**IDS and IPS**

**Intrusion Detection System**

* Used to identify possible attacks or intrusions
* Uses a rule/signature based or heuristic based approach
* Will notify admin when security concerns occur
  + Doesn’t attack the concern like an AV

**Two types:**

Host-Based

* Reside on workstations and servers
* These help detect issues and attackers on system itself
* Can look into memory, file system, network connections etc.
  + E.g., Carbon Black

Network-Based

* Normally resides on a tap somewhere on the network
  + A physical device popped into a physical medium
  + Duplicates signal going across medium
    - Allows you to inspect that traffic
  + E.g., Bro IDS

**Intrusion Prevention System**

* Uses a rule/signature based or heuristic based approach
* Used to identify possible attacks or intrusions
* Doesn’t alert admin but can actively block the connection
* Has to sit on the wire itself, cannot just sit on a tap

**Two types:**

Host-Based

* Reside on workstations or servers
* Help detect issues and attackers on system
* Can look into memory, fs, network connections
* Actively blocks attacks as seen
* Not common due to use of Avs

Network-Based

* Resides physically on the network, in front or behind the firewall
* If misconfigured, the whole network could be brought down
  + If it detects genuine traffic for malicious traffic
* Device needs to be tuned correctly, enough bandwidth, enough power etc. to analyse all the traffic