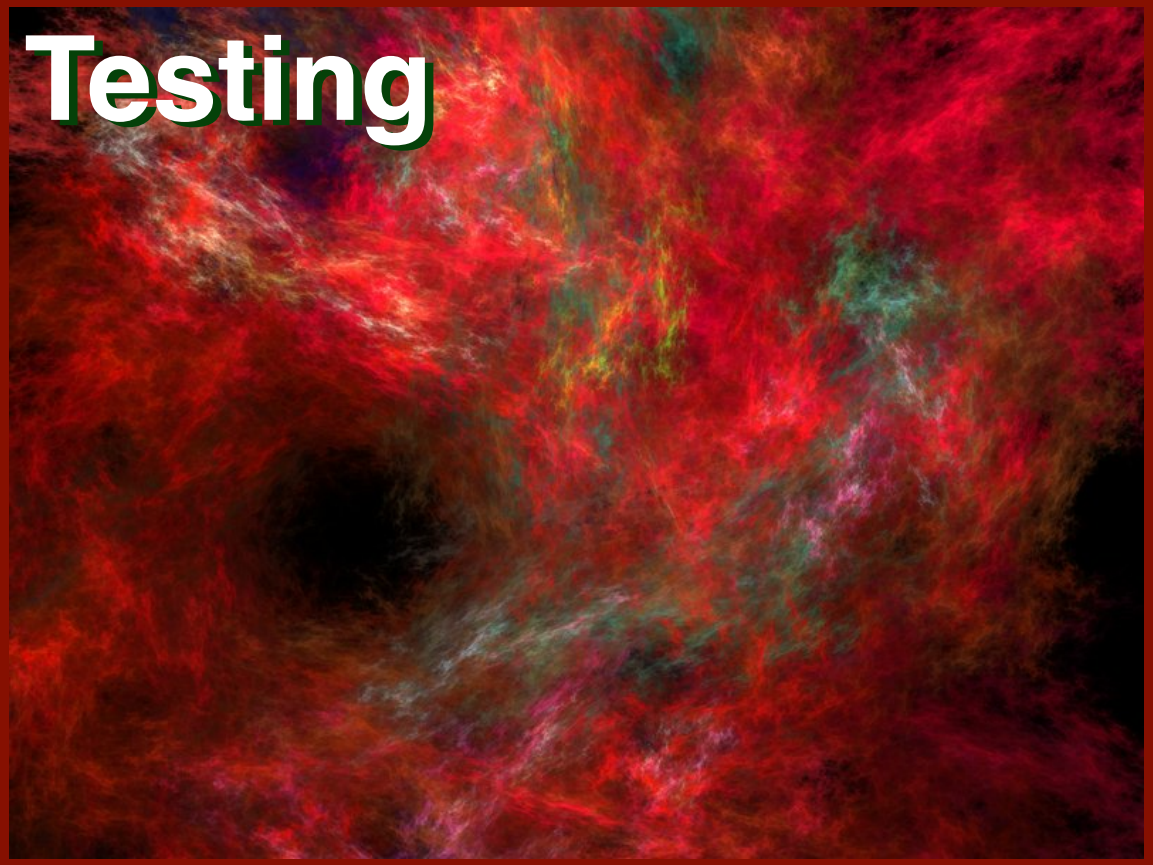
Penetration Testing



What is it?

- **Penetration testing** assesses security by actively trying to **find exploitable vulnerabilities**
  - **Black hat** activity (for a good purpose). Practitioners variously called **red teams**, **tiger teams**, etc.
- Can be applied at different **levels of granularity**
  - **program** (single process)
  - **complete application** (communicating processes)
  - **network** of many applications
  - generally *not* libraries or incomplete pieces of code

Who, and how

- Pen testers employ **ingenuity** and **automated tools**
  - To rapidly explore a system's *attack surface*, looking for weaknesses to exploit
- Typically **carried out by a separate group** within, or outside, an organization, separate from developers
  - *Avoids tunnel vision*: Same reason doctors tend to not treat themselves or their own families
- Given **varied access to system internals**
  - From *no access*, like outside attacker, to *full access*, like a knowledgable insider

History

- **1967** Ware Report
  - Task force of experts headed by Willis Ware of RAND Corp. formally assessed the security problem for time-sharing computer systems. Used term "**penetration**"
    - http://www.rand.org/pubs/reports/R609-1/index2.html
- **1970s**: DOD penetration testing teams emerge to assess "real" security of government computer systems
- **Today**: Penetration testing is expanding
  - Popular with students, e.g., "CTF" competitions
  - Many companies can be contracted to do it
  - IACRB Certified Penetration Tester (CPT)
    - http://www.iacertification.org/cpt_certified_penetration_tester.html

Benefits

- **Penetrations** are **certain** and **reproducible**, demonstrated by tests
  - **Not hypothetical**
  - **Applied** to a **whole component**
    - not (code) fragments
  - **No false alarms**

> Beware of bugs in the above code; I have only proved it correct, not tried it
> *—Donald Knuth, 1977*

- **"Feel good" factor**
  - Produces **evidence of real vulnerabilities** that would otherwise have gone unfixed
  - Thus results in a **clear improvement to security**

Drawbacks

- **Absence** of **penetrations** is ***not*** **evidence of security**
  - After fixing any issues there may be others still lurking
- **Changes to the system necessitate a retest**
  - *Security is not compositional*: a change to one component may render another component insecure
    - So must retest the entire system
  - But changes are common!
    - Can be expensive to retest too frequently
- Nevertheless, **penetration testing worth doing**

This unit

- **Overview** and **tools**
  - Pen testing is ***art*** and ***science***
  - Science is captured in **tools**. We'll briefly consider
    - **Nmap** for network scanning
    - **Zap** web proxy for probing, exploitation
    - **Metasploit** for general-purpose exploitation
    - … and provide pointers to more tools
- Useful technique: **Fuzzing**
  - Find improperly handled inputs
    - where failure implies good chance for exploitation