

Product

▼

Solutions

▼

Resources

▼

Open Source

▼

Enterprise

▼

Pricing

Sign in

Sign up

redcanaryco / atomic-red-team

Public

Notifications

Fork

2.8k

Star

9.7k

<> Code

Issues

6

Pull requests

5

Actions

Wiki

Security

Insights

Files

f339e7d

Go to file

> .github

> atomic\_red\_team

> atomics

> Indexes

> T1003.001

> T1003.002

> T1003.003

> T1003.004

> T1003.005

> T1003.006

> T1003.007

> T1003.008

> T1003

> T1006

> T1007

> T1010

> T1012

> T1014

> T1016

> T1018

> T1020

> T1021.001

> T1021.002

> T1021.003

> T1021.006

> T1027.001

> T1027.002

> T1027.004

> T1027

> T1030

> T1033

> T1036.003

> T1036.004

> T1036.005

> T1036.006

> T1036

atomic-red-team / atomics / T1552.002 / T1552.002.md

CircleCI Atomic Red Team doc...

Generate docs from job=gener...

36d49de · 3 years ago

History

PreviewCodeBlame74 lines (31 loc) · 1.96 KB

RawCopyDownloadMenu

# T1552.002 - Credentials in Registry

## Description from ATT&CK

Adversaries may search the Registry on compromised systems for insecurely stored credentials. The Windows Registry stores configuration information that can be used by the system or other programs. Adversaries may query the Registry looking for credentials and passwords that have been stored for use by other programs or services. Sometimes these credentials are used for automatic logons. Example commands to find Registry keys related to password information: (Citation: Pentestlab Stored Credentials)

- Local Machine Hive: `reg query HKLM /f password /t REG_SZ /s`
- Current User Hive: `reg query HKCU /f password /t REG_SZ /s`

## Atomic Tests

- [Atomic Test #1 - Enumeration for Credentials in Registry](#)
- [Atomic Test #2 - Enumeration for PuTTY Credentials in Registry](#)

## Atomic Test #1 - Enumeration for Credentials in Registry

Queries to enumerate for credentials in the Registry. Upon execution, any registry key containing the word "password" will be displayed.

**Supported Platforms:** Windows

**auto\_generated\_guid:** b6ec082c-7384-46b3-a111-9a9b8b14e5e7







**Attack Commands:** Run with `command_prompt` !

```
reg query HKLM /f password /t REG_SZ /s
reg query HKCU /f password /t REG_SZ /s
```

## Atomic Test #2 - Enumeration for PuTTY Credentials in Registry

Queries to enumerate for PuTTY credentials in the Registry. PuTTY must be installed for this test to work. If any registry entries are found, they will be displayed.

Page 1 of 2

- >  T1037.001
- >  T1037.002
- >  T1037.004
- >  T1037.005
- >  T1039
- >  T1040

Supported Platforms: Windows

auto\_generated\_guid: af197fd7-e868-448e-9bd5-05d1bcd9d9e5

Attack Commands: Run with `command_prompt` !

```
reg query HKCU\Software\SimonTatham\PuTTY\Sessions /t REG_SZ /s
```

