Operations Security

Mike Smith

26/04/10 - Rev.26

Penetration Testing

1. Discovery - Footprinting and info gathering
2. Enumeration - port scans and resource identification
3. Vulnerability mapping - identify vulnerabilities
4. Exploitation - attempt to gain access
5. Report to management

Vulnerability Testing

- Personnel testing
- Physical testing
- System and network testing

E-mail

- POP
- SMTP
- IMAP - can leave on server
- Replaying - Often left enabled - SPAM redirection
- Fax - use an encryptor

Contingency

- Disk shadowing
- Redundant servers
- RAID, MAIT, RAIT
- Clustering
- Backups
- Dual backbones
- Direct Access Storage Device
- Redundant power
- Mesh network topology - not star

Controls

- Administrative
  - Separation of duties
  - Job rotation
  - Least privilege
  - Mandatory vacations
- Technical /Logic
  - Limit boot sequent
  - Harden Remote Access
- Physical - System Hardening

Change Control Process

1. Request for a change to take place
2. Approval of the change
3. Documentation of the change
4. Tested and presented
5. Implementation
6. Report change to management

Change Control Documentation

- New computers or applications installed
- Different configurations implemented
- New technologies integrated
- etc.

Media Controls

- Purging
- Zeroization
- Data remanence
- Degaussing generates a coercive magnetic force
- Physical destruction
- Care with object reuse

Failure Modes and Effect Analysis - FMEA

- Block diagram of system or control
- Consider what happens if each block fails
- Tabulate failures and effects
- Correct the design
- Have engineers review