System Security

Purpose:

1) prevent users from accidentally destroying the system.

2) defeat deliberate attacks on the system.

3) recover damage after an attack or accident.

4) close security holes.

Principle:

Security actions should be appropriate for the goals of your organization.

Passwords

Many systems can be breached by a password attack.
The password file is available to all local users;
it often includes the encrypted passwords.

It is difficult to decrypt the password,
but a guess and check attack often succeeds.
Guess the password and check to see if it encrypts to anything in the password file.

With a modern computer you can sequentially guess every word in the dictionary in a under an hours.

1) Every account, especially root, should have a password.
2) Passwords should not be in the dictionary
3) Passwords should not be information commonly related to you, such as phone number, address, office number birthday.
4) Mix letters, numbers and symbols. Use both upper and lower case.

Several password checkers are available.

Login Control

`/etc/login.defs` – configuration file for logins.

Examples:

`CONSOLE /etc/securetty` – root login, references a file

`CHFN_RESTRICT` – lists what the user can change

`ENV_PATH`, `ENV_SUPATH` – login default

`FAILLOG_ENAB` – login failure reports

`PORTTIME_ENAB` – what hours you can login

`SYSLOG_SU_ENAB`, `SULOG_FILE` – track su's

`SU_WHEEL_ONLY` – yes means you must be in the wheel group (`/etc/group`) to su to root. In some version of Linux there is special wheel group, others use group 0.

Permissions

In addition to the rwx permissions there are permissions to set the user and group ID.

```
-rws--x--x  john student   jpriv
-rw-------  john student   times
```

`jpriv` does a set user id to `john`.
When anyone runs `jpriv` the program has the priviledges of `john` (not of them).

```
# jpriv
date >> times
```

Users cannot access `times`, but when they run `jpriv` the program can access `times` (and it probably cannot write into the user's home directory).

```
chmod 4711 jpriv
```

You can also do a group set id (`chmod 2711`)
You switch to the group to which the file belongs

Reminder: SUID, SGID are for the program only.

Security issue: it is too easy to modify a shell script, so many systems allow only compiled programs to be SUID/SGID.

Security issue: watch for programs that SUID to root. Keep as few around as possible; scan the system for them

occasionally.

Permissions

Make sure confidential information is not world readable.

Protect critical directories.

Be careful when building SUID and SGID programs. They are highly useful, but a badly built one can allow a user to use the granted privileges in a way you don't want.
especially keep track of SUID root programs.

Several permission checkers are available.

Local Access

If a machine allows the operating system to be reloaded by a person at the keyboard. Be careful about treating as a trusted host.

Since you can do this with most machines,
you are only as secure as the lock on your door.

You may want to restrict network address on the basis of the ID of the network card or the possession of an encryption key. The network ID can be faked, and the encryption key has to be "reset" whenever you reload the computer.

Audit

You can track: login/logout, commands issued, each IP access.

Administrators job: evaluate the level of security that is appropriate.
Make sure that level is followed.
Trace break-ins and plug holes.

CERT (Computer Emergency Response Team): issues advisories about security problems.
Get on their mailing list.

Our evaluation:

With a class of first-time student administrators:

1) our most likely source of damage is internal.

2) protecting the system you are assigned to administer against you defeats the purpose of the course.

3) most damage is due to mistakes

4) you probably left a security hole

Actions:

a) Mitigate damage: as root you can't access files on cheetah (protecting the other students files).

b) Split you up, request you keep logs: so I can figure out who is having accidents and get you to stop.

c) Insist on you following instructions.

d) Get you to read the manual entries before you make a mistake.

e) Outside access to the lab must stop at `cheetah` to prevent direct hacking of student machines.