Vulnerability Assessment and Data Security

A vulnerability assessment is a thorough and methodical evaluation of the security posture of the enterprise, examining the exposure to hackers, forces of nature, and any harmful entity

security posture - an approach, philosophy, or strategy regarding security

Vulnerability Assessment

Asset Identification

Inventory of items with value, and their relative value; how critical is the asset, how much revenue it generates, how difficult is it to replace, and the impact if it is gone.

- people
- physical assets
- data
- hardware
- software

Threat Evaluation

List potential threats that come from threat agents

- threat modeling - attempt to understand attackers and their goal, via threat scenarios
- attack tree - potential attacks

Vulnerability Appraisal

- determine current weakness
- take snapshot of current security
- catalog each vulnerability when viewing assets in light of threats

Risk Management

- assess damage that would result from attack
- determine likelihood that vulnerability is exploited

Risk Mitigation

- determine what to do about risks, and what should be tolerated

Vulnerability Assessment Tools

- port scanners

- protocol analyzers / sniffers
- honeypots & honeynets - bait
- banner grabbing tools
- crackers
- command line tools
- exploitation framework - replicate attacks
- steganography

Vulnerability scans

- intrusive, non-intrusive
- active (probes), passive (no probes), credentialed & non-credentialed
- can detect new systems added
- when an application is compromised
- when a port scanner is run
- which ports are ingress / egress
- network mapping scanner, wireless scanner, configuration compliance scanner

Penetration Testing

- blackbox, whitebox, graybox - amount of knowledge of system
- active & passive reconnaissance

Secure Methodology

- creating a security posture
- selecting and configuring controls
- hardening
- reporting

Controls

- confidentiality - encryption, steganography, access controls
- integrity - hashing, digital signatures, certificates, nonrepudiation tools
- availability - redundancy, fault tolerance, patching
- safety - fencing and lighting, locks, CCTV, escape plans and routes, safety drills

  Some are for detection, some are for prevention

What is a higher priority when X happens - security or safety?

- fail-safe locks, vs. fail-open locks