Password Security Fundamentals

The effectiveness of brute-force attacks hinges on the strength of the passwords it targets. Understanding the fundamentals of password security is crucial for appreciating the importance of robust password practices and the challenges posed by brute-force attacks.

The Importance of Strong Passwords

Passwords are the first line of defense in protecting sensitive information and systems. A strong password is a formidable barrier, making it significantly harder for attackers to gain unauthorized access through brute forcing or other techniques. The longer and more complex a password is, the more combinations an attacker has to try, exponentially increasing the time and resources required for a successful attack.

The Anatomy of a Strong Password

The `National Institute of Standards and Technology` (`NIST`) provides guidelines for creating strong passwords. These guidelines emphasize the following characteristics:

- `Length`: The longer the password, the better. Aim for a minimum of 12 characters, but longer is always preferable. The reasoning is simple: each additional character in a password dramatically increases the number of possible combinations. For instance, a 6-character password using only lowercase letters has 26^6 (approximately 300 million) possible combinations. In contrast, an 8-character password has 26^8 (approximately 200 billion) combinations. This exponential increase in possibilities makes longer passwords significantly more resistant to brute-force attacks.
- `Complexity`: Use uppercase and lowercase letters, numbers, and symbols. Avoid quickly guessable patterns or sequences. Including different character types expands the pool of potential characters for each position in the password. For example, a password using only lowercase letters has 26 possibilities per character, while a password using both uppercase and lowercase letters has 52 possibilities per character. This increased complexity makes it much harder for attackers to predict or guess passwords.
- `Uniqueness`: Don't reuse passwords across different accounts. Each account should have its own unique and strong password. If one account is compromised, all other accounts using the same password are also at risk. By using unique passwords for each account, you compartmentalize the potential damage of a breach.
- `Randomness`: Avoid using dictionary words, personal information, or common phrases. The more random the password, the harder it is to crack. Attackers often use wordlists containing common passwords and personal information to speed up their brute-force attempts. Creating a random password minimizes the chances of being included in such wordlists.

Common Password Weaknesses

Despite the importance of strong passwords, many users still rely on weak and easily guessable passwords. Common weaknesses include:

- `Short Passwords`: Passwords with fewer than eight characters are particularly vulnerable to brute-force attacks, as the number of possible combinations is relatively small.
- `Common Words and Phrases`: Using dictionary words, names, or common phrases as passwords makes them susceptible to dictionary attacks, where attackers try a pre-defined list of common passwords.
- `Personal Information`: Incorporating personal information like birthdates, pet names, or addresses into passwords makes them easier to guess, especially if this information is publicly available on social media or other online platforms.
- `Reusing Passwords`: Using the same password across multiple accounts is risky. If one account is compromised, all other accounts using the same password are also at risk.
- `Predictable Patterns`: Using patterns like "qwerty" or "123456" or simple substitutions like "p@ssw0rd" makes passwords easy to guess, as these patterns are well-known to attackers.

Password Policies

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

Organizations often implement password policies to enforce the use of strong passwords. These policies typically include requirements for:

- `Minimum Length`: The minimum number of characters a password must have.
- `Complexity`: The types of characters that must be included in a password (e.g., uppercase, lowercase, numbers, symbols).
- `Password Expiration`: The frequency with which passwords must be changed.
- `Password History`: The number of previous passwords that cannot be reused.

While password policies can help improve password security, they can also lead to user frustration and the adoption of poor password practices, such as writing passwords down or using slight variations of the same password. When designing password policies, it's important to balance security and usability.

The Perils of Default Credentials

One critical aspect of password security often overlooked is the danger posed by `default passwords`. These pre-set passwords come with various devices, software, or online services. They are often simple and easily guessable, making them a prime target for attackers.

Default passwords significantly increase the success rate of brute-force attacks. Attackers can leverage lists of common default passwords, dramatically reducing the search space and accelerating the cracking process. In some cases, attackers may not even need to perform a brute-force attack; they can try a few common default passwords and gain access with minimal effort.

The prevalence of default passwords makes them a low-hanging fruit for attackers. They provide an easy entry point into systems and networks, potentially leading to data breaches, unauthorized access, and other malicious activities.

Device/Manufacturer	Default Username	Default Password	Device Type
Linksys Router	admin	admin	Wireless Router
D-Link Router	admin	admin	Wireless Router
Netgear Router	admin	password	Wireless Router
TP-Link Router	admin	admin	Wireless Router
Cisco Router	cisco	cisco	Network Router
Asus Router	admin	admin	Wireless Router
Belkin Router	admin	password	Wireless Router
Zyxel Router	admin	1234	Wireless Router
Samsung SmartCam	admin	4321	IP Camera
Hikvision DVR	admin	12345	Digital Video Recorder (DVR)
Axis IP Camera	root	pass	IP Camera
Ubiquiti UniFi AP	ubnt	ubnt	Wireless Access Point
Canon Printer	admin	admin	Network Printer
Honeywell Thermostat	admin	1234	Smart Thermostat
Panasonic DVR	admin	12345	Digital Video Recorder (DVR)

These are just a few examples of well-known default passwords. Attackers often compile extensive lists of such passwords and use them in automated attacks.

Alongside default passwords, default usernames are another major security concern. Manufacturers often ship devices with pre-set usernames, such as `admin`, `root`, or `user`. You might have noticed in the table above how many use common usernames. These usernames are widely known and often published in documentation or readily available online. SecLists maintains a list of common usernames at top-usernames-shortlist.txt

Default usernames are a significant vulnerability because they give attackers a predictable starting point. In many brute-force attacks, knowing the username is half the battle. With the username already established, the attacker only needs to crack the password, and if the device still uses a default password, the attack can be completed with minimal effort.

Even when default passwords are changed, retaining the default username still leaves systems vulnerable to attacks. It drastically narrows the attack surface, as the hacker can skip the process of guessing usernames and focus solely on the password.

Brute-forcing and Password Security

In a brute-force scenario, the strength of the target passwords becomes the attacker's primary obstacle. A weak password is akin to a flimsy lock on a door – easily picked open with minimal effort. Conversely, a strong password acts as a fortified vault, demanding significantly more time and resources to breach.

For a pentester, this translates to a deeper understanding of the target's security posture:

- **Evaluating System Vulnerability:** Password policies, or their absence, and the likelihood of users employing weak passwords directly inform the potential success of a brute-force attack.
- **Strategic Tool Selection:** The complexity of the passwords dictates the tools and methodologies a pentester will deploy. A simple dictionary attack might suffice for weak passwords, while a more sophisticated, hybrid approach may be required to crack stronger ones.
- **Resource Allocation:** The estimated time and computational power needed for a brute-force attack is intrinsically linked to the complexity of the passwords. This knowledge is essential for effective planning and resource management.
- **Exploiting Weak Points:** Default passwords are often a system's Achilles' heel. A pentester's ability to identify and leverage these easily guessable credentials can provide a swift entry point into the target network.

In essence, a deep understanding of password security is a roadmap for a pentester navigating the complexities of a brute-force attack. It unveils potential weak points, informs strategic choices, and predicts the effort required for a successful breach. This knowledge, however, is a double-edged sword. It also underscores the critical importance of robust password practices for any organization seeking to defend against such attacks, highlighting each user's pivotal role in safeguarding sensitive information.

Previous Next

Mark Complete & Next