Securing Your System
CS 236
On-Line MS Program
Networks and Systems Security
Peter Reiher

Putting It All Together

- We've talked a lot about security principles
- And about security problems
- And about security mechanisms
- And about bad things that have really happened
- How do you put it all together to secure your system?

Things That Don't Work

- Just installing your machines and software and hoping for the best
- Simply buying a virus protection program and a firewall
- Running US government FISMA compliance procedures
  - Or any other paperwork-based method

So What Will Work?

- One promising approach is outlined by SANS Institute
- Based on experiences of highly qualified security administrators
- The 20 Critical Security Controls
  - A checklist of things to watch for and actions to take
  - Technical, not policy or physical

The 20 Critical Security Controls

- Developed primarily by US government experts
- Put into use in a few government agencies
  - With 94% reduction in one measurement of security risk
- Rolling out to other government agencies
- But nothing in them is specific to US government
- Prioritized list

Nature of Controls

- General things to be careful about
  - Not specific bug fixes
- With more detailed advice on how to deal with each
  - Including easy things to do
  - And more advanced things if schedule/budget permits
- Mostly ongoing, not one-time

How The SANS List Is Organized

- For each control,
  - Why it's important
  - Quick win
  - Visibility/attribution
  - Configuration/Hygiene
  - Advanced
- With a little text on each
- Not all categories for all controls

1. Inventory of Devices on Your System

- Why is this important:
  - If you don't know what you have, how can you protect it?
  - Attackers look for everything in your environment
  - Any device you ignore can be a point of entry
  - New devices, experimental devices, "temporary" devices are often problems
  - Users often attach unauthorized devices

Quick Win

- Install automated tools that look for devices on your network
- Active tools
  - Try to probe all your devices to see who's there
- Passive tools
  - Analyze network traffic to find undiscovered devices

2. Inventory of Software on Your System

- Why it's important:
  - Most attacks come through software installed on your system
  - Understanding what's there is critical to protecting it
  - Important for removing unnecessary programs, patching, etc.

Quick Win

- Create a list of approved software for your systems
- Determine what you need/want to have running
- May be different for different classes of machines in your environment
  - Servers, clients, mobile machines, etc.

3. Secure Configurations for Hardware and Software

- Why it's important:
  - Most HW/SW default installations are highly insecure
  - So if you use that installation, you're in trouble the moment you add stuff
  - Also an issue with keeping configurations up to date

Quick Wins

- Create standard secure image/configuration for anything you use
- If possible, base it on configuration known to be good
  - E.g., those released by NIST, NSA, etc.
- Validate these images periodically
- Securely store the images
- Run up-to-date versions of SW

4. Continuous Vulnerability Assessment and Remediation

- Why it's important:
  - Modern attackers make use of newly discovered vulnerabilities quickly
  - So you need to scan for such vulnerabilities as soon as possible
  - And close them down when you find them

Quick Wins

- Run a vulnerability scanning tool against your systems
  - At least weekly, daily is better
- Fix all flaws found in 48 hours or less
- Examine event logs to find attacks based on new vulnerabilities
  - Also to verify you scanned for them

5. Malware Defenses

- Why it's important:
  - Malware on your system can do arbitrary harm
  - Malware is becoming more sophisticated, widespread, and dangerous

Quick Wins

- Run malware detection tools on everything and report results to central location
- Ensure signature-based tools get updates at least daily
- Don’t allow autorun from flash drives, CD/DVD drives, etc.
- Automatically scan removable media on insertion
- Scan all email attachments before putting them in user mailboxes