- Filename: eccouncil-ceh31250-v10-6-6-1-covering_tracks.md
- Show Name: CEHv10 (312-50)
- Topic Name: Attacks and Exploits
- Episode Name: Covering Tracks
- Description: In this episode, Daniel and Zach discuss techniques and tactics for covering your tracks after you've breached a system. Here you'll learn how to remove traces of your activities by disabling auditing systems and clearing logs.

==

Covering Tracks

- **If we are hired to perform a penetration test, why would we need to cover our tracks?**
    - Various reasons
        - True Red Team activity
        - To test the Blue Team's ability to discover a breach
- **So how would one go about covering one's tracks?**
    - Disable auditing mechanisms
        - Prevents logging at all
    - Clear logs
        - Removes logs that attacker creates
            - Wholesale removal
            - Selective removal
    - Falsify logs
        - Change the log's attributes with false information
- **Can you demonstrate some of these techniques for us?**
    - Disable auditing
        - `export HISTSIZE=0`
        - `auditpol \\computername /audit_object:all /disable`
            - Audit Objects
                - system
                - account
                - policy
                - directory
                - logon
                - object access
                - sam
                - privilege
                - process
    - Clearing event logs
        - `echo " " > /var/log/syslog`
        - Metasploit `clearev`
            - Clears all Windows Event logs
        - Windows Cmd shell: `webtutil cl Application`
            - Clears Application logs
    - Clearing specific log entries

  - `sed -i '/revshell/d' /var/log/auth.log`

- Alter or forge log entries
- Erase shell history
  - `history -c`
    - Clears history
  - `history -w`
    - Clears current shell history
  - `echo " " > ~/.bash_history`
  - `history -c`
  - Windows: Atl+F7 clears cmd history
  - PS$:> Clear-History
- Destroy files
  - Secure overwrite with zeros
    - Linux: `shred -zu filename`
    - Windows: `format d: /fs:NTFS /p:1`
- Change timestamps
  - Meterpreter: `timestomp filename -z "08/29/2018 15:22:43"`
    - Changes all MACE values
      - Modified, Access, Created, Entry-modified