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 / T1552.003 / T1552.003.md

Atomic Red Team doc generat... Generated docs from job=generate-d... 819934c · 2 years ago History

Preview Code Blame 44 lines (21 loc) · 1.7 KB Raw

T1552.003 - Bash History

Description from ATT&CK

> Adversaries may search the bash command history on compromised systems for insecurely stored credentials. Bash keeps track of the commands users type on the command-line with the "history" utility. Once a user logs out, the history is flushed to the user's `.bash_history` file. For each user, this file resides at the same location: `~/.bash_history`. Typically, this file keeps track of the user's last 500 commands. Users often type usernames and passwords on the command-line as parameters to programs, which then get saved to this file when they log out. Adversaries can abuse this by looking through the file for potential credentials. (Citation: External to DA, the OS X Way)

Atomic Tests

- Atomic Test #1 - Search Through Bash History

Atomic Test #1 - Search Through Bash History

Search through bash history for specifice commands we want to capture

Supported Platforms: Linux, macOS

auto_generated_guid: 3cfde62b-7c33-4b26-a61e-755d6131c8ce

Inputs:

Name	Description	Type	Default Value
output_file	Path where captured results will be placed	Path	~/loot.txt
bash_history_grep_args	grep arguments that filter out specific commands we want to capture	Path	-e '-p ' -e 'pass' -e 'ssh'
bash_history_filename	Path of the bash history file to capture	Path	~/.bash_history

Attack Commands: Run with `sh`!

```
cat #{bash_history_filename} | grep #{bash_history_grep_args} > #{output_
```

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