Password Analysis Report

9/12/2025, 7:44:26 PM

Summary

A password-policy audit was performed. Exhaustive search attacks were launched against the collected hashes to provide accurate statistics.
The results highlight several inadequacies regarding current best practices.

Following this audit, the risk associated with the existing password policy is assessed as **High**.

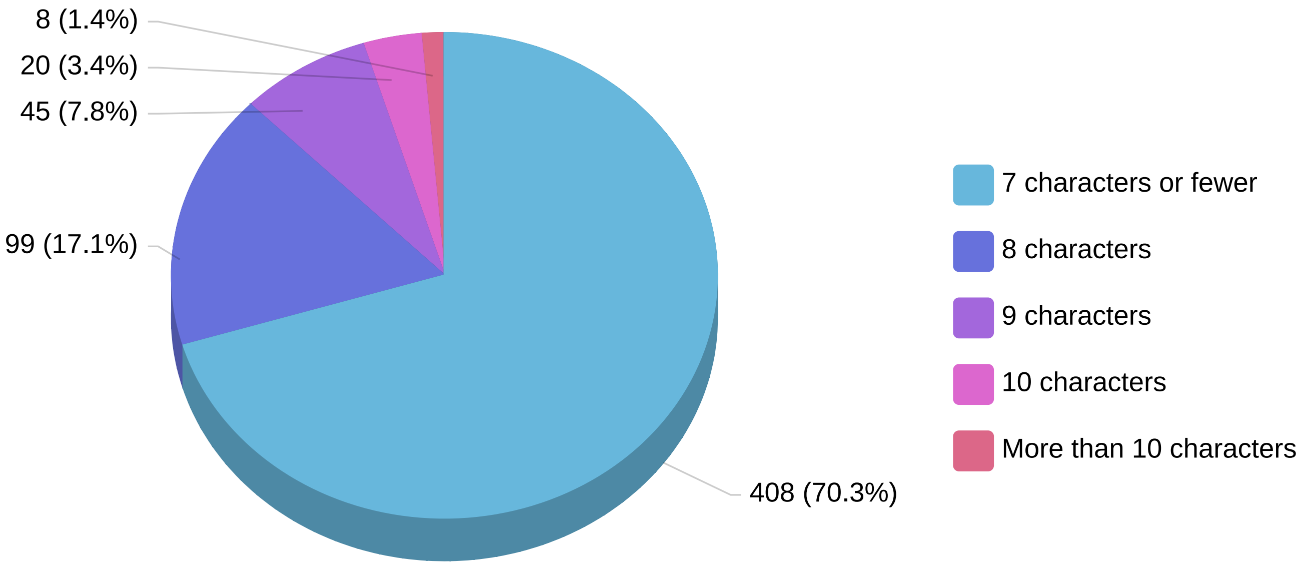
- In total, **580** of **1000** user hashes **58%** were cracked during the engagement.
- Use of the **LAN MANAGER** algorithm was detected on **230** hashes, which is obsolete and vulnerable.
- We also found that password reuse affects **30.2%** of accounts.
- Moreover, **84.3%** of cracked passwords do not meet the required complexity level and **98.6%** the recommended length.
- Finally, **5** accounts use a password identical to the username, which represents an immediate compromise risk.

Implementing the remediation measures described in this report is strongly recommended to enforce a robust, state-of-the-art password policy at every level.

Password Lengths

The chart below shows the distribution of user passwords by length. Analysis indicates that **572** cracked passwords, i.e. **98.6%**, are **10 characters or fewer**.
Short passwords are far more vulnerable to brute-force and guessing attacks because attackers can test all combinations quickly.

Major security standards recommend passwords of at least 12 characters, combining uppercase and lowercase letters, digits and special symbols whenever possible.



