8 Feb 2020

08 February 2020 10:38

Network Security

Mitigation strategies:

- Application Whitelisting
- Patch Application
- Patch OS
- Restrict Admin Privileges

Network devices

Firewall
NIDS/ NIPS
VPN
Crypto capable routers

Need for security

- Protect vital records while still allowing access to those who need it
  - IP, Sensitive data, medical records etc.
- Provide auth and access control
- Availability of resources
  - 5 9s

Attacks vs Layers:

Exploit (Application Layer)
Phishing (Presentation)
Hijacking (Transport)
Recon (Transport)
Man in the middle (Network)
Spoofing (Data link)
Sniffing (Physical)

Practices

- Install min OS Configs
- Install patches fixed
- Install most secure and UpToDate version of software
- Remove all privileges and access rights, then grant back access on a "as needed " basis
- Enable as much system logging as possible

System and Network security practices

- Prepare
  - Assume there are vulnerabilities that are not yet recognized
  - Admin needs to recognize when these vulnerabilities are being exposed
  - Hardening solves known issues, prep solves unknown issues

System Security:

- Identify services that will be provided
  - Services to be dedicated to a single purpose
- Identify network service software to be installed
  - Services bundled with OS might not be most appropriate
- Identify Users
- Determine user Privileges
- Plan authentication
- Determine access enforcement measures
- Develop intrusion detection strategies
- Document backup and recovery procedure
- Determine how network services will be maintained/restored after various kinds of failures
- Identify security concerns related to day to dday operations/administration
- Keep computer deployment plan current