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 / T1070.002 / T1070.002.md

CircleCI Atomic Red Team doc... Generate docs from job=gener... 36d49de · 3 years ago History

Preview Code Blame 117 lines (54 loc) · 2.57 KB Raw

T1070.002 - Clear Linux or Mac System Logs

Description from ATT&CK

> Adversaries may clear system logs to hide evidence of an intrusion. macOS and Linux both keep track of system or user-initiated actions via system logs. The majority of native system logging is stored under the `/var/log/` directory. Subfolders in this directory categorize logs by their related functions, such as:(Citation: Linux Logs)
>
> - `/var/log/messages:`: General and system-related messages
> - `/var/log/secure` or `/var/log/auth.log`: Authentication logs
> - `/var/log/utmp` or `/var/log/wtmp`: Login records
> - `/var/log/kern.log`: Kernel logs
> - `/var/log/cron.log`: Crond logs
> - `/var/log/maillog`: Mail server logs
> - `/var/log/httpd/`: Web server access and error logs

Atomic Tests

- Atomic Test #1 - rm -rf
- Atomic Test #2 - Overwrite Linux Mail Spool
- Atomic Test #3 - Overwrite Linux Log

Atomic Test #1 - rm -rf

Delete system and audit logs

Supported Platforms: macOS, Linux

auto_generated_guid: 989cc1b1-3642-4260-a809-54f9dd559683

Attack Commands: Run with `sh`! Elevation Required (e.g. root or admin)

```
sudo rm -rf /private/var/log/system.log*
sudo rm -rf /private/var/audit/*
```

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

Atomic Test #2 - Overwrite Linux Mail Spool

This test overwrites the Linux mail spool of a specified user. This technique was used by threat actor Rocke during the exploitation of Linux web servers.

Supported Platforms: Linux

auto_generated_guid: 1602ff76-ed7f-4c94-b550-2f727b4782d4

Inputs:

Name	Description	Type	Default Value
username	Username of mail spool	String	root

Attack Commands: Run with `bash`!

```
echo 0> /var/spool/mail/#{username}
```

Atomic Test #3 - Overwrite Linux Log

This test overwrites the specified log. This technique was used by threat actor Rocke during the exploitation of Linux web servers.

Supported Platforms: Linux

auto_generated_guid: d304b2dc-90b4-4465-a650-16ddd503f7b5

Inputs:

Name	Description	Type	Default Value
log_path	Path of specified log	Path	/var/log/secure

Attack Commands: Run with `bash`!

```
echo 0> #{log_path}
```