Project 2 DETER Information

CS 161 - Joseph/Tygar

November 9, 2006

1 Edits

If we need to make clarifications or corrections to this document after distributing it, we will post a new version to the class website and we will announce the new version on the class newsgroup. Please be patient, as this is a brand-new project that we're running for the first time.

11/9: Updated info/recommendation on where to store scripts.

11/8: Fixed URLs (.net, not .edu).

2 DETER Overview

2.1 What is DETER?

DETER is a large-scale network testbed that provides a wide range of options in creating and using computer networks. These networks are not simulated—they are real machines actually connected to each other.

2.2 Using DETER

In order to use DETER, one must have a DETER user account. An account has been created for each CS 161 student group. You can log in to the web interface to create and configure experiments, and once an experiment is running you can ssh to the nodes (machines) in the experiment. You should have received an account name and password from your TA in section (one per group). You can use that username/password to log in to the web interface and to connect via ssh. For ssh, you need to connect to `users.ucb.deterlab.net` and from there to nodes in your experiment (or `users.isi.deterlab.net`; see below). Your home directory will be the same on `users` and on all experiment nodes. You have root access on all experiment nodes via *sudo* (but not on `users`).

Important note: There are two separate front-ends to DETER: `http://www.isi.deterlab.net` and `http://www.ucb.deterlab.net`. For this project, we will use the UCB interface as the primary one and the ISI interface as secondary. (The ISI web address was listed on your slip with username/password, but that was a mistake.) These two front-ends are very similar, but they have different pools of machines behind them. Your home directory on UCB is different from your home directory on ISI.

There may not be quite enough capacity on DETER for all groups to run experiments at the same time. Therefore we have set up a sign-up sheet: `http://arrakis.cs.berkeley.edu/wiki/deter`. Please use this to sign up for priority on the testbed.

Try out DETER early on; we've had to do a lot of setup to get this ready, and there may be bugs. Better to find them earlier rather than later!

3 Experiments on DETER

3.1 Starting an experiment

Log in to `http://www.ucb.deterlab.net`. On the left, click "Begin an experiment". The project should be CS161 and the group should be your group number. Pick a name (8 or fewer lowercase characters is best) and give it a short description. For the NS file, you can either upload the NS file posted on the class webpage or enter the following in the "On Server" field: `/proj/CS161/ns/project2.ns`. (Both NS files are identical.) Leave the rest of the

settings alone and submit. You'll see lots of information scroll slowly by as the experiment starts up; it'll probably take 5-10 minutes.

You have ssh access to your experiment via `users.ucb.deterlab.net`. Once you've ssh'd there, you can identify machines by name.experiment.project. So, for example, if I have started up an experiment called "corp" using this project's NS file, I could ssh in to the first firewall by typing "ssh fw1.corp.cs161". You can use sudo for root access on experiment nodes, though not on users.ucb.deterlab.net. Also, you can upload ssh keys via the web interface, which you can then use to log on via ssh without having to type the account password.

When you are done working on your experiment, please always remember to swap it out or terminate it so the nodes can be returned to the pool of free nodes.

3.2 Filesystems

DETER nodes have several different categories of filesystem mounted. Each node will have its own root filesystem. Each node will also have home directories mounted in /users (for example, group 7's home directory is /users/cs161g7). There is a filesystem global to the CS161 project in /proj/CS161 (which includes all student groups as well as some other accounts associated rather loosely with the class). Each group has a private filesystem at /groups/CS161/gXX (replace XX with your group number). (Note: /groups denotes DETER groups, but for this project there is a separate DETER group for each student group, even though each student group has its own DETER account.)

You should keep your firewall scripts in /groups/CS161/gXX. Please do **NOT** keep scripts or anything else private in your home directory, as that is world-readable. (And even if you change permissions, it may be mounted on experiment nodes where others have root access.)

We recommend using your subversion repository for version control, though unfortunately users.ucb.deterlab.net doesn't currently have subversion installed. (If there is enough demand, we could install it there, though.) So for now at least you will have to copy files by hand between instructional machines and users.ucb.deterlab.net. Once files are there, you can put them /groups/CS161/gXX, where they will be available to fw1 and fw2.

3.3 Land of Make-Believe

While DETER emulates a true network environment much better than other options, it is not perfect. There are a few things we would like to point out.

There is a *control network* that connects every node in your experiment to each other node and to the outside world (see `https://www.ucb.deterlab.net/tutorial/tutorial.php3#ControlNet`). You will need to make sure your network traffic, firewall, and attacks (in Phase II) don't use the control network at all. Also, while the remote machine and each firewall is its own physical computer, the other nodes are all virtualized over fewer nodes. Please ignore this as much as possible and treat them as separate machines.

This admonition applies most to the attacks you will perform in Phase II. You are to attack the network via any means a real attacker would have at their disposal, but you should not take advantage of anything artificial introduced by DETER. This includes the control net, shared filesystems, virtualized resources, etc.

3.4 Tools

The tools `hping3`, `ngrep`, and `nmap` are in `/proj/CS161/toolBinaries`. There may be problems with shared libraries that we are looking into; please let us know whether they work for you.

4 Notes

- There is currently no content in the web server or the database, and the signing server is not fully functional. This is unimportant for Phase I and will be fleshed out as necessary for Phase II.
- When writing your firewall, you should be sure it applies only to the *experimental* network and not to the *control* network. There are a couple ways you could do this. The easiest is probably to put blanket allow rules at the beginning of your firewall script for traffic to/from control net IPs, but you could also try doing it by interface. Maybe you can think of another way too.
- If you have questions, the DETER documentation is a good place to look (the link is on the left on the DETER webpage). Feel free to ask us questions as well. There will undoubtedly be more bugs