies brute-force techniques by adding or modifying characters, numbers, and symbols to them.

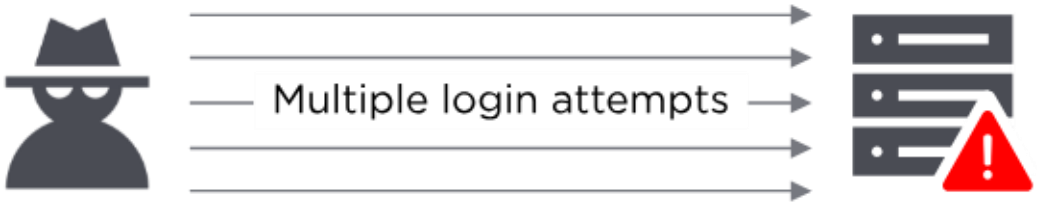
- This approach allows hackers to discover passwords that combine common or popular words with numbers, years, or random characters, such as "SanDiego123" or "Rover2020.“ It is time consuming and limited by initial dictionary.

4. **Reverse brute force attack** A reverse brute force attack sees an attacker begin the process with a known password, which is typically discovered through a network breach.

- They use that password to search for a matching login credential using lists of millions of usernames. Attackers may also use a commonly used weak password, such as "Password123," to search through a database of usernames for a match.

Brute Force Attacks

5. **Credential stuffing** if a hacker has a username-password combo that works for one website, they'll try it in tons of others as well. Since users have been known to reuse login info across many websites, they are the exclusive targets of an attack like this.



Brute Force Attack Tools

- Commonly used brute force attack tools include:

1. **Aircrack-ng:** A suite of tools that assess Wi-Fi network security to monitor and export data and attack an organization through methods like fake access points and packet injection.

2. **John the Ripper:** An open-source password recovery tool that supports hundreds of cipher and hash types, including user passwords for macOS, Unix, and Windows, database servers, web applications, network traffic, encrypted private keys, and document files.

3. **Hydra:** Specifically designed for online brute-force attacks against various network services (e.g., SSH, FTP, HTTP, Telnet, SMTP, databases). It supports a wide range of protocols and can perform dictionary and brute-force attacks against login interfaces.

4. **Wfuzz:** A web application fuzzing tool that can be used for brute-forcing by injecting payloads into various parts of HTTP requests, including login parameters.

Brute Force Attacks

- let's calculate the number of possible combinations for a 4-digit password in a brute-force attack.
- To do this, we need to consider the possible characters for each of the four positions. Assuming a standard 4-digit PIN or password uses only numerical digits (0-9), there are 10 possible characters for each position.
- The total number of combinations would be: 10×10×10×10=10^4 =10,000.
- Therefore, there are 10,000 possible combinations for a 4-digit numerical password. A brute-force attack would, in the worst case, have to try all 10,000 of these combinations to find the correct one.

Brute Force Attacks

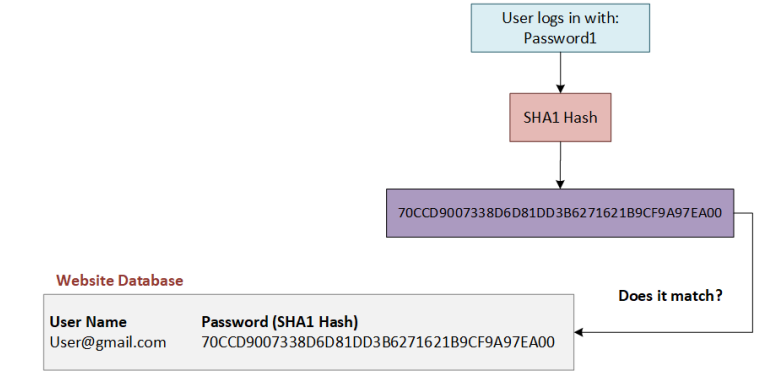
- Now, if the 4-digit password could include letters (both uppercase and lowercase) and symbols (Alphanumeric Password) as well, the number of combinations would be significantly larger.
- If we consider lowercase letters (26), uppercase letters (26), and digits (10), we have 26+26+10=62 possible characters per position.
- In this case, the total combinations would be 62^4 =14,776,336.

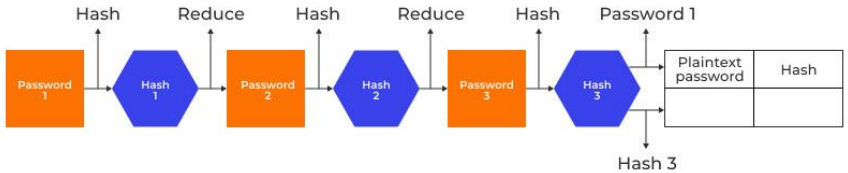
How many combinations needed for 8- and 16-digits password in case of Numerical and Alphanumerical password?

