**Why Cover Your Tracks**

**To hide history**

* Commands
* Logins
* Elevation
* File changes

**Clearing options**

Partial

* Clearing specific log entries to hide specific actions

Full

* Full clear of whole log file

**Partial**

* When stealth is paramount
* Avoiding monitoring system like Splunk that pull the logs
  + Log at syslog and Splunk config files to see how often it pulls the logs
  + Write a wrapper for your commands that execute and wipe from the correct log as you go

**Full**

* When stealth isn’t important
  + Very obvious when a log has been completely cleared
* Can be used on a pivot machine to avoid following the attacker
* Not commonly used