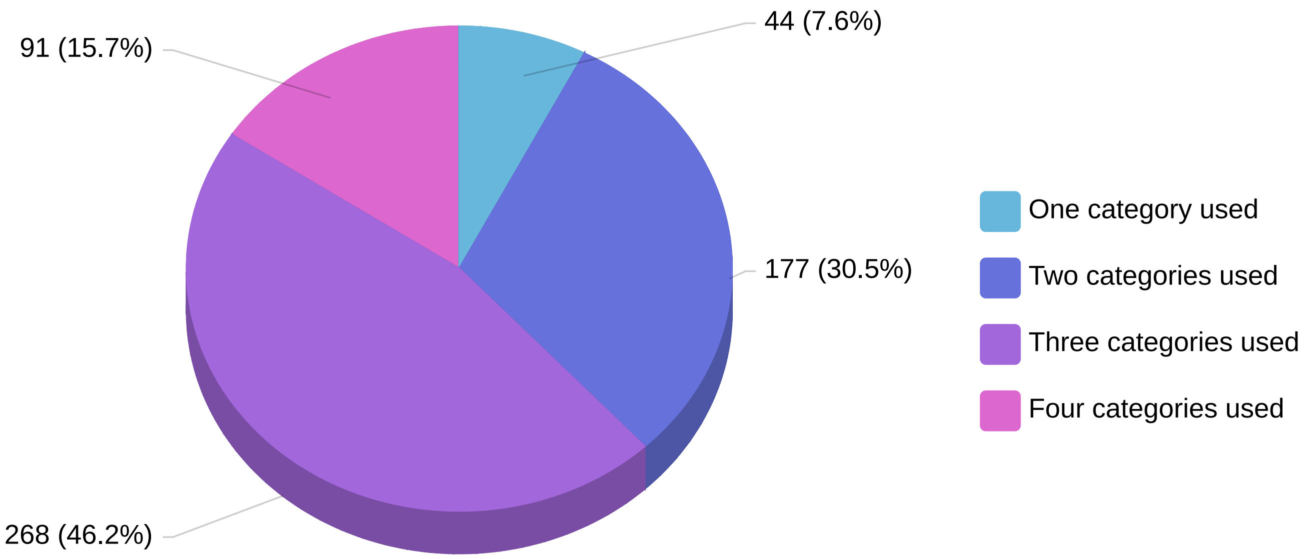
Password Complexity

Password complexity can be assessed by counting the character categories used:

- Lower-case letters;
- Upper-case letters;
- Digits;
- Special characters.

The chart below shows password complexity. Analysis reveals that **489** passwords, i.e. **84.3%**, use only **three or fewer categories**.

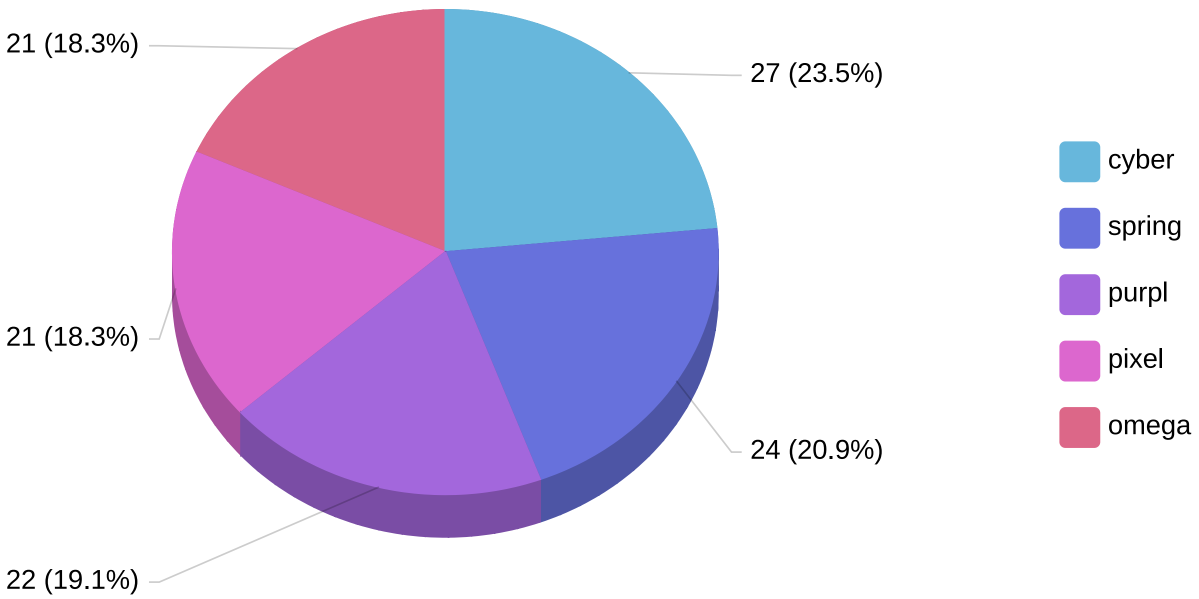
Passwords combining all four categories are much more resistant to exhaustive-search attacks. Security guidance recommends using all four to reduce compromise risk.



Most Common Keywords

The chart below lists the most frequent keywords in the dataset. The words **cyber** and **spring** appear in **4.7%** and **4.1%** of cracked passwords, respectively.

