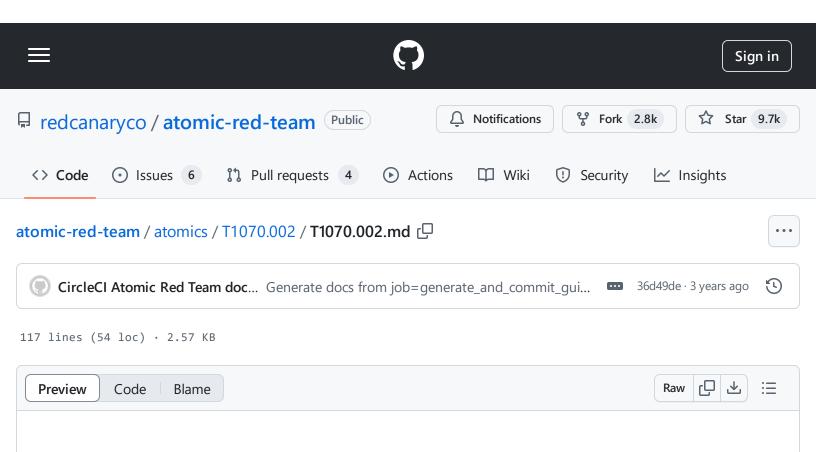
atomic-red-team/atomics/T1070.002/T1070.002.md at f339e7da7d05f6057fdfcdd3742bfcf365fee2a9 · redcanaryco/atomic-red-team · GitHub - 31/10/2024 15:08 https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1070.002/T1070.002.md



# 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 <a href="https://www.logs/">/www.logs/</a> 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/*
```

راً

### **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	Туре	Default Value
username	Username of mail spool	String	root

Attack Commands: Run with bash!

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

ی

## 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	Туре	Default Value
log_path	Path of specified log	Path	/var/log/secure

Attack Commands: Run with bash!

echo 0> #{log\_path}

ιÖ