Session Nine: Standard Security Practices

Keeping the System under Your Control...

Critical Security-Related Tasks...

- Follow Internet Bulletins!
- Keep up-to-date on packages (RPMs)
- Running minimal services
- Remote access: encryption vs. plaintext

Critical Security-Related Tasks...

- Being Familiar with your system
- Managing secure passwords
- Verifying package integrity
- Social engineering - *security is more than just the box!!*

Keeping Up-To-Date

- Internet Advisories and Bulletins:
  - CERT (www.cert.org) and mailing list.
  - PacketStorm (packetstorm.securify.com)
- Keeping up on Package RPMs:
  - RedHat (updates.redhat.com) ftp server (and mirrors as listed at www.redhat.com/mirrors.html)
  - RedHat's Website (support section)
  - **rpm -q packagename** gets the package version
  - **rpm -U packagename.rpm** installs an upgraded RPM

Running Minimal Services...

- If You Don't Need It Don't Run It!
- See /etc/inetd.conf for inet-related services
- Binding services to specific interfaces
  - Most servers (Samba, Apache, etc) permit this
  - On a masquerading firewall, the service is NOT VISIBLE from the internet even if you aren't running ipchains, etc.!!!

Remote Access Considerations...

- Telnet, ftp, rlogin, etc., send passwords in "plaintext" across the Internet.
- SSH encrypts the data and the passwords
- Remember your modems!
- SSH for internal purposes as well...
- Switches vs. Hubs...

Know What's Running...

- Use **ps** regularly to view running processes
- Use the /proc directory for more information
- Use **netstat** with the **-p** option
- Watching the logfiles...
  - /var/log/messages
  - /var/log/secure

Good Password Security...

- Don't use a word, your name, your spouse's name, your username, your pet's name, etc.
- Complex/unusual acronyms are good
  - Unusual Bible verse or phrase
  - Use "4", "2", and "1" in place of corresponding words at times.
  - Use mixed case if possible
- Change passwords regularly...
- Don't re-use your password for a website!!!

Verifying Package Integrity...

- Using **rpm -V** on critical packages.
- Using cryptographic tools such as **tripwire**.

Social Engineering...

- Never give out passwords over the phone, especially if *they called you!!!*
- Don't give a password to someone over email, no matter who he/she claims to be.
- Consider screening your volunteers.
- Be on the lookout for "trojan horses"
    - Programs downloaded from questionable websites...
    - EMail attachments are also a problem...
    - Verify RPM cryptographic signatures with GnuPG...