2. Rainbow Table Attacks

Rainbow Table Attacks

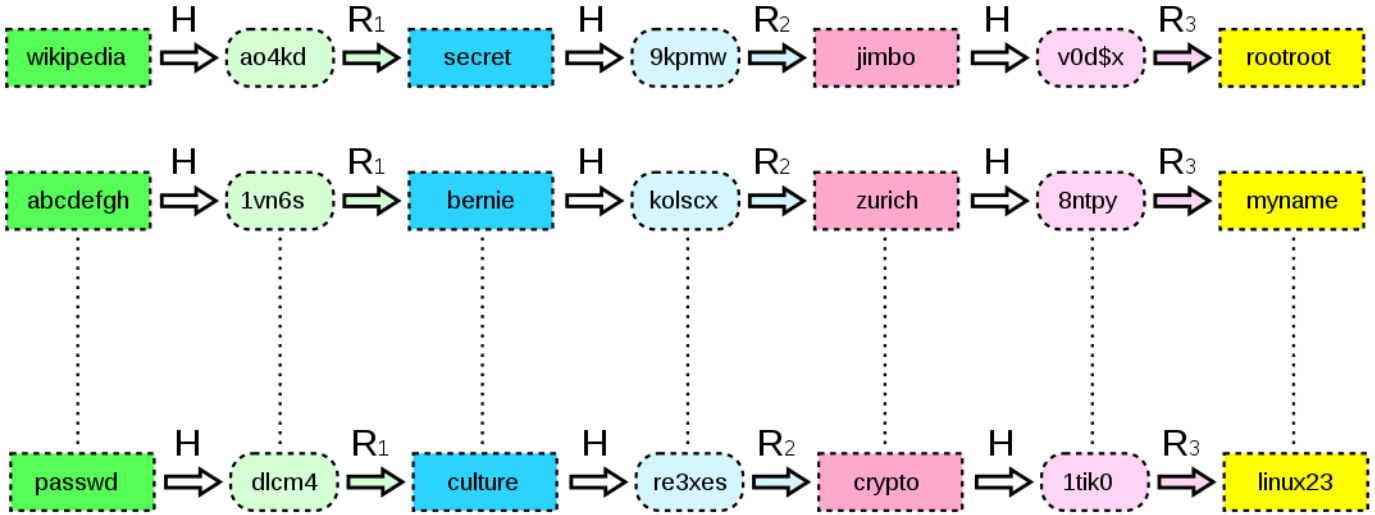
- When a user creates a password, it gets turned into a hash, which is a fixed-length string that looks nothing like the original (plaintext) password.
- Attackers use premade rainbow tables filled with plaintext passwords and their corresponding hash values to quickly find a matching plaintext password for a given hash value.
- If attackers can get their hands on a company's database of hashed passwords, they can simply look for each of the hashed values in their rainbow tables. If they find a match, they instantly know the corresponding plaintext password.
- This approach requires far less time and computational resources than brute force attacks.





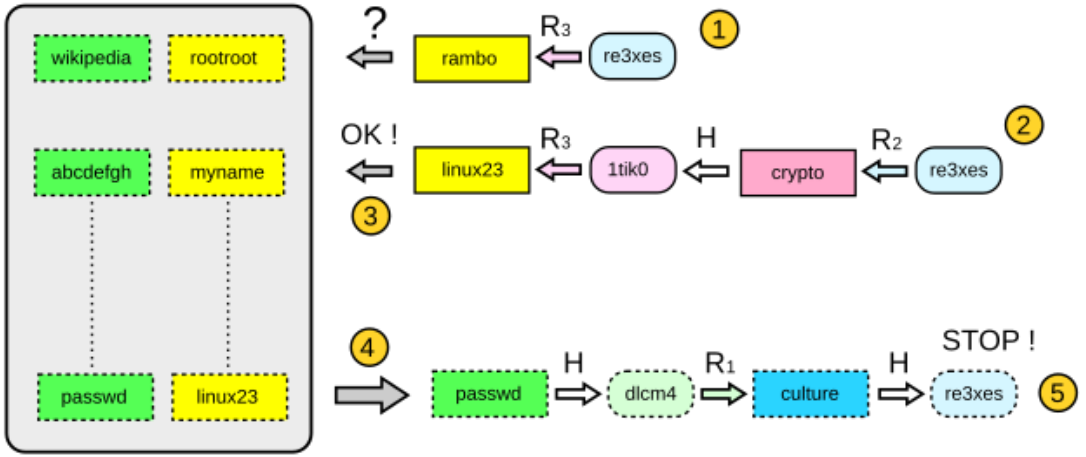
How Does Rainbow Table Attack Work?

