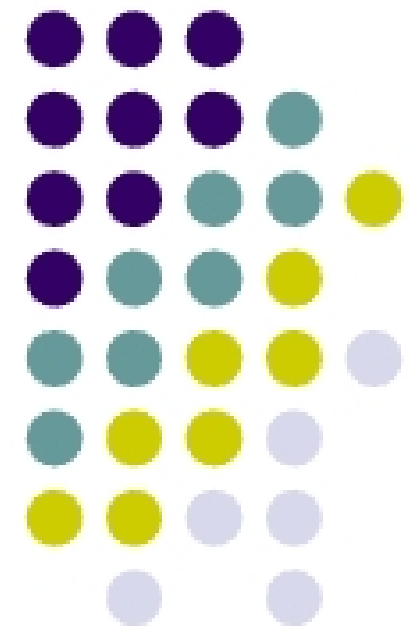
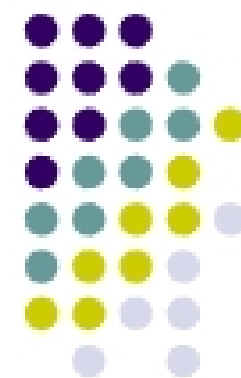


CSCI 530L

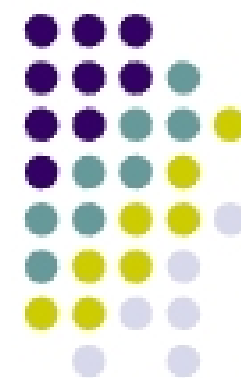
Vulnerability Assessment





Vulnerability Assessment

- Process of identifying vulnerabilities that exist in a computer system
- Has many similarities to risk assessment
- Four main steps
 - Cataloging assets and capabilities (resources) in a system
 - Assigning quantifiable value and importance to the resources
 - Identifying the vulnerabilities or potential threats to each resource
 - Mitigating or eliminating the most serious vulnerabilities for the most valuable resources



Penetration Testing

- Method of evaluating the security of a system by simulating a hacker attack
 - Penetration Test and Vulnerability Assessment are different
 - In a vulnerability assessment, we identify the weaknesses, but do not exploit them
- Tools for a penetration test
 - Metasploit
 - Exploit Tree