2022 Cyber Storm

Note: This document may be amended/changed at any time.

Cyber Storm is a "hacking" competition (or hackfest) that pits several teams against each other in a fierce battle to the death! Well, not really, but you get the general idea. The teams are split from Introduction to Cyber Security (CSC 442/542) and Computer Network Security (CYEN 301), and are denoted by unique colors (e.g., `Red`, `Blue`, etc). The "administrative" team (Dr. Kiremire, Dr. Timofeyev, Dr. Gates, Dr. Walters, Mr. Spurgeon, Mr. Digilormo and a few other carefully selected students that have participated in the event in the past) will comprise `White`. I should probably mention that this event serves as the final examination for the class. And, no, losing the competition does not mean failing the course. At least not in odd numbered years...

The teams will be provided with some hardware and a lot of know-how (a large part of succeeding in Cyber Storm is a desire to learn and explore on your own – to tinker). This document outlines a set of requirements, goals, and rules that, in part, define the competition to be held on Friday, May 13, 2022 from 9am-5pm (although you will need to set aside from 7am-7pm), in the **new** Integrated Engineering and Science Building.

Cyber Storm has significantly evolved since its inaugural event in 2010. In years past, the event had a significant defend and attack component. That is, teams would defend their part of the network and attack opposing teams. Over the years, however, this has become minimal in favor of challenges. To be clear, attacking opposing teams is still acceptable (and often quite fun!). Teams are permitted to attempt to infiltrate, compromise, disrupt, and generally take down their opponents. But it is not always about "taking down" your opponents. Often, we prefer to covertly "own" our opponents. More about that later. Of course, all teams are to leave `White` alone (we will discuss exactly what this means later) under penalty of death. Or maybe just losing 100% of your points at the time of the infraction in addition to failing the course. Gah!

You will need permission from `White` to carry out any exploit that may *irreversibly* take down an opponent's system. For example, you may not format an opponent's drive should you have the capability to do so if and until `White` has given the OK. However, no permission is required to take over a system. In other words, if it is something destructive, ask. And if in doubt, you might also want to ask first.

The only requirement for the competition is that you have your various systems (e.g., laptops, desktops, possibly servers in a provided rack, etc) setup and ready to go. This means that your systems have a host OS installed (and hopefully secured), and possibly setup with various virtual machines. As the competition goes on, you will be given various challenges.

Some notes:

1. It is usually the case that some member of your team (usually the team lead) has a bout of diarrhea during Cyber Storm. No, not the actual thing (well, hopefully not

