Breadth of Network Vulnerabilities

- Limit and Control Access to Network Elements, Services, and Applications.
- Techniques Include: ACL, Firewall, IDS, Password, Security Token, RBAC.

Access Management

Authentication

- Ensure Proof of Identity of the Claimed Entity (Person, Device, Application).
- Techniques Include: Shared Secret, PKI, Digital Signature, Digital Certificate.

- Prevent the Denial of an Activity on the Network or Transmission Through a Network.
- Techniques Include: System Logs, Digital Signatures, Asymmetrical Encryption.

Non-repudiation

Data Confidentiality

- Ensure the Confidentiality of Data to Prevent Unauthorized Viewing.
- Techniques Include: Encryption.

- Ensure Information Only Flows from the Source to the Destination.
- Techniques Include: VPN, MPLS, L2TP, Source Path Routing.

Communication Security

Integrity

- Ensure that Data is Received as Sent or Retrieved as Stored.
- Techniques Include: MD5, Digital Signature, Anti-Virus Software.

- Ensure network elements, services and application are available to legitimate users.
- Techniques Include: Reliable network design, IDS, network redundancy, and disaster recovery.

Availability

Privacy

- Ensure that Data is Received as Sent or Retrieved as Stored.
- Techniques Include: MD5, Digital Signature, Anti-Virus Software.

www.bestitdocuments.com