Security Assessment & Testing | Ivan Notes 2022

- **Validation**
  - Verification
    - Rigour
- **Testing a system**
  - unit
  - interface
  - integration
  - system
- **Testing techniques**
  - methods & tools
    - manual
    - automated
  - runtime
    - static
    - dynamic
    - fuzz
  - access to code
    - white box
    - black box
  - techniques
    - positive
    - negative
    - misuse
    - boundary value analysis
    - equivalence partitioning
  - operational

        - real user monitoring
        - synthetic performance monitoring
        - regression testing

Testers / Assessors

- internal
- external
- 3P
    - usually SOC reports
        - SOC 2
            - Type 1 (DE)
            - Type 2 (OE over period of time)
- Roles
    - Executive mgmt
    - audit committee
    - security officer
    - compliance manager
    - internal / external auditor

Metrics

- KPIs
    - backword looking metrics
- KRIs
    - forward looking metrics

Identifying Vulns

- Vuln assessment
- Pentesting
- Process
    - recon
    - enumeration (active)
    - vuln analysis
    - execution

    - document findings
  - Testing techniques
    - perspective
      - internal
      - external
    - approach
      - blind
      - double blind
    - knowledge
      - zero / blackbox
      - full / whitebox
      - partial
  - types of scans
    - credentialed
    - uncredentialed
  - Banner grabbing & fingerprinting
  - interpreting & understanding results
    - CVE
      - unique identifier for each vuln
    - CVSS
      - 0-10
  - False positives, False negatives
- **Log review & analysis**
  - Monitor for
    - errors
    - modifications
    - breaches
  - SIEM
    - generation
      - limiting log file size

      - circular overwrite
      - clipping levels
    - time stamps
      - consistent
      - NTP
  - transmission
  - collection / aggregation
  - normalization
  - Analysis
  - Retention
  - Disposal
- Continuous monitoring