Security

Risk Assessment

Determine how important your computer is to your group

• Mission critical?

• Sensitive information?

• Expensive hardware?

• Service easily replaced in 24 hours?

• How many users depend on it?
Security

Physical Security
Security

Physical Security

Should it be locked down?

Does it need to be in a protected room?

Should the case be locked?

Are there any removable devices?

Do you leave your office door open?
Security

Physical Security

Story: Christmas Holiday in Britain
Security

BIOS

Your BIOS determines from which device your computer boots

The order of which device from which to boot can be set in most BIOSes
Security

BIOS

Reformatting your drive is only a CD or floppy away

Most CD drives are bootable and several distributions can now exist on a CD

So, what is stopping someone from inserting a disk in your computer, booting from it, and starting an attack?

BIOS PASSWORD
Security

Booting

Now you've blocked access to the devices and the BIOS. So you are safe...

WRONG!

Anyone can still access your system – as ROOT!

How do they do this?!?!?
Security

Booting

Simple:

When grub starts, just edit the configuration file and add the word “single” at the end of the kernel line and boot

The system will boot into single user mode and now your are root!
Exercise: Single User Mode

At GRUB screen, select kernel

Type “e” to edit

Select line with word “kernel” in it

Type “e” to edit

Add the word “single” at the end

Press ENTER

At GRUB screen type “b”
Security

Booting

How can I prevent this?!?!?!

Add a *boot password* to the grub config file:

(1) Create the encrypted password:

```
/sbin/grub-md5-crypt
```

This will return an password encrypted in an MD5 hash
(2) Edit the grub config file
   /boot/grub/grub.conf and add the
password directive and the password:

   password --md5 <password-hash>

Where <password-hash> is the
encrypted password you were given
from grub-md5-crypt.

The next time you boot, you must use
the p command and enter a password in
order to access the grub environment
Security
Booting
Exercise

# /sbin/grub-md5-crypt
# nano /boot/grub/grub.conf

Add

password --md5 <password-hash>

to the top of the file

Reboot and try to edit the grub config file

Remember to use “p” to get Grub to prompt you for the password
The next layer of security is good passwords.

Simple passwords are easy to crack with packages such as crack and John the Ripper.

Exercise: John the Ripper

```bash
# cd /opt/exercises/Security
# john-1.6/run/john /etc/passwd
# john-1.6/run/john /etc/shadow
```
Security

Passwords

These programs need access to the actual passwords

This is a good reason for using shadow passwords – only root has access
Security

Passwords

Never use a word found in a dictionary as a password. Cracking programs are even smart enough to try changed character classes that still spell words.

Never use your account name as your password.
Security

Passwords

Good passwords should have mixed cases and mixed character sets.

Pick a phrase that is easy to remember and use the first letter of each word:

Iowa State Rules But U of I Sucks
ISR3UoIS

or better yet, with mixed character sets

I$R3UoI$
Security

Root Access

Who “needs” to be root?

As few people as possible

How should root access the computer?

The most secure ways possible with the least chance of intercepting the password

How do we accomplish this?

/etc/securetty
su
sudo
Security

Root Access

/etc/securetty

root should NEVER login remotely

Force root users to access the system via secure terminals:

• Console
• virtual terminals
• serial terminals

Which terminals are allowed is specified in the file /etc/securetty
Security

Root Access

/etc/securetty

console  - actual display
vc/1     - virtual consoles
vc/2...

tty1      - connected terminals
tty2...   (now mostly associated with virtual consoles)

ttyS0     - serial console
ttyS1...
Security

Root Access

su and sudo

If you must, login over a secure connection

Use su to access root

You MUST use a secure connection to avoid password sniffing

A better way is to implement sudo

sudo is a package which permits sets of users to execute commands as root without the root password
Security

Root Access

**sudo**

**sudo** has many possible configuration options.

Modify the **sudo** config file `/etc/sudoers` to control who has access and what they may access.

Access must be done by root with the command **visudo**

See! you DO NEED to learn **vi**

:+D
Security

Root Access

_sudo_

# User privilege specification
root    ALL=(ALL)    ALL
linuxed  ALL=(ALL)    ALL
# Uncomment to allow people in group wheel to run all commands
# %wheel    ALL=(ALL)    ALL

# Same thing without a password
# %wheel    ALL=(ALL)    NOPASSWD: ALL

# Samples
# %users  localhost=/sbin/shutdown -h now


**Security**

**Root Access**

*sudo*

*sudo* is invoked with the *sudo* command and the command to be run

```
sudo <command>
```

The user is then prompted for THEIR password:

```
[linuxed@counter ]$ sudo cat /etc/sudoers
Password:
# sudoers file.
#
# This file MUST be edited with the 'visudo' command as root.
...
```