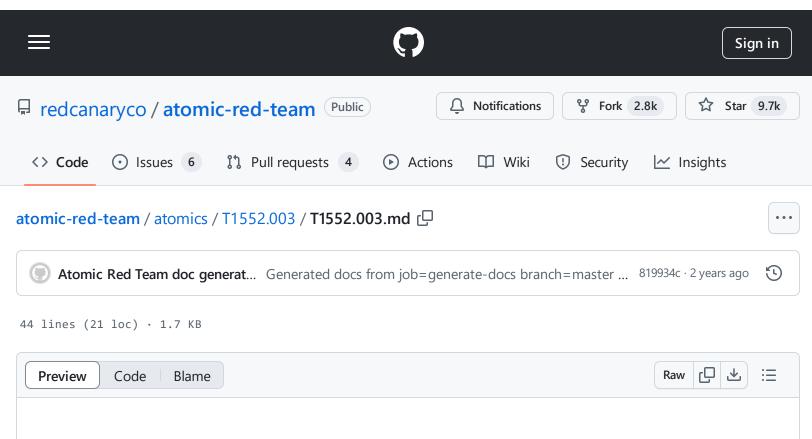
atomic-red-team/atomics/T1552.003/T1552.003.md at f339e7da7d05f6057fdfcdd3742bfcf365fee2a9 redcanaryco/atomic-red-team · GitHub - 31/10/2024 14:45 https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1552.003/T1552.003.md



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 <code>.bash_history</code> file. For each user, this file resides at the same location: <code>~/.bash_history</code>. 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 | Туре | 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!