- Filename: eccouncil-ceh31250-v11-6-10-1-covering-tracks.md
- Show Name: CEHv11 (312-50)
- Topic Name: System Hacking Phases and Attack Techniques - System Hacking
- Episode Name: Covering Tracks
  ==

Covering Tracks

Objectives:

- Explain the reasoning behind why an attacker clears logs
- Demonstrate techniques and tactics for clearing logs in a Windows and Linux Operating Systems
- Explain the purpose of disabling auditing systems during an attack
- Show how auditing systems could be disabled during an attack
- List and define common defensive maneuvers against attackers attempting to cover their tracks

---

- Once a threat actor has compromised a system or network only part of the battle has been won. It seems that now they would be scrambling to hide their presence and destroy evidence of their compromise or 'cover their tracks'. What are some of the main ways in which they try to accomplish this?
  - Disable Auditing systems
    - Stop recording/reporting activity that may alert admins to compromise
  - Clearing Logs
    - Destroy evidence so that admins...
      - Don't pick up on intruder presence
      - Thwart forensic investigation
- It really makes sense that an attacker would turn off systems that would be gathering evidence of their presence and activity. What are some methods used by attackers and ethical hackers to disable auditing?
  - If Windows
    - Auditpol
      - `auditpol /set /category:"system","account logon" /success:disable /failure:disable`
    - Fsutil (disable last access timestamp)
      - `fsutil behavior set disablelastaccess 1`
    - Disable Restore Points
      - Attacker could trigger events that create a restore point
    - Other
      - Windows Hibernation file
      - Windows Virtual memory (Page file)
  - If Linux
    - Disable bash history recording
      - `export HISTSIZE=0`

        - Auditd (RHEL)
            - `auditd -s disable`

- Now you also mentioned something about clearing logs. What methods would an attacker use to clear logs to cover their tracks?
    - Windows
        - `Clear-EventLog "Windows PowerShell"`
        - `wevutit -cl Security`
        - Metasploit `clearev`
        - `cipher.exe`
            - overwrites deleted files
        - Windows Event Viewer
    - Linux
        - `/var/log`
        - `history -c`
        - `history -w`
        - `echo " " > ~/.bash_history`
        - `shred file1.txt`
            - makes file contents unreadable

- Are there any good defenses against this type of activity?
    - syslog
    - Event Viewer Subscriptions
    - SIEM