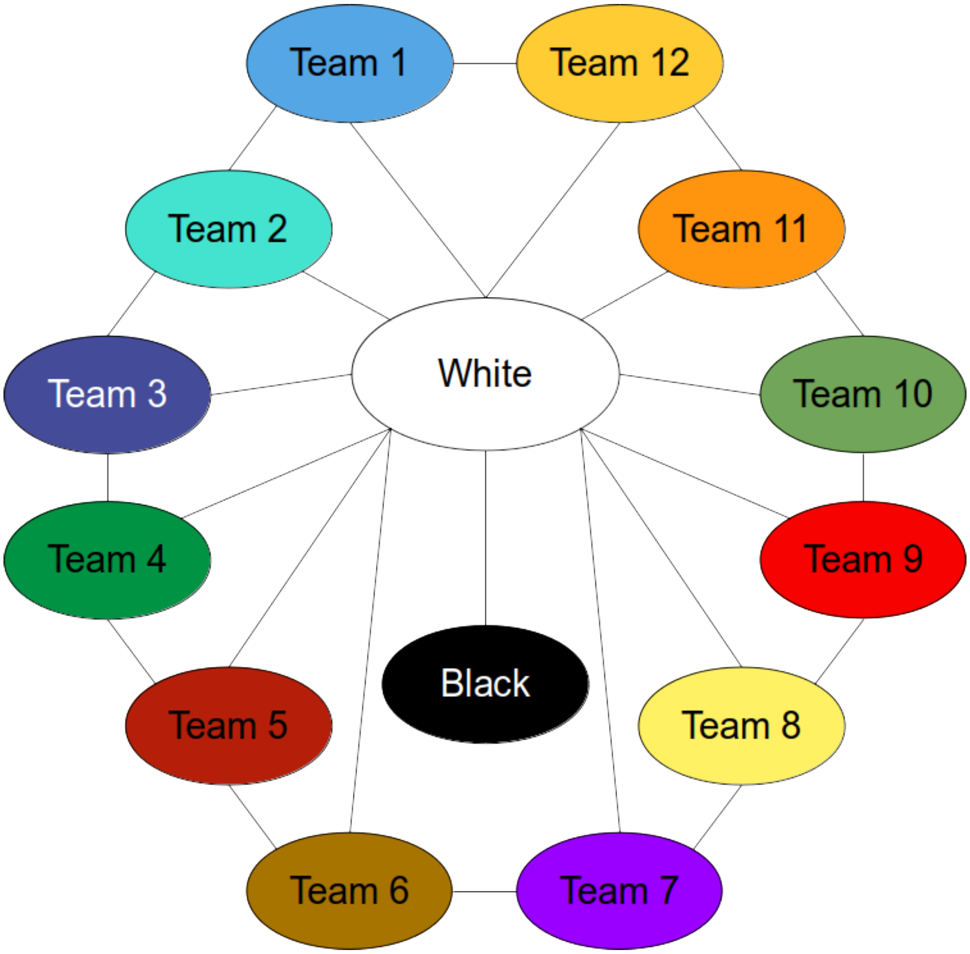
anyways). It's merely a simulation, in that some member of your team is temporarily pulled off to see how the rest of the team functions without a valuable team member!

2. Since Cyber Storm occurs all day (you must be there from 7am to 7pm), it may be necessary to obtain a university excuse. I can provide one for you if needed. Usually, just communicating the event with your instructors works.

3. Every participant will get food and drinks (during the event) and perhaps some candy! The winning team gets bragging rights – and possibly a poster of the event.

Network topology:

During Cyber Storm, a network topology **similar** to what is shown below will be used. Generally, the teams are connected to each other to provide overall connectivity. The administrative team is also connected and periodically polls all of the network switches for data. This provides overall situational awareness. This configuration may also be utilized during some of the labs and in-class challenges. **Note that no team should ever be simultaneously connected to the Cyber Storm network and to any LA Tech production network!**



Ground rules (you know, so that we actually have a competition):

1. No DOS or DDOS attacks;
2. No ARP spoofing or spoofing any other team (i.e., stay within your set of assigned IPs);
3. No MAC address spoofing (see #2);
4. No altering of the Cyber Storm network (e.g., creating subnets, VLANs, etc; see #2);
5. Don't go after switches (`White` is using them to deliver situational awareness);
6. No destructive attacks unless you obtain permission from `White` first;
7. No simultaneous connections to the Cyber Storm network and any production network (e.g., LaTech OpenAir, LaTechWPA2, etc); **unplug from the Cyber Storm network before going on the Internet – or use your cell phones or dedicated laptops**;
8. Wireless networks within the Cyber Storm network will all relate to the theme and will be advertised when available;
9. No attacking `White` or spectators (who may be browsing around and inspecting the network);
10. Do not bring your personal power-hungry gaming desktops (they demand too much power); each team member **must** bring **one** laptop and can bring a mobile device (if desired); however, each team is limited to **one standard** desktop (for the entire team); and
11. Remember that the point of Cyber Storm is **not** to try to find weaknesses in the competition itself and exploit those!

The rest of the document outlines the example of network specifics provided for teams during the competition. Currently displays information from previous year.

White

The Sun
Administrative Team

Network

Subnet:	`10.0.0.0/8`
Netmask:	`255.0.0.0`
IP Constraints:	`10.0`, `10.50` (challenges)
Access Portal:	`https://10.0.0.10:1337/access`

Black

The Moon
Black-Ops Team

Network

Subnet:	`10.0.0.0/8`
Netmask:	`255.0.0.0`
IP Constraints:	`10.13`