Detection Methods

Objectives

- Discuss methods of detection
- Differentiate between the different kinds of detection and mitigation methods

Detection Methods

- Signature Based
- Heuristic Based
- Others

Signature Based

- Signatures are developed for all kinds of detection
  - Intrusion detection
  - Intrusion prevention
  - Antivirus/Antimalware
  - Traffic patterns
  - Application
- Signatures are developed to detect characteristics of certain kinds of content
  - Byte patterns
  - File types
  - Port
  - Protocols
  - Hashes

Signature Based Detection - Advantages

- Updates deployed regularly – sometimes even multiple updates per day
- Signatures can usually be written for IDS/IPS/Applications
- Can often point to a family of malicious content
- Not many false positives

Signature Based Detection - Disadvantages

- Can be evaded
- Zero day threats may not have signatures – False Negatives
- Deployment of updates may be slow
- The more you check for, the more data you have to match

Heuristics Based

- Looks at what the content is doing
    - File changes
    - Network traffic
- Can look at the same characteristics as signature based
    - Byte patterns
    - File types
    - Port
    - Protocols

Heuristics Based - Advantages

- Usually faster scanning since all signatures are not looked at
- Looks only at behavior
- Evasion can be more difficult since malware can follow patterns
- May not actually scan the file to evade

Heuristics Based - Disadvantages

- Usually produces generic information, not detail
- Evasion can still be performed
- False positives may go up
- False negatives might also go up

Other detection methods

- Anomaly detection
  - Historical traffic patterns
  - Statistical patterns for accessing information
- Machine Learning