Introduction

Keys and passwords, the modern equivalent of locks and combinations, secure the digital world. But what if someone tries every possible combination until they find the one that opens the door? That, in essence, is brute forcing.

What is Brute Forcing?

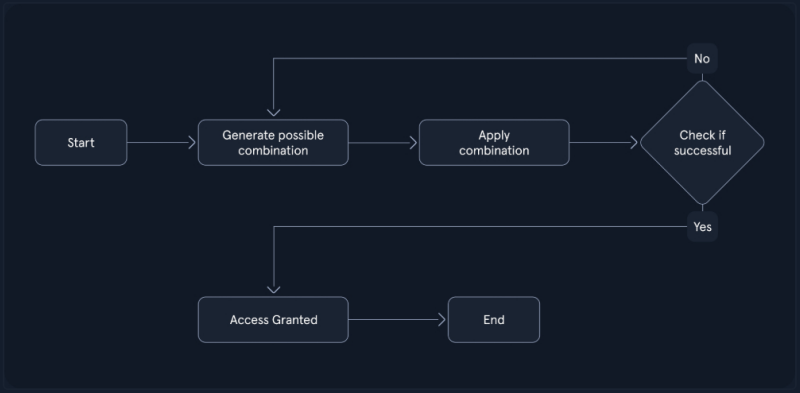
In cybersecurity, brute forcing is a trial-and-error method used to crack passwords, login credentials, or encryption keys. It involves systematically trying every possible combination of characters until the correct one is found. The process can be likened to a thief trying every key on a giant keyring until they find the one that unlocks the treasure chest.

The success of a brute force attack depends on several factors, including:

- The complexity of the password or key. Longer passwords with a mix of uppercase and lowercase letters, numbers, and symbols are exponentially more complex to crack.
- The computational power available to the attacker. Modern computers and specialized hardware can try billions of combinations per second, significantly reducing the time needed for a successful attack.
- The security measures in place. Account lockouts, CAPTCHAs, and other defenses can slow down or even thwart brute-force attempts.

How Brute Forcing Works

The brute force process can be visualized as follows:



1. Start: The attacker initiates the brute force process, often with the aid of specialized software.
2. Generate Possible Combination: The software generates a potential password or key combination based on predefined parameters, such as character sets and length.
3. Apply Combination: The generated combination is attempted against the target system, such as a login form or encrypted file.
4. Check if Successful: The system evaluates the attempted combination. If it matches the stored password or key, access is granted. Otherwise, the process continues.
5. Access Granted: The attacker gains unauthorized access to the system or data.
6. End: The process repeats, generating and testing new combinations until either the correct one is found or the attacker gives up.

Types of Brute Forcing

Brute forcing is not a monolithic entity but a collection of diverse techniques, each with its strengths, weaknesses, and ideal use cases. Understanding these variations is crucial for both attackers and defenders, as it enables the former to choose the most effective approach and the latter to implement targeted countermeasures. The following table provides a comparative overview of various brute-forcing methods:

Method	Description	Example	Best Used When...
Simple Brute	Systematically tries all possible	Trying all combinations of	No prior information about the

Cheat Sheet

Table of Contents

Introduction
Introduction
Password Security Fundamentals

Brute Force Attacks
Brute Force Attacks
Dictionary Attacks
Hybrid Attacks

Hydra
Hydra
Basic HTTP Authentication
Login Forms

Medusa
Medusa
Web Services

Custom Wordlists
Custom Wordlists

Skills Assessment
Skills Assessment Part 1
Skills Assessment Part 2

My Workstation

OFFLINE

Start Instance

∞ / 1 spawns left

Force	combinations of characters within a defined character set and length range.	lowercase letters from 'a' to 'z' for passwords of length 4 to 6.	password is available, and computational resources are abundant.
Dictionary Attack	Uses a pre-compiled list of common words, phrases, and passwords.	Trying passwords from a list like 'rockyou.txt' against a login form.	The target will likely use a weak or easily guessable password based on common patterns.
Hybrid Attack	Combines elements of simple brute force and dictionary attacks, often appending or prepending characters to dictionary words.	Adding numbers or special characters to the end of words from a dictionary list.	The target might use a slightly modified version of a common password.
Credential Stuffing	Leverages leaked credentials from one service to attempt access to other services, assuming users reuse passwords.	Using a list of usernames and passwords leaked from a data breach to try logging into various online accounts.	A large set of leaked credentials is available, and the target is suspected of reusing passwords across multiple services.
Password Spraying	Attempts a small set of commonly used passwords against a large number of usernames.	Trying passwords like 'password123' or 'qwerty' against all usernames in an organization.	Account lockout policies are in place, and the attacker aims to avoid detection by spreading attempts across multiple accounts.
Rainbow Table Attack	Uses pre-computed tables of password hashes to reverse hashes and recover plaintext passwords quickly.	Pre-computing hashes for all possible passwords of a certain length and character set, then comparing captured hashes against the table to find matches.	A large number of password hashes need to be cracked, and storage space for the rainbow tables is available.
Reverse Brute Force	Targets a single password against multiple usernames, often used in conjunction with credential stuffing attacks.	Using a leaked password from one service to try logging into multiple accounts with different usernames.	A strong suspicion exists that a particular password is being reused across multiple accounts.
Distributed Brute Force	Distributes the brute forcing workload across multiple computers or devices to accelerate the process.	Using a cluster of computers to perform a brute-force attack significantly increases the number of combinations that can be tried per second.	The target password or key is highly complex, and a single machine lacks the computational power to crack it within a reasonable timeframe.

The Role of Brute Forcing in Penetration Testing

Penetration testing, or ethical hacking, is a proactive cybersecurity measure that simulates real-world attacks to identify and address vulnerabilities before malicious actors can exploit them. Brute forcing is a crucial tool in this process, particularly when assessing the resilience of password-based authentication mechanisms.

While penetration tests encompass a range of techniques, brute forcing is often strategically employed when:

- **Other avenues are exhausted**: Initial attempts to gain access, such as exploiting known vulnerabilities or utilizing social engineering tactics, may prove unsuccessful. In such scenarios, brute forcing is a viable alternative to overcome password barriers.
- **Password policies are weak**: If the target system employs lax password policies, it increases the likelihood of users having weak or easily guessable passwords. Brute forcing can effectively expose these vulnerabilities.
- **Specific accounts are targeted**: In some instances, penetration testers may focus on compromising specific user accounts, such as those with elevated privileges. Brute forcing can be tailored to target these accounts directly.