Sign in

redcanaryco / atomic-red-team Public

Notifications Fork 2.8k Star 9.7k

Code Issues 6 Pull requests 4 Actions Wiki Security Insights

atomic-red-team / atomics / T1070.003 / T1070.003.md

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

383 lines (163 loc) · 7.9 KB

Preview Code Blame Raw

T1070.003 - Clear Command History

Description from ATT&CK

> In addition to clearing system logs, an adversary may clear the command history of a compromised account to conceal the actions undertaken during an intrusion. Various command interpreters keep track of the commands users type in their terminal so that users can retrace what they've done.
> On Linux and macOS, these command histories can be accessed in a few different ways. While logged in, this command history is tracked in a file pointed to by the environment variable `HISTFILE`. When a user logs off a system, this information is flushed to a file in the user's home directory called `~/.bash_history`. The benefit of this is that it allows users to go back to commands they've used before in different sessions.
>
> Adversaries may delete their commands from these logs by manually clearing the history (`history -c`) or deleting the bash history file `rm ~/.bash_history`.
>
> Adversaries may also leverage a Network Device CLI on network devices to clear command history data.(Citation: US-CERT-TA18-106A)

> On Windows hosts, PowerShell has two different command history providers: the built-in history and the command history managed by the `PSReadLine` module. The built-in history only tracks the commands used in the current session. This command history is not available to other sessions and is deleted when the session ends.
>
> The `PSReadLine` command history tracks the commands used in all PowerShell sessions and writes them to a file (`$env:APPDATA\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt` by default). This history file is available to all sessions and contains all past history since the file is not deleted when the session ends.(Citation: Microsoft PowerShell Command History)
>
> Adversaries may run the PowerShell command `Clear-History` to flush the entire command history from a current PowerShell session. This, however, will not delete/flush the `ConsoleHost_history.txt` file. Adversaries may also delete the `ConsoleHost_history.txt` file or edit its contents to hide PowerShell commands they have run.(Citation: Sophos PowerShell command audit)(Citation: Sophos PowerShell Command History Forensics)

Atomic Tests

- Atomic Test #1 - Clear Bash history (rm)
- Atomic Test #2 - Clear Bash history (echo)
- Atomic Test #3 - Clear Bash history (cat dev/null)
- Atomic Test #4 - Clear Bash history (ln dev/null)
- Atomic Test #5 - Clear Bash history (truncate)
- Atomic Test #6 - Clear history of a bunch of shells
- Atomic Test #7 - Clear and Disable Bash History Logging
- Atomic Test #8 - Use Space Before Command to Avoid Logging to History
- Atomic Test #9 - Disable Bash History Logging with SSH -T
- Atomic Test #10 - Prevent Powershell History Logging
- Atomic Test #11 - Clear Powershell History by Deleting History File

Atomic Test #1 - Clear Bash history (rm)

Clears bash history via rm

Supported Platforms: Linux, macOS

auto_generated_guid: a934276e-2be5-4a36-93fd-98adbb5bd4fc

Attack Commands: Run with `sh`!

```
rm ~/.bash_history
```

Atomic Test #2 - Clear Bash history (echo)

Clears bash history via rm

Supported Platforms: Linux

auto_generated_guid: cbf506a5-dd78-43e5-be7e-a46b7c7a0a11

Attack Commands: Run with `sh`!

```
echo "" > ~/.bash_history
```

Atomic Test #3 - Clear Bash history (cat dev/null)

Clears bash history via cat /dev/null

Supported Platforms: Linux, macOS

auto_generated_guid: b1251c35-dcd3-4ea1-86da-36d27b54f31f

Attack Commands: Run with `sh`!

```
cat /dev/null > ~/.bash_history
```

Atomic Test #4 - Clear Bash history (ln dev/null)

Clears bash history via a symlink to /dev/null

Supported Platforms: Linux, macOS

auto_generated_guid: 23d348f3-cc5c-4ba9-bd0a-ae09069f0914

Attack Commands: Run with `sh`!

```
ln -sf /dev/null ~/.bash_history
```

Atomic Test #5 - Clear Bash history (truncate)

Clears bash history via truncate

Supported Platforms: Linux

auto_generated_guid: 47966a1d-df4f-4078-af65-db6d9aa20739

Attack Commands: Run with `sh`!

```
truncate -s0 ~/.bash_history
```

Atomic Test #6 - Clear history of a bunch of shells

Clears the history of a bunch of different shell types by setting the history size to zero

Supported Platforms: Linux, macOS

auto_generated_guid: 7e6721df-5f08-4370-9255-f06d8a77af4c

Attack Commands: Run with `sh`!

```
unset HISTFILE
export HISTFILESIZE=0
history -c
```

Atomic Test #7 - Clear and Disable Bash History Logging

Clears the history and disable bash history logging of the current shell and future shell sessions

Supported Platforms: Linux, macOS

auto_generated_guid: 784e4011-bd1a-4ecd-a63a-8feb278512e6

Attack Commands: Run with `sh`!

```
set +o history
echo 'set +o history' >> ~/.bashrc
. ~/.bashrc
history -c
```

Cleanup Commands:

```
sed -i 's/set +o history//g' ~/.bashrc
. ~/.bashrc
set -o history
```

Atomic Test #8 - Use Space Before Command to Avoid Logging to History

Using a space before a command causes the command to not be logged in the Bash History file

Supported Platforms: Linux, macOS

auto_generated_guid: 53b03a54-4529-4992-852d-a00b4b7215a6

Attack Commands: Run with `sh`!

```
hostname
whoami
```

Atomic Test #9 - Disable Bash History Logging with SSH -T

Keeps history clear and stays out of lastlog,wtmp,btmp ssh -T keeps the ssh client from catching a proper TTY, which is what usually gets logged on lastlog

Supported Platforms: Linux

auto_generated_guid: 5f8abd62-f615-43c5-b6be-f780f25790a1

Attack Commands: Run with `sh`!

```
sshpass -p 'pwd101!' ssh testuser1@localhost -T hostname
```

Cleanup Commands:

```
userdel -f testuser1
```

Dependencies: Run with `sh`!

Description: Install sshpass and create user account used for excuting

Check Prereq Commands:

```
$(getent passwd testuser1 >/dev/null) && $(which sshpass >/dev/null)
```

Get Prereq Commands:

```
/usr/sbin/useradd testuser1
echo -e 'pwd101!\npwd101!' | passwd testuser1
(which yum && yum -y install epel-release sshpass)||(which apt-get && DEBIAN_FRONT
```

Atomic Test #10 - Prevent Powershell History Logging

Prevents Powershell history

Supported Platforms: Windows

auto_generated_guid: 2f898b81-3e97-4abb-bc3f-a95138988370

Attack Commands: Run with `powershell`!

```
Set-PSReadlineOption –HistorySaveStyle SaveNothing
```

Cleanup Commands:

```
Set-PSReadLineOption -HistorySaveStyle SaveIncrementally
```

Atomic Test #11 - Clear Powershell History by Deleting History File

Clears Powershell history

Supported Platforms: Windows

auto_generated_guid: da75ae8d-26d6-4483-b0fe-700e4df4f037

Attack Commands: Run with `powershell`!

```
Remove-Item (Get-PSReadlineOption).HistorySavePath
```