

T1201 - Password Policy Discovery

Description from ATT&CK

Adversaries may attempt to access detailed information about the password policy used within an enterprise network or cloud environment. Password policies are a way to enforce complex passwords that are difficult to guess or crack through [Brute Force] (https://attack.mitre.org/techniques/T1110). This information may help the adversary to create a list of common passwords and launch dictionary and/or brute force attacks which adheres to the policy (e.g. if the minimum password length should be 8, then not trying passwords such as 'pass123'; not checking for more than 3-4 passwords per account if the lockout is set to 6 as to not lock out accounts).

Password policies can be set and discovered on Windows, Linux, and macOS systems via various command shell utilities such as net accounts (/domain), Get-ADDefaultDomainPasswordPolicy, chage -1, cat /etc/pam.d/common-password, and pwpolicy getaccountpolicies (Citation: Superuser Linux Password Policies) (Citation: Jamf User Password Policies). Adversaries may also leverage a Network Device CLI on network devices to discover password policy information.(Citation: US-CERT-TA18-106A)

Password policies can be discovered in cloud environments using available APIs such as GetAccountPasswordPolicy in AWS (Citation: AWS GetPasswordPolicy).

Atomic Tests

- Atomic Test #1 Examine password complexity policy Ubuntu
- Atomic Test #2 Examine password complexity policy CentOS/RHEL 7.x
- Atomic Test #3 Examine password complexity policy CentOS/RHEL 6.x
- Atomic Test #4 Examine password expiration policy All Linux
- Atomic Test #5 Examine local password policy Windows
- Atomic Test #6 Examine domain password policy Windows
- Atomic Test #7 Examine password policy macOS
- Atomic Test #8 Get-DomainPolicy with PowerView
- Atomic Test #9 Enumerate Active Directory Password Policy with getaddefaultdomainpasswordpolicy

Atomic Test #1 - Examine password complexity policy - Ubuntu

Lists the password complexity policy to console on Ubuntu Linux.

Supported Platforms: Linux

auto_generated_guid: 085fe567-ac84-47c7-ac4c-2688ce28265b

Attack Commands: Run with bash!

cat /etc/pam.d/common-password

Q

Atomic Test #2 - Examine password complexity policy - CentOS/RHEL 7.x

Lists the password complexity policy to console on CentOS/RHEL 7.x Linux.

Supported Platforms: Linux

auto_generated_guid: 78a12e65-efff-4617-bc01-88f17d71315d

Attack Commands: Run with bash!

cat /etc/security/pwquality.conf



Dependencies: Run with bash!

Description: System must be CentOS or RHEL v7

Check Prereq Commands:

if [\$(rpm -q --queryformat '%{VERSION}') -eq "7"]; then exit /b 0; els

Get Prereq Commands:

echo Please run from CentOS or RHEL v7



Atomic Test #3 - Examine password complexity policy - CentOS/RHEL 6.x

Lists the password complexity policy to console on CentOS/RHEL 6.x Linux.

