WHITE KNIGHT LABS

ACME Corp
Password Audit Report

Report Details

Client Name: ACME Corp

Report Folder: ACME Corp Password Audit Report

Engagement Start Date: 01/13/2022

Engagement End Date: 01/15/2022

Total Runtime: 2 Days

Report Generation Date: 01/17/2022

Current Password Policy

Name: Default Password Policy

Complexity Enabled: True

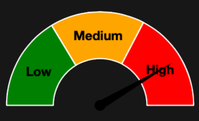
Max Password Age: 42 Days

Min Password Length: 8 Characters

Lockout Duration: 30 Minutes

Reversible Encryption Enabled: False

Risk of Current Passwords Cracked



Password Hashes
8549

Unique Password Hashes
5052

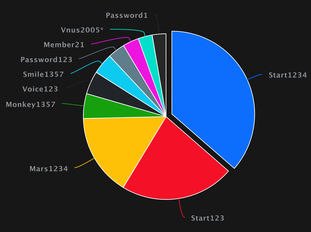
Passwords Discovered Through Cracking
7177

Unique Password Discovered Through Cracking
4013

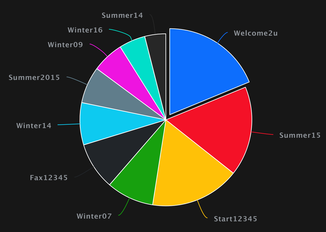
Percent of Current Passwords Cracked
83.95%

Percent of Unique Passwords Cracked
79.43%

Top 10 Password Reuse Stats



High Risk Password Stats



Password Length Stats

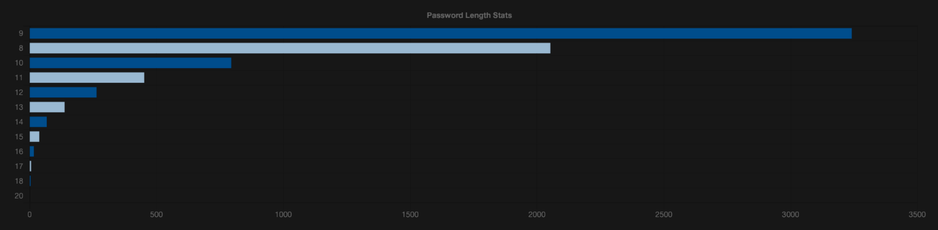
Top Password Use Stats

Password Reuse Stats

Password History

High Risk Password Stats

High Risk Users with Common Passwords



Active Directory Groups

Members of "Domain Admins" group
8

"Domain Admins" Passwords Cracked
4

Members of "Executives" group
18

"Executives" Passwords Cracked
12

Members of "VPN Users" group
122

"VPN Users" Passwords Cracked
89

Findings and Recommendations

Finding: High – Weak Password Policy

WKL discovered a weak domain account password policy for the domain. The 8-character password length allowance is a serious issue because this length of password makes brute-force attacks much simpler and oftentimes more successful. When the password hash of a 8-character password is retrieved and a cracking attempt is made, the likelihood of the password being cracked is far greater than a more lengthier password. The entire sequence of possible passwords within the alphanumeric range for a 8-character password can be brute forced within hours. It is almost guaranteed that this length of password can be cracked.

Recommendations

WKL recommends that ACME Corp adopt a domain-wide password policy with the following characteristics:

- 15+ characters minimum length
- Password complexity enabled
- 24 previous passwords remembered
- 15+ characters minimum length
- Max password age of 265 days
- 5 invalid logon attempts before lockout
- Indefinite lockout duration (until unlocked by administrator)
- Store passwords using reversible encryption: Disabled

Finding: High – Passwords Susceptible To Brute Force Attacks

WKL discovered multiple user accounts using a commonly guessable password or also known as a weak password. Weak passwords refer to any passwords that can easily be guessed. Examples of weak passwords would include variations of the following: username, company name, season and year, or common words such as 'password' Brute force attacks occur when a bad actor attempts a large amount of combinations on a target. These attacks frequently involve multiple attempts on account passwords with the hopes that one of them will be valid. The most common type of brute force attack is a dictionary attack and involves a list of credentials, typically by using common usernames and easily guessable passwords to gain access to emails accounts or remote services such a VPN.

Recommendations

WKL recommends deploying security awareness training to help combat the use of easly guessable passwords. Corporate password policies should include the following items to help users understand how to set secure passwords that cannot be easly guessed or brute forced.

Avoid using the following in passwords:

- Address (home and office)
- Name of employer or business office
- Date of birth or (Marriage, Childern, Pets, etc)
- Phone numbers
- Hobbies, sports teams, seasons, etc
- Common passphrases or song lyrics

Incorporate the following best password practices into corporate policies and security awareness training:

- **Password Length:** The longer the password, the harder to crack. While the password policy may only require 6 to 9 characters, expanding to 12, 16 or more will provide a stronger password.
- **Not in the dictionary:** Avoid single words or common phrases that can be found in the dictionary or vernacular.
- **Character substitutions:** Substituting characters for letters is a good practice. Best practice is to substitute uncommon characters for letters such as using the ampersand (&) for O.
- **Illogical phrases:** String together completely random words like "BreadSourDixyMuch" or "ToothLadyDifficultAnger"
- **Acronyms and abbreviations:** Instead of spelling out words, abbreviate them or replace phrases with acronyms that can be remembered.