Honey pot – A system that is left deliberately unsecure / unprotected to encourage attacks on it. Attacks can then be analyzed to protect the real system.

Firewalls open packets and look at:

1. Source
2. Destination
3. Port

They then check these against a list of rules and determine if the packet can continue on to the internal network.

Because Firewalls don’t check the contents of the packets (they only check the headers), Intrusion prevention systems / Intrusion detection systems are needed. These systems examine the payloads of packets.

Network based detection systems:

- Can uses sensors to look at packets.
  - Packet header can help you find higher level threats
  - Opening the packet’s contents will help you find other, more specific malicious attacks.
  - Can actively look at packets, or passively look at packets:
    - Passively – we make copies and look at them later
    - Actively – look at them as receive them. May overload the router.
  - Sensors can look at packets:
    - Inside the external firewall – In the DMZ
      - Advantage, some packets have already been filtered by the firewall
    - Outside the external firewall
      - Advantage, will see all attacks
      - Disadvantage has too look at everything.
    - Behind the internal firewall
      - Advantage: Can help with internal attacks (that were not filtered by the internal firewall).
- Host based protection / detection systems need to be able to talk to the network based detection systems – called Gossip.

Ports: Basically just mailboxes, address that goes on a mailbox. Ports are usually associated with specific protocols. Ports below 1024 are usually reserved for specific applications. This can be a threat because they are well advertised ports (that are generally open).

Port Scanners: Send messages to all ports and looks to see who responds. Allows the attacker to find open ports to launch attacks at.
**Stateful protocol Analysis:** Subset of anomaly detection that is tracking the network and application states. They then checks for unusual activity.

**Logging of Alerts:** Check time stamps to try and determine if you are under attack – by DoS for example.

**PEP:** Policy enforcement point

**DDI:** Distributed detection and inference.

**Honeypots:** Attack me, to lure attackers away from other systems and to understand attacks coming at the system. Want to encourage attacker to stay on it.

- Low interaction honeypot: Usually just a software package that emulates IT services. Less realistic target
- High interaction: Actual operating system / system.
- If a honeypot is inside the internal firewall, then we need to make sure you can’t get privileges escalated.

**Snort:** Open source IPS / IDS that is commonly used. It is a rule based system.