Software Penetration Testing

Laurie Williams
williams@csc.ncsu.edu

What is penetration testing?

• A penetration test is a method of evaluating the security of a computer system or network by simulating an attack from a malicious source
• In “real” production environment; directed at operational and configuration issues
• Currently the most commonly-applied mechanism used to “inject” security
Penetration testing’s all black …


Software Security Touchpoints

Security Testing: Testing for What It’s NOT supposed to do

Who does penetration testing

- Can be hired “reformed hackers” or other skill security consultants/analst
- Or internal security testers
- Best if not “regular testers”
  - Due to lack of security knowledge prevalent today
Approaches to Penetration Testing

- Based upon findings from requirements analysis, architectural analysis, and so on.
  - Problems tend to cluster and to not be 100% removed
- Tied to perceived risk
  - Metrics can be used for prioritization
- Include fuzzing: use of a tool to submit malformed, malicious, and random data to a system’s entry points in an attempt to uncover faults
- Based upon knowledge of common vulnerabilities