Lecture notes for 7.5-7.6 Network Security 2

Defense in depth
- Layers of defenses, not just single defense
- Firewall at perimeter
- NIDS at perimeter
- Internal NIDS
- HIDS, AV
- Proactive: Vulnerability scanners

Intrusion detection systems (IDS)
- Monitor “events”, decide if attack is occurring
- Events: network packets, user activity, system activity, filesystem changes, configuration changes
- Signature based
  - Database of attack events, search for matches
- Anomaly based
  - Database of normal events, search for deviation
- Network based
  - Standalone device monitoring traffic passing through network
- Host based
  - Runs on single machine to protect that machine

Intrusion prevention systems (IPS)
- IDS + response
- Responses: increase logging, terminate connection, alert human
- Difficulty: false alarms have very high cost

Vulnerability scanners
- Search for known vulnerable software / configurations
- Nessus, ISS Scanner

Security for email
- Requirements
  - Message confidentiality: Message not exposed en route
  - Message integrity: Message not modified en route
  - Sender authenticity: Receiver has confidence in identity of sender
  - Nonrepudiation: Sender cannot deny having sent message
- Protocols
  - PGP (encryption, digesting, & signing / uses ring of trust)
  - S/MIME (similar to PGP / uses certificates)