Intrusion Prevention

Objectives

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

What is intrusion prevention?

- Detecting actions and events that attempt to compromise confidentiality, integrity, or availability of assets and resources and then take action based on the signatures
- Can be:
  - Network Based
  - Host Based
  - Physically Based

They’re always watching and protecting…

- Intrusion prevention systems are designed to monitor, alert, and be the gatekeeper for systems - Active
- Understand what to look for
- Typically signature based, heuristics
- Must be real-time, inline
- Can be trickier to set up due to traffic flow
- If system fails, traffic stops flowing

Network Based

- Intrusion prevention systems can be hardware or software
- Can be built into bastion hosts as application level or multilayer firewalls
- Organizations that have intrusion prevention often have large networks
- Prevention must be inline to be most effective
- Other software can send TCP resets out-of-band, but not common
- Mostly performed by hardware

Host Based

- Host based intrusion prevention or HIPS is designed to look at the entirety of a system
- Monitors many aspects of a system
- Lives as an application
- Software can monitor nearly every aspect of the system
- Software can be sandboxed or virtualized as not to infect host system

Physically Based

- Anything that physically stops someone from doing harm
- Electric fence is a good example – probably not practical though