Capture the flag

Group attack list

Please see here for the groups you will attack.

Your machines

Begin by sending me the 2 ip addresses you will use for your machines. I am going to at least firewall them at the border so that we don't actually get hacked by some unknown person.

In this project you will create an instance of a linux machine as well as an instance of a Windows machine (preferably windows xp). On each OS you should enable between 5-10 services that can be seen on the network. Another group will try to compromise your machines and you will try to compromise another groups' machines. Document everything.

The services that you select to run on your OS should be minimally configured (and perhaps even have some glaring holes that the other group can find fairly readily). You should also configure a couple of different users on each OS (some could have dictionary based passwords). Disable firewalls.

You should consider installing a vulnerable web app of some sort (old versions of phpbb are notorious).

Once your machines are set up, you should provide the ip address(es) to the other team.

You have one week to prepare your machines.

Remote machines

The machines of the group that you are to attack: You should try to compromise the systems that have been set up by any method possible (I bet you won't be lucky enough for a social-engineering hack). Document all the attacks that you try and whether or not they were successful. If you sucessfully compromise the system, document what you did also and provide that information to the remote group.

You have one week to attack machines.

Hardening

When/if you receive notification from the other group that they were able to compromise your machine, you should take steps necessary to secure it so that the vulnerability will be gone. Document what you did.

You have 3 days to harden machines.

To pass off

You will present your findings above in class. Please create a slideshow presentation and have the entire group participate.