* Filesystem monitoring
  + What 2 collect
    - Permission
    - Size
    - Link
    - Checksums
  + Cons
    - Not real time
    - New application => huge amount of alerts
* Log file
  + System log
  + Web server log
* Connection analysis
  + Monitor connection to host
  + Not perform pattern matching + correlation( snort job)
  + Scan 4
    - Unauthorized TCP connection
    - Port scan
    - Passive detection
    - Flood detection
* Kernel-based intrusion detection: add feature to kernel. Kernel itself detects intrusion.
  + Effective