

Homework 10

This homework is designed to give you some more experience on CTFs, especially on the super easy side of things. In the NCAE CyberGames, you'll have lots of points you *can* get from the CTF, and if you don't get many, the odds that you win are low.

First of all, a Jeopardy-style CTF is a competiiton format where you are presented with a broad variety of challenges in a similar format to "Jeopardy," meaning you have a set of categories and can choose which challenges to solve. In each challenge, there is a vulnerability baked into the code by the author, and you are expected to exploit it to find the flag, which will be a string. In NCAE, the flag format is `c2ctf{...}`, meaning every flag will start with `c2ctf` and be wrapped in curly braces. This is what you will submit to the competition for points.

The typical categories in a CTF are Web Exploitation, Reverse Engineering (re/rev), Forensics, Binary Exploitation (pwn), and Cryptography. Most challenges in these categories are out of scope for the regionals, and if they do give you challenges in those categories, it will be very basic. NCAE has a lot of categories in a custom category for SIEMs, which is why we will have you do some Splunk training for this.

This lab is split into a couple of pieces based on categories, and for each category, the requirement will be that you submit a PDF with a screenshot of completion for each of the 3 requirements (so one PDF with 3 screenshots, submitted to learning suite):

- Cryptography : go to [Cryptohack](#), make an account, and complete the course [Introduction to Cryptohack](#). When you've completed it, the home courses page should have a little banner that says you finished that you can submit a screenshot of.
- Web Exploitation : play the [natas](#) wargame on OverTheWire. Submit a screenshot of you receiving the flag for natas9->natas10 (the password for natas10)
- SIEM : play through the [Boss of the SOC - Splunk](#) website defacement scenario. Get at least the first 3 answers AND at least 250 points then submit a screenshot demonstrating both, but go further if it interests you.

If you have questions regarding those assignments, look online, google things, etc. In the CTF you won't have external help from us, so we will ask that you also solve these on your own (though most challenges have good hints built in).