- The Inner workings of rainbow tables rainbow tables utilize hash chains.
- a sequence of hashed passwords generated from an initial starting password. This involves hashing an initial password, then converting the resulting hash back into a new password using a reduction function. The new password is then hashed again, and the process repeats.



How Does Rainbow Table Work?

- Starting from the hash ("re3xes") in the image below, one computes the last reduction used in the table and checks whether the password appears in the last column of the table (step 1).
- If the test fails, one computes a chain with the two last reductions (step 2).
- Note: If this new test fails again, one continues with 3 reductions, 4 reductions, etc. until the password is found. If no chain contains the password, then the attack has failed.
- If this test is positive (step 3, linux23 appears at the end of the chain and in the table), the password is retrieved at the beginning of the chain that produces linux23. Here we find passwd at the beginning of the corresponding chain stored in the table.
- At this point (step 4), one generates a chain and compares at each iteration the hash with the target hash. We find the hash re3xes in the chain, and the password that produced it (culture) one step earlier in the chain: the attack is successful.



Rainbow Table Pros and Cons.

Rainbow Table Pros:

- Speed of Cracking (Compared to Brute-Force).
- Reduced Storage (Compared to All Hashes).
- Effectiveness Against Common Hashing Algorithms (Without Salt).
- Offline Attack Efficiency.

Rainbow Table Cons:

- Ineffectiveness Against Salt
- High Generation Time and Resource Cost.
- Limited to the Password Space Covered.
- Storage Requirements Can Still Be Significant.

3. Keylogging Attack

Keylogging Attack

- **A keylogger** or keystroke logger/keyboard capturing is a form of malware or hardware that keeps track of and records your keystrokes as you type.
- It takes the information and sends it to a hacker using a command-and-control (C&C) server.
- The hacker then analyzes the keystrokes to locate usernames and passwords and uses them to hack into otherwise secure systems.
- There are two types of Keylogger:

1. Software keylogger
2. Hardware keylogger

Software Keyloggers

- Software keyloggers consist of malware/ applications that have to be installed on a computer to steal keystroke data. They are the most common method hackers use to access a user's keystrokes.
- A software keylogger is put on a computer when the user downloads an infected application. Once installed, the keylogger monitors the keystrokes on the operating system you are using, checking the paths each keystroke goes through.
- After the keystrokes have been recorded, they are then automatically transferred to the hacker that set up the keylogger.
- The stolen passwords may include email accounts, bank accounts, or those that the target uses to access websites where their personal information can be seen.

Hardware Keyloggers

- A hardware keylogger is physically connected to the target computer to record the user's keystrokes. For this reason, it is important for an organization to carefully monitor who has access to the network and the devices connected to it.
- After hardware keystroke loggers have finished keylogging, they store the data, which the hacker must download from the device.
- The downloading should be performed only after the keylogger has finished logging keystrokes. This is because it is not possible for the hacker to get the data while the key logger is working.
- In some cases, the hacker may make the keylogging device accessible via Wi-Fi. This way, they do not have to physically walk up to the hacked computer to get the device and retrieve the data.

4. Phishing Attack

Phishing Attack

- **Phishing** remains one of the primary delivery mechanisms for many types of cyberattacks including password attacks. These include:
- **Email phishing:** Attackers send deceptive emails impersonating legitimate organizations to convince users to click on an embedded link to a fake login page to capture entered passwords or attachments that contain malware to steal stored passwords.
- **SMS phishing (Smishing):** These are fraudulent text messages sent to mobile devices that claim to come from financial institutions or other trusted entities. The message usually includes a shortened URL leading to a phishing website.
- **Voice-based phishing (Vishing):** Attackers use phone calls to manipulate victims into divulging passwords by impersonating IT support, bank representatives, or government officials.

Password Attacks Mitigation

Password attacks Mitigation Methods

1. **Enforce Strong Password Policies:**
   - Minimum Length: 12 characters or more.
   - Complexity Requirements: mix of uppercase and lowercase letters, numbers, and symbols.
   - Regular Password Changes: frequently force password change.

2. **Implementing Multi-Factor Authentication:**
   - Require users to provide at least two different authentication factors (e.g., password + OTP, password + biometric) to gain access.

3. **Implement Strong Hashing Algorithms with Salt:**
   - Use modern, computationally expensive hashing algorithms

4. **Account Lockout Policies:**
   - Temporarily disable an account after a certain number of failed login attempts.

5. **Rate Limiting:**
   - Limit the number of login attempts allowed from a specific IP address or user within a given time frame.

Password attacks Mitigation Methods

6. **Protecting Password Data bases:**

   - Secure Storage
   - Regular Security Patching
   - Principle of Least Privilege
   - Database Activity Monitoring

7. **User Awareness and Training:**

   - reinforce password security best practices through regular reminders and updates and conduct phishing awareness training.

Thanks!

Do you have any questions?