

System Security Group Project #3

(10% of class grade, due 3/2 at midnight)

Capture the flag with training-wheels on. Follow slightly out-of-date documentation to exploit vulnerable servers. Update the documentation with words and screenshots for Kali Linux. 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 CTF4](#)
- [LAMPsec CTF5](#)
- Kali Linux (same from previous project)

You will also need the original LAMPsec documentation for each machine:

- [ctf4_instructions.pdf](#)
- [ctf5_instructions.pdf](#)

Directions:

Follow the [instruction video](#) for downloading, installing, and running the CTF4 and CTF5 machines. Be sure to follow the directions so you know how to find the IP addresses of the CTF machines. Follow the provided documentation to learn how to exploit weak services and protections in the CTF virtual machines. The documentation is old (does not use Kali Linux), and it may use outdated tools. Create updated instruction documentation for each CTF virtual machine based on the old documentation.

The deliverable

I am expecting **updated** documentation on the wiki for each CTF machine. Create new pages in your group wiki page called "CTF4" and "CTF5". Place your updated documentation in this area. Specifically, in terms of your updated documentation, I'm looking for screenshots of each step using Kali as the attacking machine, as well as explanations. Use the provided documentation 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.

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.)

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.
- I know other walkthroughs exist on the Internet. 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.