Best Practices for Linux Security

Added by Matthew Miller, last edited by Matthew Miller on May 27, 2010

Best Practices for Linux Security

IRCS Workshop

Matthew Miller

Show Show Hide inline

Where I'm Going with This

1. Handling Confidential Information
2. Interacting with SEAS Servers
3. Keeping Your Own System Secure
4. Questions!

1 / 23

Handling Confidential Information

Informal Guide and FAQ

http://www.security.seas.harvard.edu/hciatseas.php

(But you just have to remember the http://www.security.seas.harvard.edu/ part.)

2 / 23

Definitions

HRCI (High Risk Confidential Information): In short: Legal Consequences

Harvard Confidential: Blanket term for everything else.

3 / 23

The Don't-Do-Its

- No HIPPA data – we can't handle medical records.
- HRCI
  - Not on your desktop
  - Not on your laptop
  - Not in your home directory
  - Not in your group directory

4 / 23

So, what, then?

- Custom solution for each instance of HRCI.
- What about Harvard Confidential?

5 / 23

Interacting with SEAS Servers

With some general advice as well.

6 / 23

Clear text vs. Encrypted

- login/shell
- file transfer
- remote desktop
- e-mail access

7 / 23

Authentication

- Passwords are bad.
- SSH keys are better, with caveats.
- Kerberos is better too, with different caveats.
- Hardware tokens (combining high security with high inconvenience)

8 / 23

Logging into SEAS systems

- SSH or Kerberos, please.

9 / 23

No shared accounts!

There's better ways. Please ask!

10 / 23

Storing data centrally

NFS is convenient and fast....

11 / 23

Keeping Your Own System Secure

Servers, desktops, laptops.

12 / 23

Servers and Shared Services

Best option: make it our problem. (**That's what IRCS is here for.**)

13 / 23

Failing that...

- Minimize exposure
- Keep it simple (and separated)
- Use SE Linux and similar technology
- Advice for workstations applies here too

14 / 23

Workstations

There's basically two points:

- minimize
- patch

15 / 23

Distribution

Use a supported distribution!

- Ubuntu 8.04: EOL April 30th, 2010
- Fedora 11: EOL June 18th, 2010

Enterprise/LTS vs. Bleeding Edge

- RHEL 6 / CentOS 6
- Ubuntu 10.04 LTS

16 / 23

Updates

Balancing risks: updates breaking, vs. attackers.

On Fedora/CentOS/RHEL:

- yum-updatesd
- yum-cron

On Ubuntu:

Handy check box!

17 / 23

If you don't need it, don't have it

- don't run it
- don't even have installed
- block access with iptables

18 / 23

So, yeah, SELinux

...

19 / 23

Physical Security

- bootloader
- root password
- screensaver
- hardware – encryption is the answer here

20 / 23

Encryption

- Laptops: must be done.
- Desktops: good idea, *less* inconvenient.
- On central storage: perhaps.

21 / 23

If there's a problem

1. **STOP! Don't touch it**
2. Don't even unplug!
3. Contact security@seas.harvard.edu

- if there's HRCI...
- After: nuke it from orbit (so, keep it disposable)

22 / 23

Questions?

Questions!

23 / 23