System Security Group Project #4

(10% of class grade, due 3/21 in class)

Capture the flag without training-wheels. Attempt to get root on a CTF vulnerable virtual machine without documentation. Update your group wiki with steps and screenshots detailing what you did. Give a 5-minute lightening talk about what you did. This project is worth 10% of your class grade.

What you will need:

You will need access to VirtualBox and the following virtual machine images:

- LAMPSec CTF9 - Download it directly from the source at https://sourceforge.net/projects/lampsecurity/files/CaptureTheFlag/CTF9/
- Kali Linux (same from previous project)

Directions:

Download and install the new CTF9 virtual machine using the instructions from the previous project. (Pay attention to make sure you have a host-only network adapter installed and only attack the virtual machine on that host-only network.) Create instruction documentation on your group wiki for the CTF9 virtual machine, and prepare to give a 5-minute talk on 3/9 talking about what you did and what challenges you encountered.

The deliverable

I am expecting **new instruction** documentation on your group wiki area for the CTF9 machine. Create a new page in your group wiki page called "CTF9", and place your documentation (with screenshots) in this area. Specifically, I'm looking for screenshots of each step using Kali as the attacking machine, as well as explanations. Use the documentation you created in your last project as a starting point. If you use other documentation or teams for help, ***you must cite the help*** in your documentation.

You may want to work physically together to brainstorm and work your way through the exploitation.

On the due date, prepare to give a 5-minute talk about 1) what you did, and 2) any challenges you encountered. You can use the documentation you create as a visual aid, or you can just talk without a visual aid. All team members do not have to talk due to the abbreviated time.

In addition, you will be required to fill out a blackboard survey on the distribution of work before you get a grade. (You cannot skip this part.)

Finally, don't just put down that you don't know how to do it. We've been learning and practicing multiple tools and attacks until now. Document ***what doesn't work*** along with what does work. I already know there are a couple of Russian and foreign-language websites out there with supposed "walk-throughs". Don't use these. Don't copy and paste from these. They defeat the very spirit of the original CTF9 documentation which states solutions should not be posted online to give learners a chance to learn for themselves. The point is for you to try stuff to figure it out, and your grade is based on what you try and document. Also, there are likely multiple ways to get root, so your solution may differ from another team's solution.

Other Things

- I do not have all the answers. (I know, I look like I do…)
- I'm expecting things to sometimes be difficult, even with the hints and solution videos available. Sometimes the difficulty will be in getting things set up. Other times it might be in figuring out what you should be watching or modifying.
- If you don't know what something is, Google it to find out!
- I expect you to have to use Google to figure out features of the tools discussed, or you may even have to find a newer tool that does the same thing.
- If you use another source, cite it!
- Make sure you are taking the time to learn. If your documentation doesn't convince me you really understand what's going on, I will award less points.