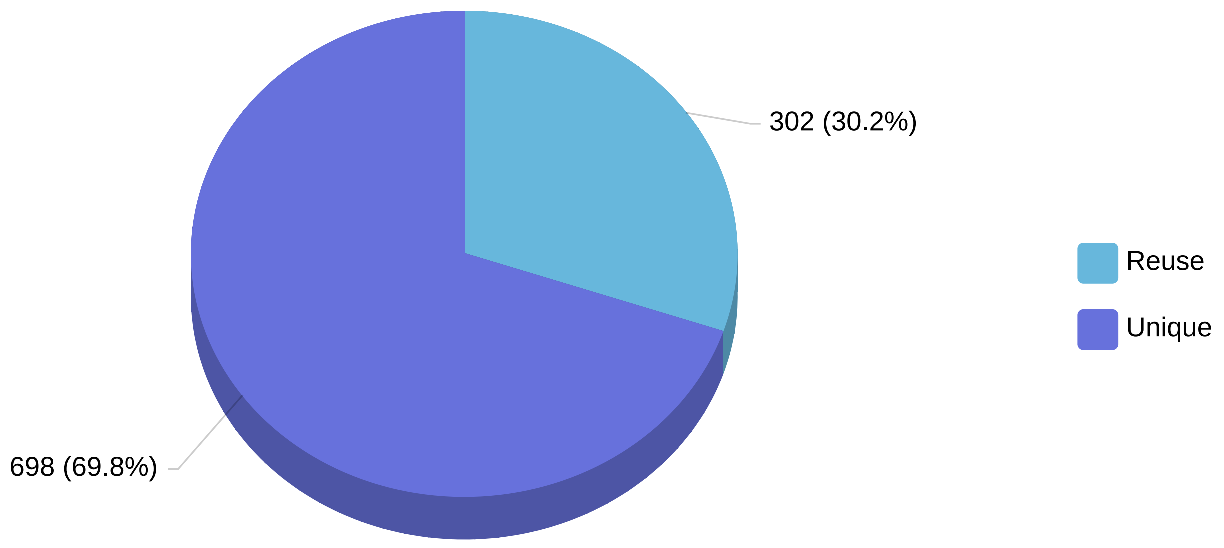
These passwords are generally weak and widespread, making them prime targets for attackers. A significant portion of compromised accounts used commonly chosen passwords.



Password Reuse

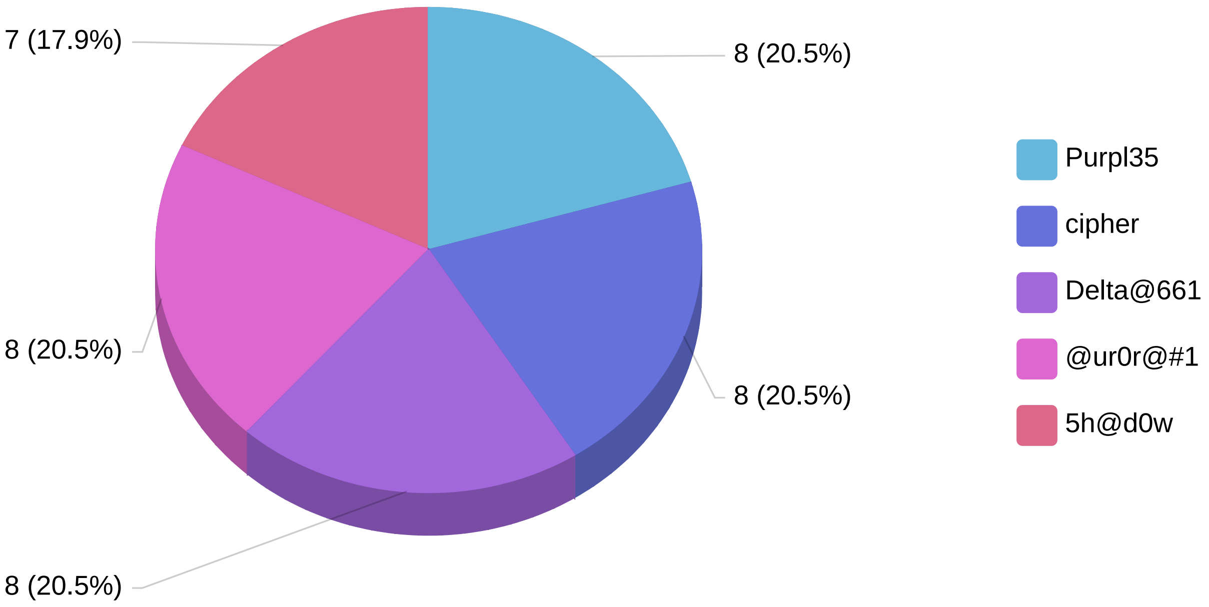
The chart below highlights password reuse among user accounts in the dataset (**all password hashes**).

