

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

atomic-red-team / atomics / T1003.005 / T1003.005.md

Atomic Red Team doc generat...

Generated docs from job=generate-...

d0dad62 · 2 years ago

History

Files

b27a3cb

Go to file

> .github

> atomic_red_team

> atomics

> Indexes

> T1003.001

> T1003.002

> T1003.003

> T1003.004

> T1003.005

T1003.005.md

T1003.005.yaml

> T1003.006

> T1003.007

> T1003.008

> T1003

> T1006

> T1007

> T1010

> T1012

> T1014

atomic-red-team / atomics / T1003.005 / T1003.005.md

↑ Top

PreviewCodeBlame

47 lines (22 loc) · 1.82 KB

RawCopyDownloadMenu

be used to extract the cached credentials.

Note: Cached credentials for Windows Vista are derived using PBKDF2.(Citation: PassLib mscache)

Atomic Tests

• Atomic Test #1 - Cached Credential Dump via Cmdkey

Atomic Test #1 - Cached Credential Dump via Cmdkey

List credentials currently stored on the host via the built-in Windows utility cmdkey.exe Credentials listed with Cmdkey only pertain to the current user Passwords will not be displayed once they are stored <https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/cmdkey> <https://www.peew.pw/blog/2017/11/26/exploring-cmdkey-an-edge-case-for-privilege-escalation>























Supported Platforms: Windows

auto_generated_guid: 56506854-89d6-46a3-9804-b7fde90791f9

Attack Commands: Run with `command_prompt` !

cmdkey /list

Page 1 of 2

- >  T1016
- >  T1018
- >  T1020
- >  T1021.001
- >  T1021.002
- >  T1021.003
- >  T1021.006
- >  T1027.001
- >  T1027.002
- >  T1027.004
- >  T1027.006
- >  T1027
- >  T1030
- >  T1033
- >  T1036.003
- >  T1036.004
- >  T1036.005
- >  T1036.006
- >  T1036
- >  T1037.001
- >  T1037.002
- >  T1037.004