CompTIA Security + 1.0 Threats,Attacks and Vulnerabilities

Filename: comptia-secplussy0501-1-6-impact_of_various_vulnerabilities
Title: Impact of Various Vulnerabilities
Subtitle: CompTIA Security+ (SY0-501)

1.6 Impact of Various Vulnerabilities

- 1.6 Explain the impact associated with types of vulnerabilities
  - Race conditions
    - A situation in which a system tries to accomplish two or more operations at the same time.
    - If the operations need to be processed sequentially, there might be a condition in which the operations are processed incorrectly causing a crash or data coruptions
    - Light switch analogy (more than one can render all of the switchs irrelavent)
    - A system recieves two operations on a large amount of data in which one operation is read, and one is write.
    - Old data might be overwritten before the read process finishes
  - Vulnerabilities due to:
    - End-of-life systems
    - Embedded systems
      - Lack of software updates
      - Could be new technology with old software
      - Code injection attacks
    - Lack of vendor support
  - Improper input handling
    - Application trusting, external entity trusting
    - Not checking/validating the data coming from the client or external source
    - Not checking for syntax correctness
    - Larger or more complex applications can have multiple data entry points
    - Code Injection, SQL Injection, XSS, Directory Traversal
    - DoS situtaions can happen when a *resource exhaustion* is accomplished by flooding the system with unexpected input.
  - Improper error handling
    - Examples (Incorrect)
      - Login for *User*: Invalid Password
      - Login Failed: Invalid User ID
      - Login Failed: Account Disabled
      - Login Failed: User is not active
    - Examples (Correct)
      - Login Failed: Invalid UserID or Password
  - Misconfiguration/weak configuration
  - Default configuration
  - Resource exhaustion(*mentioned in Improper input handling*)
  - Untrained users
  - Improperly configured accounts
    - Guest Accounts
    - Administrator Accounts
    - Shared Accounts
    - Managed Service Accounts
    - Not Implementing SSO
  - Vulnerable business processes
  - Weak cipher suites and implementations
    - SSL 2.0/3.0
    - TLS 1.0(no downgrade to SSL 3.0), 1.1, 1.2
    - WEP, WPA, WPA2
    - PPTP/MPPE vs L2TP/IPSec
    - RC4 vs RC5
  - Memory/buffer vulnerability
    - Memory leak
    - Integer overflow
      - 8 Bits of data are required to store the number 155(10011011) and if a process adds 101 to this value then 8 bits no longer holds the results of the process as 256 takes 9 bits or = 100000000
    - Buffer overflow
    - Pointer dereference
      - Also known as NULL pointer dereference
      - Can cause application crashes
      - Can cause code injection depending on applicaton privileges.
    - DLL injection
      - Attach to the process
      - Allocate Memory within the process
      - Copy the DLL or the DLL Path into the processes memory and determine appropriate memory addresses
      - Instruct the process to Execute your DLL

- System
- Architecture/design weaknesses
- New threats/zero day
  - Most tools rely on a database of only KNOWN threats
  - Polymorphic, code morphing, and obfuscation techniques make it hard for these tools to maintain a database on known threats
  - On average a threat can remain unknown to the public including vendors from 8 months to a year
  - very popular for purchase on the black market
- Improper certificate and key management
  - Unauthorized disclosure of the private key
  - Key modification
  - Key integrity issue or corruption
  - Improper key usage (show key usuage in Chrome >Developer Tools > Security Tab at top)