System Security Group Project #4

(10% of class grade, due 3/19 at 11:59pm)

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 the departmental vSphere and the following virtual machine images:

- LAMPSec CTF9 (slightly modified from original LAMPSec CTF9 vm)
- Kali Linux (same from previous project)
- Optionally, you may want to look at other LAMPSec CTF walkthrough documentation for some other ideas. The sourceforge website with links to all the virtual machines and documentation is here: https://www.vulnhub.com/series/lampsecurity,43/

Directions:

Create instruction documentation on your group wiki for the CTF9 virtual machine, and prepare to give a 5-minute talk on the Tuesday after Spring Break about what you did and what challenges you encountered.

The deliverable

I am expecting a **new instruction** documentation in your group google folder 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.

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

On the class period after 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 the internal peer assessment on the distribution of work on the due date. (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.

Some Rules

1. We assume that you do not have physical access to the real machine. This means that you **cannot** attack the machine from its terminal:

   In other words, **you must attack it from Kali**. Remember, we are acting as a pen tester. We do not know the logins to this machine – we are trying to exploit weaknesses of the configuration and vulnerabilities of the software to gain remote administrative access.

2. Going further on rule #1, you cannot do any grub-based attacks on CTF9. For example, if you are familiar with how to root a machine by changing init=/bin/bash, this attack **is not allowed.** Again, we are attacking from Kali with the goal of discovering configuration weaknesses and vulnerabilities.

3. You can restart the CTF9 machine if it is misbehaving for any reason, but you should not be controlling it in any other way on vSphere.

4. There are at least two ways I am aware of off the top of my head to gain remote root on this box, but I wouldn't be surprised if there were more….

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.