Wrapping up Intrusion Detection

Video - How do Intrusion Detection Systems work?

Firewall
- Looks at packet headers
  - Source IP
  - Dest IP
  - Port #

Firewalls can't detect payloads
IPS examine payloads.

Network-based Detection
- Examining Packet-by-Packet
  - Can look at either header or its contents
We can look at packets as they come in - active viewing
  - Problem is overloading
We can make copies of packets that we inspect - passive viewing

Zones where IDS can be
Between internal and external firewalls, can't see filtered packets or internal attacks

Distributed System
- A combination of Host Based and Network Based.

Anomaly based
  - Behavior
Signature based
  - Source based
Systems compare what they are seeing.

If one system is attacked, the other systems on network know.

Slides

NIDS - Network Intrusion Detection
- Watches traffic at network ports - Ports below 1024 are reserved
- Examines traffic packet-by-packet close to real-time
- Analyzes traffic patterns
- May examine network transport, and/or application level protocol activity

Passive NIDS Sensors
- Create copies of packets to examine

Intrusion Detection Techniques
- Attacks suitable for signature detection
  - App layer reconnaissance & attacks
  - Transport layer reconnaissance & attacks

Stateful Protocol Analyses
- Subsets of anomaly detection that compares observed network traffic to expected patterns

Logging of Alerts
- Timestamp
- Connection or session ID
- Event or alert type
- etc.
Honeypots

- Decoy System
  - Lures attackers to find information
  - Systems are filled with fabricated information that a legitimate user of a system wouldn't access
  - Resources that have no production value.

- Low Interaction Hp

- High Interaction Hp

![Diagram of network zones for honeypots]

Zones for Honeypots

Snort
- Open source IPS-IDS
- Rule-based Architecture