# CompTia Notes: Application, Data, and Host Security

* Application Security Controls and Techniques
  + Fuzzing
    - Trying to crash a program by putting in random data over and over again
    - Kali-Linux, CERT BFF
  + Kali Linux and Pen Testing Tools
    - Install on VMWare and explore applications
  + Secure Coding Concepts
    - Balance between time to market and security
    - Imput validation
      * Sanitize and validate
      * Mitigate attacks via XSS
      * OWASP and CERT
  + XSS and XSRF
  + Application Baseline Configuration and Application Hardening
    - Everything is up to date and patched
    - All unnecessary features, ports, services, etc. are disabled and removed
  + Multi-tiered Approach and Application Patching
    - 2 tier: client and database
    - 3 tier: client, webserver, database server
    - Applications should be routinely patched as part of a monthly maintenance cycle, as well as able to be manually patched if necessary
  + SQL vs. NoSQL databases
    - Table of related data
    - NoSQL is good for big data, mongoDB, Google BigTable , non-relational or distributed database, document based, key value pairs, graph,
  + Server-side vs. Client-side validation
    - Client-side is faster than server side
    - Can be bypassed by disabling JavaScript in the browser or intercepting HTTP post and modifying before its sent to the server
    - Server-side talks longer but is more secure as it can’t be bypassed by the client
* Mobile Security concepts and Technologies
  + Device Security
    - Challenges:
      * Full Device Encryption
      * Remote Wiping
      * Lockout
      * GPS
      * Storage segmentation
      * Things getting lost/stolen
      * Being compromised on public Wi-Fi
      * Asset tracking
      * Application management
    - Things like airwatch and mobile iron allow you to partition off a piece of a laptop or phone to be under corporate control. Makes it easier to BYOD and for corporate to control just what they need to.
    - Require strong passwords, constantly enabled and required
  + Key Credential Management and Authentication
    - Manage device content, access and authentication is critical to providing a secure environment
    - Digital certificates are used to authenticate users to access resources.
    - Allows certificate to be revoked if user leaves company, gets phone stolen, etc.
  + Geo-tagging
    - Pictures are geotagged when taken on most devices
    - Shows where phone has been, could be problematic when photos are uploaded to other websites
  + Transitive Trusts
    - A=B and B = C then A = C
    - If we allow this, we must make sure all transitive trusts are secure
  + BYOD Concerns
    - Data ownership
    - Support ownership
    - Patch management
    - Must have a clearly defined agreement with the employee
    - Forensics
    - Antivirus management
    - On-boarding/off-boarding
    - Infrastructure considerations
    - Legal concerns
    - Acceptable use policy
* Establishing Host Security
  + Operating System Security and Settings
    - Patch
    - Disable unnecessary applications
    - Disable unnecessary services
    - Enable Firewall, possibly set up extra firewalls
  + OS Hardening
  + Patch Management
  + White Listing and Black Listing Applications
  + Trusted OS
    - Evaluation Assurance levels are on a scale of 1 to 7
    - Most OS are at 4 for commercial use
    - Higher EAL is more secure
  + Host Based Firewalls
    - ZoneAlarm will allow you to see all the different types of connections going in and out of a network
  + Host Based Intrusion Detection
  + Hardware Security
  + Host Software Baselining and Virtualization
    - Can use VMWare to take snapshots of OS and can be saved
    - Can be used for testing upgrades, patches, and adjustments to the OS, applications or settings
    - Makes restoration very easy
    - Can do P2v (physical to virtual) to clone systems
    - Times to use it:
      * Testing Patch Compatibility
      * Regression testing
      * Better host availability/ elasticity
      * Test scale, see what happens when use goes up
      * Makes isolated environment (sandbox) to test when viruses get introduces to the system