Ubuntu Desktop Hardening

Assignment due: 4/8/16

In order to better understand the lecture topics for this week, your assignment is to provide additional security measures to the default Ubuntu Desktop installation. This assignment PDF contains a series of tasks you should perform in order to complete the assignment. An accompanying PDF file will help you carry out the tasks outlined in this document. You may also find it helpful to look back at the links provided for the IDS/IPS assignments.

These tasks can be done on either an Ubuntu 14 LTS or Ubuntu 15 virtual machine.

To get full credit for the assignment, you should:

1. Install ClamAV
2. Update the ClamAV virus definitions using the command *sudo freshclam*
3. Run a full system scan using the command *sudo clamscan –v –r /*
4. Install rkhunter
5. Update rkhunter
6. Search for rootkit infections using rkhunter
7. Install tiger
8. Run tiger to generate a security report
9. Configure Ubuntu for daily automatic backups (save these in ~/my_backups)
10. Configure Ubuntu for daily automatic updates

Submit the following screenshots in a compressed archive for the assignment:

1. Output of the *sudo freshclam* command
2. The SCAN SUMMARY section from the output of *sudo clamscan –v –r /*
3. The output of *sudo ls –l /var/log/tiger*
4. The contents of the “my_backups” folder after performing your first backup
5. Your automatic update settings

While you could do this assignment using an existing virtual machine, I recommend creating a new virtual machine; certain steps, such as the full system scan using ClamAV, may take a lot longer if there’s more files present than just the default installation of the OS.