System Security Group Project #4

(10% of class grade, due 3/28 at 11:59pm)

Capture the flag without training-wheels. Attempt to get root on a CTF vulnerable virtual machine without documentation. Create a group vulnerability analysis report with steps and screenshots detailing what you did. This project is worth 10% of your class grade.

What you will need:

You will need access to vSphere and the following:

- LAMPSec CTF9 virtual machine (one per group)
- Kali Linux (same from previous project – one per group member)
- Vulnerability Analysis Report template
- 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/

Deliverable and Rubric:

I am expecting a **new** vulnerability analysis report (documentation) in your group google folder for the CTF9 machine. Base your report on the project 4 vulnerability analysis report template found in the class google folder.

Your team will be graded based on:

Item	**Possible Points**	**To receive full credit:**
Reconnaissance	35	• Cover reconnaissance with tools nmap, nikto, nessus, and at least 2 other methods. • For each reconnaissance method, don't just copy and paste what the tool tells you. I also expect a narrative of what it means. (For example, what is the nmap readout telling us?) For nessus, please show and discuss all red and yellow findings.
Attempted attack vectors	25	• At least 4 different attack vectors are attempted based on weaknesses found in the previous section. Each attack vector should have its own chapter and be written as a narrative. What did you try first? Did that work? What did you do next? I expect a lot of screenshots in this area. Attempted attack vectors do not have to be successful,

		but I do expect a strong effort to be put forth to get them to work. • If the attack vector is not fruitful, please include a section in the chapter of what could be tried in the future.
Documentation	25	The following must be present: • Cover page • Table of contents • Reconnaissance chapter • At least 4 attempted attack vector chapters • Page numbers • Screenshots of tool readouts/command line • Narration paragraphs explaining what was found and/or attempted • Complete sentences • Chapter headings and subheadings
Compromise level	15	Finally, 15 points will be set aside for the compromise level of the machine. The machine is vulnerable to multiple types of attacks in different ways. Your team will score the full 15 points if at least one method was able to gain root privilege with a root command prompt. You will receive partial credit for successful website XSS attacks, local non-root account compromise, and/or being very close to compromising root.

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.