Computer and Network Security
Laboratory Exercise 9

CS-455 **Winter, 2016**

In this *optional* lab, we will create an ELF virus, following the directions given in Himanshu Arora's article, "ELF Virus, Part I," appearing in the January, 2012 issue of *Linux Journal*.

To perform the lab, open your copy of Arora's article and follow the directions. Install your code on the virtual machine you created last lab.

Notes

1. The virus code is available on Blackboard, slightly modified for your convenience.
   (a) Create a directory named `tmp` in your home directory. This gives the code a place to create a temporary file, and prevents a subtle error I encountered.
   (b) Change all instances of `/home/cater` in the source code to your home directory. Make sure all the paths are correct, changing them in your code as needed.
2. I found the shell script more trouble than not. The basic idea is compile, check the size, correct if necessary and recompile. Then run.
3. Consider running the code as root on the VM, locating the code in `/` or `/usr/bin`. What happens?
4. You can remove a couple of comments from the code and cause it to execute over your home directory. This is probably not wise.
5. After you have finished the lab, please clean up after yourself. The safest thing to do is remove the infected OS from the VM. At a minimum, remove any infected executables you created.
6. You are encouraged to continue to experiment with this code on a machine you control. Perhaps you can write and include some attack code to be included with the infection code.
7. As always, do not run this code or code like it on any Kettering system other than in this lab.

Deliverables

If you wish to obtain credit for this optional lab, submit a text report describing your activities, and submit it to Blackboard by 16 Mar 2016.