The results show a reuse rate of **30.2%**, i.e. **302 accounts**. Reuse greatly increases the attack surface: if one account is compromised, all others sharing the same password become vulnerable.



Most Reused Passwords

The chart below shows the most reused passwords among those cracked. Passwords **cipher** and **@ur0r@#1** are reused in **1.4%** and **1.4%** of cracked passwords, respectively.



Most Common Patterns

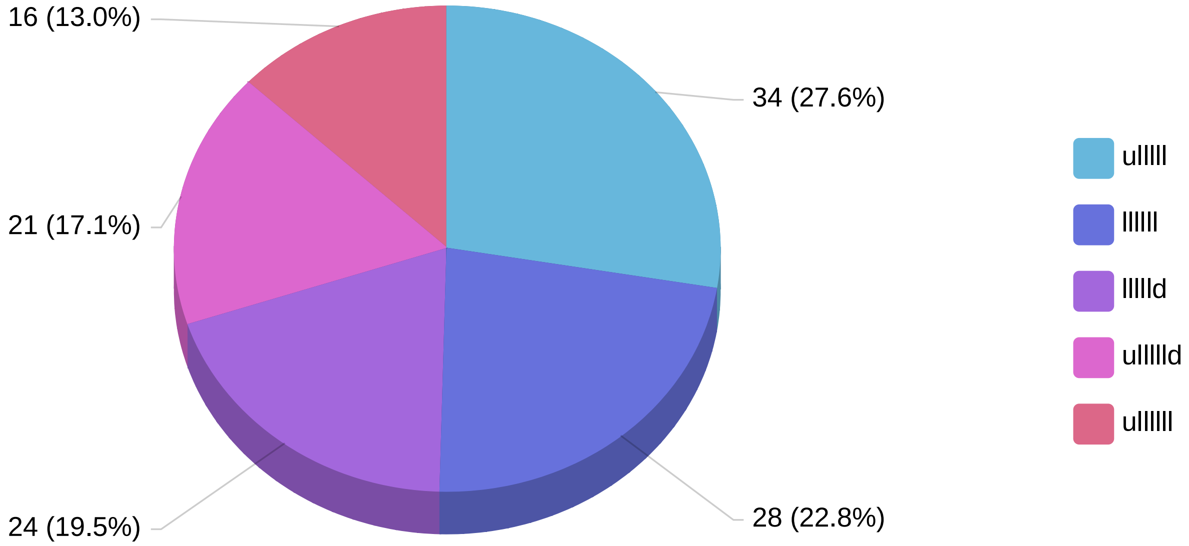
The pattern of a password can be analysed by looking at the sequence of character types it contains:

- **l** : lower-case letter
- **u**: upper-case letter
- **d**: digit
- **s**: special character

Examples of frequent patterns include:

- **`ullllllldd`**: e.g. *Password21*, starting with a capital letter and ending with two digits.
- **`ulllldddds`**: e.g. *Summer2018!*, starting with a capital letter and ending with four digits and a special character.

This analysis helps understand password-creation habits and target the most predictable combinations.



Remediation

To implement a strong password policy, apply the following measures:

- Use unique, complex passwords for each account or service.
- Ban common or company-related passwords.
- Encourage password-manager use to generate and store strong passwords.
- Use passwords of at least 12 characters.
- Combine uppercase, lowercase, digits and special symbols.
- Implement multi-factor authentication (MFA) for sensitive access.
- Disable storage of hashes using the LAN Manager (LM) algorithm.

References

- [FR] ANSSI – Multi-factor auth & password recommendations: https://www.ssi.gouv.fr/administration/guide/recommandations-relatives-a-lauthentification-multifacteur-et-aux-mots-de-passe/
- [FR] ANSSI – Active Directory security recommendations: https://www.ssi.gouv.fr/uploads/IMG/pdf/NP_ActiveDirectory_NoteTech.pdf
- [EN] OWASP – Authentication Cheat Sheet: https://www.owasp.org/index.php/Authentication_Cheat_Sheet#Implement_Proper_Password_Strength_Controls
- [EN] Microsoft – Prevent storing LM hash: https://learn.microsoft.com/en-us/troubleshoot/windows-server/windows-security/prevent-windows-store-lm-hash-password