NCS 490:
Shell Shock Lab

By: Tony Perez

October 8, 2014

1 Abtsract

In this lab we learned about the Bash remote code execution vulnerability. This has been named the ”Shell Shock” vulnerability found within Bash.

2 Introduction

The bug within bash has been found to be able to allow remote code executions through Bash. Bash is used in many Unix environments like Linux and Mac OS X. This is a huge problem because an hacker can gain access to our shell without permission. In most cases Bash is used in the background and so the user would not even know what is happening. Since this need remote access of Bash it might not be easy if they do not allow network connection their shell like through SSH.

3 Shell Shock

To prove that your Bash is vulnerable RedHat has come up with a command to check.

```
env x=’() { :;}; echo vulnerable’ bash −c ‘‘echo this is a test’’
```

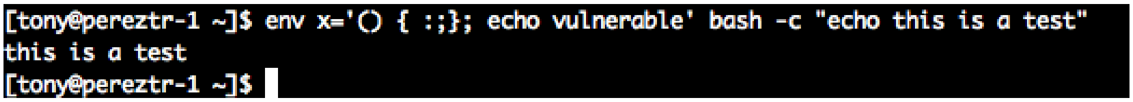
If this commands prints out:

```
vulnerable
this is a test
```

Then it means that your current version of bash has the bug. If it does not print out **vulnerable** and only **this is a test** then you are fine.
If you are vulnberable on CentOS a simple update to your bash would fix it.

```
yum update bash
```

This is how it would appear if you are not vulnerable:



```
[tony@pereztr-1 ~]$ env x='() { :;}; echo vulnerable' bash -c "echo this is a test"
this is a test
[tony@pereztr-1 ~]$ 
```

4 Conclusion

Here we have learned how to protect our systems from the new bug that has been out for a while now and only recently has been discovered.