Final Project

Requirements

group list

Your machines

In this project you will create an instance of a linux machine, a Windows XP machine, and a Windows 7 machine. 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.

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).

Choose one of you machine and install a HIDS on it. Hopefully it will let you know if you have been compromised.

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. - Connecting to their vnc terminal is fair game (will only really work if they haven't logged out). - When you compromise the remote machine you could: * create a backdoor * change the desktop - You should NOT make the system unusable.

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. Security does not consist of simply unplugging the machine from the network!!! Document what you did.

To pass off

- You might document what alerts your HIDS gave you.
- How did you gain access to their machines
- What did you do once you were there
- How did you secure your machines once you were hacked.

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