

CSc 466/566 Computer Security

Assignment 4

Due 23:59, Nov 18, 2014
Worth 5% (ugrads), 5% (grads)

Christian Collberg
Department of Computer Science, University of Arizona

Copyright © 2014 Christian Collberg

1. Introduction

In this assignment we'll network security, in particular ARP spoofing.

- This is an individual assignment.
- If you have any question, please ask the TA!

2. Setup

1. Login to Deterlab at

`https://www.isi.deterlab.net`

2. Under the “Experimentation” menu at the top of the page, click “Begin an Experiment”.
3. Select the Project name “CSC466566” from the “Select Project” dropdown. Leave the “Group” set to default.
4. In the “Name” field, enter your experiment name “Experiment1 - CSusername”.
5. In the “Your NS File” field, use the network simulator file on server:

`/share/education/LinuxDETERIntro_UCLA/intro.ns`

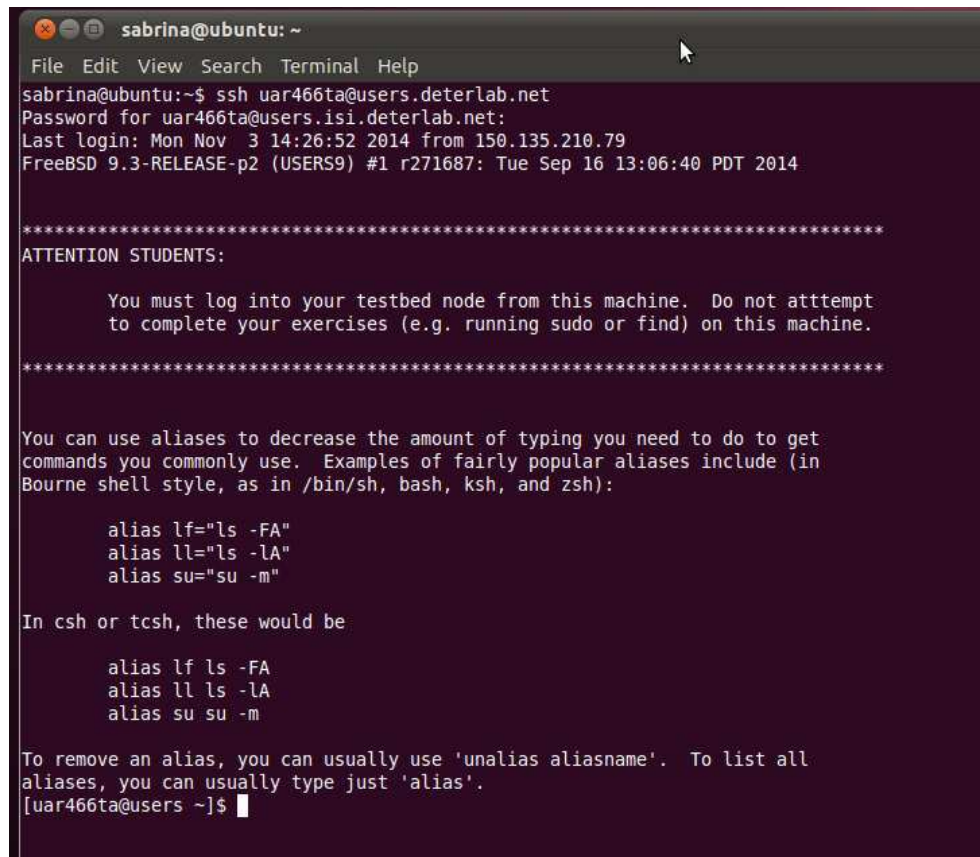
6. Set the “Idle Swap” field to 1 hour.
7. Leave the field “Linktest Option” and “Batch Mode Experiment” to its default values.
8. If you would like to start your experiment now, check the “Swap In Immediately” box.
9. Click “Submit.” Please note that it takes few minutes to get the experiment fully configured. You will get an email message notifying that the system has finished swapping in your experiment.
10. Click on the “My DETERlab” link on the left hand menu. In the “Current Experiments” table, click on the name of the experiment you just created.

3. Accessing experiment node

1. To access your experimental nodes, you'll need to use secure shell (ssh) to connect to

`users.isi.deterlab.net`

using your username and password.



```
sabrina@ubuntu: ~  
File Edit View Search Terminal Help  
sabrina@ubuntu:~$ ssh uar466ta@users.deterlab.net  
Password for uar466ta@users.isi.deterlab.net:  
Last login: Mon Nov  3 14:26:52 2014 from 150.135.210.79  
FreeBSD 9.3-RELEASE-p2 (USERS9) #1 r271687: Tue Sep 16 13:06:40 PDT 2014  
  
*****  
ATTENTION STUDENTS:  
  
    You must log into your testbed node from this machine. Do not attempt  
    to complete your exercises (e.g. running sudo or find) on this machine.  
  
*****  
  
You can use aliases to decrease the amount of typing you need to do to get  
commands you commonly use. Examples of fairly popular aliases include (in  
Bourne shell style, as in /bin/sh, bash, ksh, and zsh):  
  
    alias lf="ls -FA"  
    alias ll="ls -lA"  
    alias su="su -m"  
  
In csh or tcsh, these would be  
  
    alias lf ls -FA  
    alias ll ls -lA  
    alias su su -m  
  
To remove an alias, you can usually use 'unalias aliasname'. To list all  
aliases, you can usually type just 'alias'.  
[uar466ta@users ~]$
```

2. Once you log into

`users.isi.deterlab.net`,

you can `ssh` to the experiment nodes using either the physical NodeIDs or the “Qualified Name” which has the format

`nodename.experimentname.projectname.isi.deterlab.net`.

You get this information from the experiment webpage or in the email you got after your NS file was swapped in.

Experiment (CSC466566/Experiment1)

Experiment Options

- View Activity Logfile
- Swap Experiment Out
- Terminate Experiment
- Modify Experiment
- Make Experiment Risky
- Modify Traffic Shaping
- Modify Settings
- Link Tracing/Monitoring
- Event Viewer
- Update All Nodes
- Reboot All Nodes
- Run LinkTest
- Show History
- Duplicate Experiment

163 Free PCs, 4 reloading

bpc2800010	bpc213360	pc2133n8	bpc300016
pc300017	pc300012	bpc300020	bpc140000
pc213317	MicroCloud13	bvx220018	pc2133x0

Experiment: CSC466566/Experiment1
State: active

Virtual Node Info:

ID	Type	OS	Qualified Name
intro	pc	Ubuntu1204-64-STD	intro.Experiment1.CSC466566.isi.deterlab.net

Physical Node Mapping:

ID	Type	OS	Physical
intro	pc3060	Ubuntu1204-64-STD	pc199

Event Groups:

Group Name	Members
__all_programs	intro_startcmd
__all_program-agents	__intro_program-agent

Event Summary:

Event count:	2
First event:	0.000 seconds
Last event:	0.000 seconds

4. Introductory Exercise

1. You can start working on your first set of tasks on deter and Linux now. Here are the detailed instructions: /50

https://education.deterlab.net/file.php/12/LinuxDETERIntro_UCLA/Exercise.html

2. After you are done with your experiment, make sure to save your work and then to “swap out” the experiment. Do not “terminate” it unless you are sure you will never need it again!

5. ARP Poisoning

1. Now you should be ready to do the ARP assignment! Follow these instructions: /50

https://education.deterlab.net/file.php/12/MITMARF_USC/Exercise.html#tasks.