Unsecured Credentials: Shell History, Sub-technique T1552.003 - Enterprise

Archived: 2026-04-05 13:29:57 UTC

Adversaries may search the command history on compromised systems for insecurely stored credentials.

On Linux and macOS systems, shells such as Bash and Zsh keep 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 history file. For each user, this file resides at the same location: for example, `~/.bash_history` or `~/.zsh_history`. Typically, these files keeps track of the user's last 1000 commands.

On Windows, PowerShell has both a command history that is wiped after the session ends, and one that contains commands used in all sessions and is persistent. The default location for persistent history can be found in `%userprofile%\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline\ConsoleHost_history.txt`, but command history can also be accessed with `Get-History`. Command Prompt (CMD) on Windows does not have persistent history.[1][2]

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.[3]

Source: https://attack.mitre.org/techniques/T1552/003