Intrusion Detection

Objectives

- Understand what intrusion detection systems do
- Categorize different systems based off what they do

What is intrusion detection?

- Detecting actions and events that attempt to compromise confidentiality, integrity, or availability of assets and resources
- Can be:
  - Network Based
  - Host Based
  - Physically Based

They’re always watching…

- Intrusion detection systems are designed to monitor and alert - Passive
- Can be real time or out-of-band
- They require good input to produce good output
- Understand what to look for
- Typically signature based
- Anomaly based systems can catch oddities in transactions
  - Lancope

Network Based

- Intrusion detection systems can be hardware or software
- Can be built into bastion hosts as application level or multilayer firewalls
- Typically built for organizations that may not be able to purchase dedicated hardware
- Monitoring must be performed by
  - Inline
  - Span port
  - Tap
- Most common software is SNORT

Host Based

- Host based intrusion detection or HIDS is designed to look at the entirety of a system
- Monitors many aspects of a system
- Lives as an application
- Software can monitor
  - Security events
  - Normal communications
  - System behavior
- Software
  - OSSEC
  - Tripwire
  - AIDE

Physically Based

- This one is simple
- Security guards
- The department store gate
- Security cameras
- Alarms
- All are designed to monitor and alert
- Can be used as deterrents