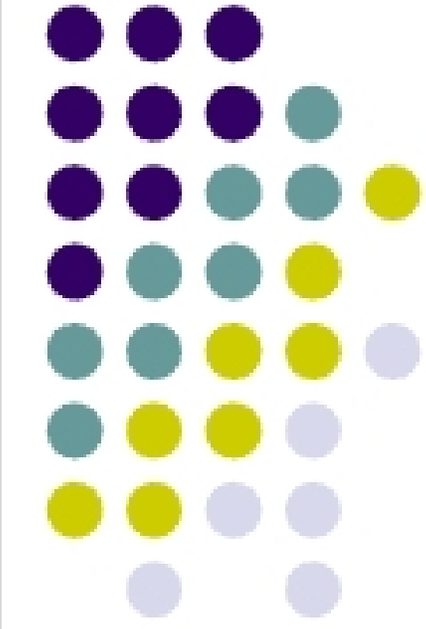
CSCI 530 Lab

Packet Sniffing



Scenarios

- You are a network administrator. You suspect that some of the employees are not working and instead spending all their time at www.espn.com
  - Could filter at the firewall for this address
  - But you want to see what sites they are accessing, without their knowledge
- You are a hacker. You have compromised a system. You are unable to gain access to other systems on the network. You want to get some usernames and passwords to access these systems.

Solution – Packet Sniffer

- Packet Sniffer
  - A tool that captures, interprets, and stores network packets for analysis
  - Works at the Transport layer of the OSI 7 layer model (Layer 4), but some can work at Network Layer (Layer 3)
    - Normal network traffic is based on the destination IP address
    - Your network card will throw away any packets that are not intended for that card
    - In “Promiscuous Mode”, your network card will take all the packets on the network, regardless of the destination IP address.