Fortify against brute force cyber attacks

Usernames and passwords are one of the most common and important security controls in use today. They're like the door lock that organizations use to restrict access to their networks, services, and data. But a major issue with relying on login credentials as a critical line of defense is that they're vulnerable to being stolen and guessed by attackers.

In a video, you learned that **brute force attacks** are a trial-and-error process of discovering private information. In this reading, you'll learn about the many tactics and tools used by threat actors to perform brute force attacks. You'll also learn prevention strategies that organizations can use to defend against them.

A matter of trial and error

One way of opening a closed lock is trying as many combinations as possible. Threat actors sometimes use similar tactics to gain access to an application or a network.

Attackers use a variety of tactics to find their way into a system:

- *Simple brute force attacks* are an approach in which attackers guess a user's login credentials. They might do this by entering any combination of username and password that they can think of until they find the one that works.
- *Dictionary attacks* are a similar technique except in these instances attackers use a list of commonly used credentials to access a system. This list is similar to matching a definition to a word in a dictionary.
- *Reverse brute force attacks* are similar to dictionary attacks, except they start with a single credential and try it in various systems until a match is found.
- *Credential stuffing* is a tactic in which attackers use stolen login credentials from previous data breaches to access user accounts at another organization. A specialized type of credential stuffing is called *pass the hash*. These attacks reuse stolen, unsalted hashed credentials to trick an authentication system into creating a new authenticated user session on the network.

Note: Besides access credentials, encrypted information can sometimes be brute forced using a technique known as *exhaustive key search*.

Each of these methods involve a lot of guess work. Brute forcing your way into a system can be a tedious and time consuming process—especially when it's done manually. That's why threat actors often use tools to conduct their attacks.

Tools of the trade

There are so many combinations that can be used to create a single set of login credentials. The number of characters, letters, and numbers that can be mixed together is truly incredible. When done manually, it could take someone years to try every possible combination.

Instead of dedicating the time to do this, attackers often use software to do the guess work for them. These are some common brute forcing tools:

- Aircrack-ng
- Hashcat
- John the Ripper
- Ophcrack
- THC Hydra

Sometimes, security professionals use these tools to test and analyze their own systems. They each serve different purposes. For example, you might use Aircrack-ng to test a Wi-Fi network for vulnerabilities to brute force attack.

Prevention measures

Organizations defend against brute force attacks with a combination of technical and managerial controls. Each make cracking defense systems through brute force less likely:

- Hashing and salting
- Multi-factor authentication (MFA)
- CAPTCHA
- Password policies

Technologies, like multi-factor authentication (MFA), reinforce each login attempt by requiring a second or third form of identification. Other important tools are CAPTCHA and effective password policies.

Hashing and salting

Hashing converts information into a unique value that can then be used to determine its integrity. **Salting** is an additional safeguard that's used to strengthen hash functions. It works by adding random characters to data, like passwords. This increases the length and complexity of hash values, making them harder to brute force and less susceptible to dictionary attacks.

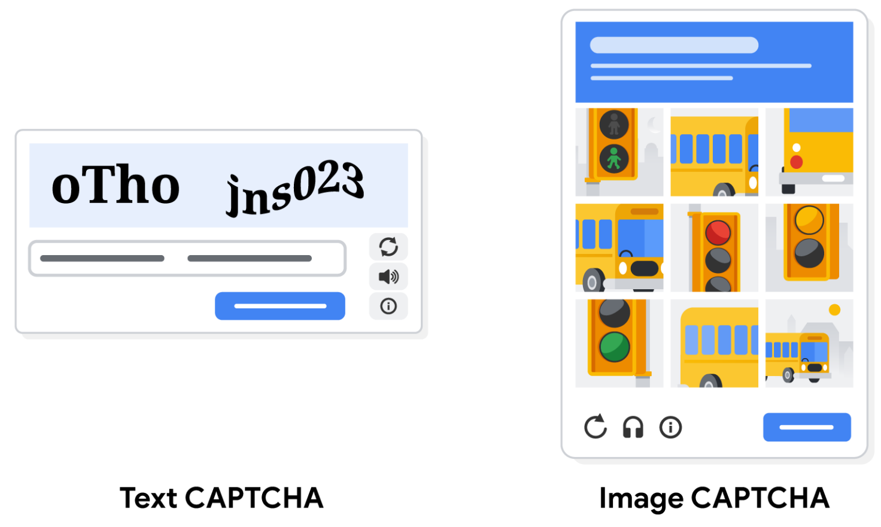
Multi-factor authentication (MFA)

Multi-factor authentication (MFA) is a security measure that requires a user to verify their identity in two or more ways to access a system or network. MFA is a layered approach to protecting information. MFA limits the chances of brute force attacks because unauthorized users are unlikely to meet each authentication requirement even if one credential becomes compromised.

CAPTCHA

CAPTCHA stands for Completely Automated Public Turing test to tell Computers and Humans Apart. It is known as a challenge-response authentication system. CAPTCHA asks users to complete a simple test that proves they are human and not software that's trying to brute force a password.

Here are common CAPTCHA examples:



There are two types of CAPTCHA tests. One scrambles and distorts a randomly generated sequence of letters and/or numbers and asks users to enter them into a text box. The other test asks users to match images to a randomly generated word. You've likely had to pass a CAPTCHA test when accessing a web service that contains sensitive information, like an online bank account.

Password policy

Organizations use these managerial controls to standardize good password practices across their business. For example, one of these policies might require users to create passwords that are at least 8 characters long and feature a letter, number, and symbol. Other common requirements can include password lockout policies. For example, a password lockout can limit the number of login attempts before access to an account is suspended and require users to create new, unique passwords after a certain amount of time.

The purpose of each of these requirements is to create more possible password combinations. This lengthens the amount of time it takes an attacker to find one that will work. The National Institute of Standards and Technology (NIST) Special Publication 800-63B provides detailed guidance that organizations can reference when creating their own password policies.

Key takeaways

Brute force attacks are simple yet reliable ways to gain unauthorized access to systems. Generally, the stronger a password is, the more resilient it is to being cracked. As a security professional, you might find yourself using the tools described above to test the security of your organization's systems. Recognizing the tactics and tools used to conduct a brute force attack is the first step towards stopping attackers.

Mark as completed

Like **Dislike** **Report an issue**