Advanced Unix System Administration

Lecture 17
April 21, 2008

Steven Luo
<sluo+decal@OCF.Berkeley.EDU>

Types of Attacks

- Some remarks on PHP webapps
  - register_globals is dangerous!
    - Convenient, but discourages input validation
    - With register_globals on, an attacker can set arbitrary variables in your environment!
    - Gone in PHP 5, but many PHP apps depend on (even worse) register_globals emulation
  - PHP allows remote file includes
    - Combined with the above, makes some very dangerous exploits very easy
  - magic_quotes not so magic

Types of Attacks

- Attacks that aren't so technically clever
  - Brute force
    - Particularly relevant for authentication systems
    - You can mitigate the problem sometimes, but can't make it go away
    - Always design the system with such attacks in mind!
  - Social engineering
    - Humans can be easier to exploit than computers
    - User education is only part of the solution – limit what your users can do

Securing Against Local Attack

- Determine what your system and your users need to do first!
- Users and groups
  - Do users really need to be on the system?
  - Enforce strong password requirements
  - Use groups judiciously to grant access by role
  - Restrict access to the root account
- Filesystem permissions
  - Nothing should be world-writable without very good reason

Securing Against Local Attack

- Filesystem permissions con't
  - Directories should never be world-writable without the sticky bit set
  - Group ownership and ACLs are useful tools
  - Split up your disks into separate filesystems, use attributes like nodev, nosuid, noexec where appropriate
- Setuid and setgid binaries
  - Can be great for security (reduce use of root) or dangerous (when exploited or excessively used)

Securing Against Local Attack

- Setuid and setgid binaries con't
  - Look at every setuid and setgid binary, understand what it does
  - Limit setuid/gid binaries to those that you need, no more
- Resource limiting
  - Setting resource limits prevents fork bomb attacks and other resource exhaustion attacks
  - Occasionally also prevents more severe attacks