Brute Force Attack

What is a Brute Force Attack

A brute force attack is a popular cracking method: by some accounts, brute force attacks accounted for five percent of confirmed security breaches. A brute force attack involves ‘guessing’ username and passwords to gain unauthorized access to a system. Brute force is a simple attack method and has a high success rate.

Some attackers use applications and scripts as brute force tools. These tools try out numerous password combinations to bypass authentication processes. In other cases, attackers try to access web applications by searching for the right session ID. Attacker motivation may include stealing information, infecting sites with malware, or disrupting service.

While some attackers still perform brute force attacks manually, today almost all brute force attacks today are performed by bots. Attackers have lists of commonly used credentials, or real user credentials, obtained via security breaches or the dark web. Bots systematically attack websites and try these lists of credentials, and notify the attacker when they gain access.

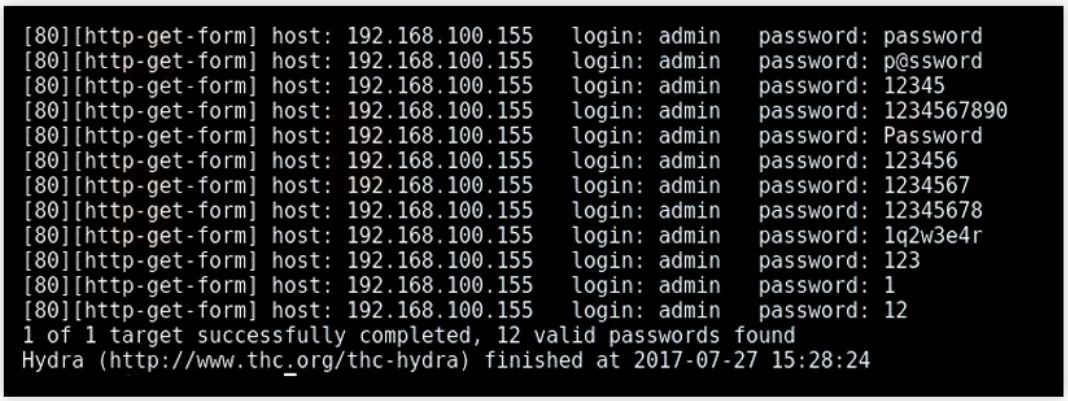
Types of Brute Force Attacks

- **Simple brute force attack**—uses a systematic approach to ‘guess’ that doesn’t rely on outside logic.
- **Hybrid brute force attacks**—starts from external logic to determine which password variation may be most likely to succeed, and then continues with the simple approach to try many possible variations.

- **Dictionary attacks**—guesses usernames or passwords using a dictionary of possible strings or phrases.
- **Rainbow table attacks**—a rainbow table is a precomputed table for reversing cryptographic hash functions. It can be used to guess a function up to a certain length consisting of a limited set of characters.
- **Reverse brute force attack**—uses a common password or collection of passwords against many possible usernames. Targets a network of users for which the attackers have previously obtained data.
- **Credential stuffing**—uses previously-known password-username pairs, trying them against multiple websites. Exploits the fact that many users have the same username and password across different systems.

Hydra and Other Popular Brute Force Attack Tools

Security analysts use the THC-Hydra tool to identify vulnerabilities in client systems. Hydra quickly runs through a large number of password combinations, either simple brute force or dictionary-based. It can attack more than 50 protocols and multiple operating systems. Hydra is an open platform; the security community and attackers constantly develop new modules.



Hydra brute force attack

Other top brute force tools are:

- **Aircrack-ng**—can be used on Windows, Linux, iOS, and Android. It uses a dictionary of widely used passwords to breach wireless networks.
- **John the Ripper**—runs on 15 different platforms including Unix, Windows, and OpenVMS. Tries all possible combinations using a dictionary of possible passwords.
- **L0phtCrack**—a tool for cracking Windows passwords. It uses rainbow tables, dictionaries, and multiprocessor algorithms.
- **Hashcat**—works on Windows, Linux, and Mac OS. Can perform simple brute force, rule-based, and hybrid attacks.
- **DaveGrohl**—an open-source tool for cracking Mac OS. Can be distributed across multiple computers.
- **Ncrack**—a tool for cracking network authentication. It can be used on Windows, Linux, and BSD.

Weak Passwords that Enable Brute Force Attacks

Today, individuals possess many accounts and have many passwords. People tend to repeatedly use a few simple passwords, which leaves them exposed to brute force attacks. Also, repeated use of the same password can grant attackers access to many accounts.

Email accounts protected by weak passwords may be connected to additional accounts, and can also be used to restore passwords. This makes them

particularly valuable to hackers. Also, if users don't modify their default router password, their local network is vulnerable to attacks. Attackers can try a few simple default passwords and gain access to an entire network.

Some of the most commonly found passwords in brute force lists include: date of birth, children's names, qwerty, 123456, abcdef123, a123456, abc123, password, asdf, hello, welcome, zxcvbn, Qazwsx, 654321, 123321, 000000, 111111, 987654321, 1q2w3e, 123qwe, qwertyuiop, gfhjkm.

Strong passwords provide better protection against identity theft, loss of data, unauthorized access to accounts etc.

How to Prevent Brute Force Password Hacking

To protect your organization from brute force password hacking, enforce the use of strong passwords. Passwords should:

- Never use information that can be found online (like names of family members).
- Have as many characters as possible.
- Strong passwords, Combine letters, numbers, and symbols.
- Be different for each user account.
- Avoid common patterns.

- As an administrator, there are methods you can implement to protect users from brute force password cracking:

  •**Lockout policy**—you can lock accounts after several failed login attempts and then unlock it as the administrator.

  •**Progressive delays**—you can lock out accounts for a limited amount of time after failed login attempts. Each attempt makes the delay longer.

  •**Captcha**—tools like reCAPTCHA require users to complete simple tasks to log into a system. Users can easily complete these tasks while brute force tools cannot.

  •**Requiring strong passwords**—you can force users to define long and complex passwords. You should also enforce periodical password changes.

  •**Two-factor authentication**—you can use multiple factors to authenticate identity and grant access to accounts. I.e sms, finger print