Covering Your Tracks

- Hide - malicious acts
  - Goal - maintain access, unnoticed, avoid getting caught
- Use of rootkits, log overwriting, concealed channels
  - Cookies over the browser
- Once a system has been compromised, the attacker is not finished
- The attacker must cover their tracks
  - Disable logging, Clear log files, Eliminate evidence, Plant additional tools

Covering Your Tracks

- Planting Rootkits
  - One of the goals of hacking is to allow the attacker to access the box at a later time
  - This can be done by installing a rootkit
  - Rootkit
    - A collection of software tools that a cracker uses to obtain administrator access
    - Can also monitor traffic, keystrokes, create backdoors, alter log files, attack other systems, alter existing tools to circumvent detection

Covering Your Tracks

- Clearing the Event Log
  - The attacker will want to clear the logs in Event Viewer
  - Tools
    - Eslave – clears the security log
    - Evidence Eliminator – very powerful, easy to use log cleanser
    - Winzapper – can erase event records selectively

Covering Your Tracks

- **Practice**: check for rootkit vs system audit
- Using: rkhunter
  - sudo apt-get install rkhunter
- Run:
  - sudo rkhunter –check

Covering Your Tracks

- **Practice**: check for rootkit vs system audit
- Using: chkrootkit
  - sudo apt-get install chkrootkit
- Run:
  - sudo chkrootkit

Covering Your Tracks

- **Practice**: check for rootkit vs system audit
- Using: lynis
  - sudo apt-get install lynis
- Run:
  - sudo lynis --check-all –quick
  - sudo lynis –pentest

Happy Day