Supported Platforms: Linux

auto_generated_guid: 6ce12552-0adb-4f56-89ff-95ce268f6358

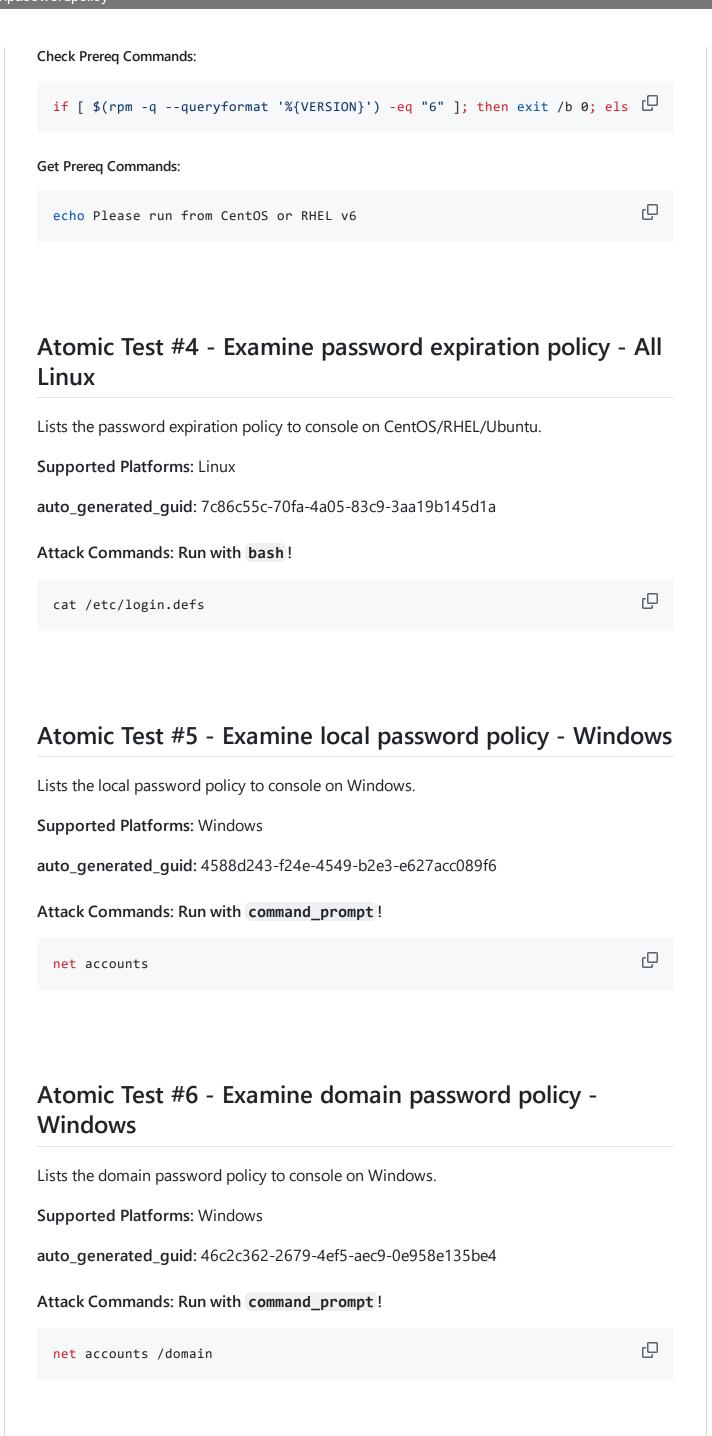
Attack Commands: Run with bash!

cat /etc/pam.d/system-auth
cat /etc/security/pwquality.conf

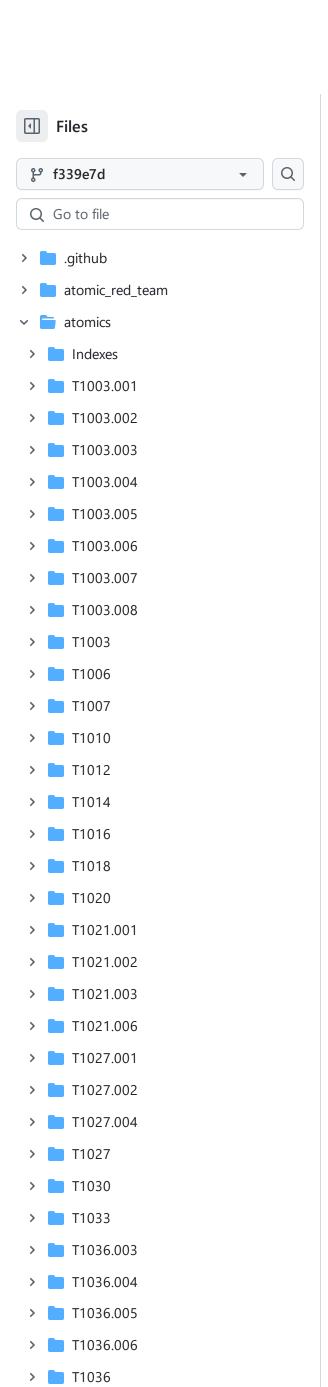


Dependencies: Run with bash!

Description: System must be CentOS or RHEL v6



Atomic Test #7 - Examine password policy - macOS



> T1037.001

