Honeypots

Margaret Asami

What are honeypots ?

- an intrusion detection mechanism
- entices intruders to attack and eventually take over the system, while their moves are being monitored without them knowing
- 2 types:
  - production
  - research

How do honeypots address security ?

- prevention
  - can’t prevent bad guys !
- detection
  - leverages traditional IDS - no false positives nor false negatives
- reaction
  - provides incident response team un-polluted data & stoppable system