

## Hands On with Hardening

### Directions

In this exercise, you will have an opportunity to try your hands at hardening. Do these exercises from the command line. Log in with a secure shell session, so you can copy and paste (don't use the VIC console). You should follow along line by line, at the end you'll email me output from some commands so I can see your progress. If you don't follow along pretty closely, you won't get credit.

### Part I. Getting tiger and running it the first time

We're going to make a snapshot of our running machine **BEFORE** we do anything.

Make a snapshot. Go to VIC, select your machine, right click on it, take a snapshot. Name it and give it some meaningful description. If the stuff hits the fan, you can select "revert to snapshot" and the machine will be again as it was when the snapshot was made.

I was going to have you use the venerable Bastille package, but it appears to not be in current development and doesn't easily support RHEL/CentOS 5. That's a shame, I've used it for a long time. One thing cool about bastille was that not only did it report on problems, it could actually try to "fix" them. You could run it on a fresh install, it would harden up the install considerably, and it usually wouldn't break much.

Something similar (but reporting only) is the tiger package at <http://savannah.nongnu.org/projects/tiger/>. This is basically a 'tarball' archive of scripts. The basic set of steps is:

1. Figure out where you want the tiger scripts to live. Maybe make a directory. Cd to the directory.
2. Download the latest tarball 'wget tiger\_download\_url'
3. Extract the tarball 'tar -xvf file\_name'
4. Change the permissions on the extracted content 'chown -R root:root tiger\_dir\_name' on the tiger directory

### Part II. Trying a bit of hardening

Get a tiger report. Go to the tiger directory and './tiger'. It'll run a minute or two and then give you a path to a report.

Basically you have a couple of sets of inputs now. Get the hardening documents from NSA and CIS (CIS requires free registration) mentioned in the lecture. (The easiest one of these to read is the 2 page hardening tips for RHEL 5 from NSA. Each item on this list is explained in great detail in the larger NSA document if you need an immediate reference.) You have the output from the tiger run about your system specifically. Some of the things tiger found were valid, others may not be.

So your job is to apply some of the hardening tips from the documents that also seem to be tiger

complaints, and get tiger to stop complaining (without breaking or rendering your system useless).

It's an iterative process. Find a class of tiger complaint. Find the section in a hardening document that talks about that. See if the hardening suggestions seem easy to do and not likely to break something important. Apply the hardening tip. Re-run tiger. See if the complaint went away. "Fiddle" with your machine some and make sure you didn't break anything. Lather, rinse, repeat.

If you destroy your machine, all is not lost. You made a snapshot. You can "revert to snapshot" and put your machine in a "time machine" and whisk it back to the way it was.

### **Part III. Get some points**

Email me at least 2 tiger reports, the first one before you "fixed" anything, and a later (hopefully shorter) one showing that you "fixed" something. Attach the reports to an email and email it to me with the subject "Hands On with Hardening". **This is due by next class period.**

If you are in a Cal Poly class, email it to me at [glporter@csc.calpoly.edu](mailto:glporter@csc.calpoly.edu).

If you are in a Cuesta class, email it to me at [gregory\\_porter3@cuesta.edu](mailto:gregory_porter3@cuesta.edu).

I need to know who you are to give you credit, so if you email it from a non-campus account, make sure you mention your full name.

### **Part IV. Things to Ponder**

Bastille doesn't like out 64 bit machines and this version of CentOS. Lord knows if someone will ever fix it. That's too bad.

If you are doing this all the time, instead of running semi-lame funky scripts you downloaded from "Joe's Security Site", pay the \$300 and get the CIS tool. It will work. It's a GUI. It will report on compliance with the CIS Benchmark (which you can download for free), which covers a lot more areas than the tiger script does.

The methodology we used here in the lab is the one you'll do in "real life". Maybe you'll use the CIS tool, or something else, but the idea is valid. Find some (automatic) way of figuring out what needs to be fixed, try it, see if it breaks anything, do it again (and again, and again). At some point you can tell the boss your machine(s) are secure.

That's another advantage of the CIS tools. They have credibility with non-technical bosses and customers. Would you rather tell someone "our systems are in full compliance with the CIS Level One Security Benchmark" or "I fiddled with some open source tool I downloaded until it stopped complaining". Hmm.

### **Part V. Clean up**

Snapshots rapidly grow and fill up the disk. If you are done with this lab, then delete all the snapshots you might have made. Use VIC, Snapshot Manager, Delete All.