Retrospective for April 22, 2023 CDC

A cooperative document produced by the second-best high school cyber-defense team in Iowa

What went well?

- we got second place
- our ability to do things under pressure was SWEET
    - very little time to get things back up and running
- specialization:
    - Anna focused on anomolies
    - Tristan focused on servers
    - Michael was the utility infielder/focused on everything
    - prevented unintentional damage to each others' work
- having a small team helped us communicate better

What could have gone better?

- Number on priority should be to make it work; number two should be securing it

    - chris says: good item to discuss :)
- Plan ahead of time for contingencies
    - if we are pwned, do we roll back to a previous state or do we recover in place?
    - another good item to discuss

What would we like to change in the future?

- Aksel and Isaac have been recruited; little do they understand what awaits them
    - Aksel has at least some programming ability
    - Isaac has general knowledge about networking and programming
- what should the size of our teams be in future years?
- emphasize that students should experiment with tech between meetings
    - there were activities available this year
    - apparently I (Chris) did not give clear enough guidance about how to experiment with these technologies. I apologize for that and have some comments that I will sent to you later.
- look at SQL injection and other common app vulnerabilities
- hands-on is important for anna w.r.t. coming back next year

What was the impact of getting the scenario so late?

Negative impacts

- very little time for documentation
- things broke suddenly and repeatedly: not a lot of time to diagnose
- didn't get default users setup: not a lot of time to understand scenario requirements
- default passwords changed: we missed one because of time - no redzone checklist
- no nessus scans

Neutralizing impacts

- at the beginning of the competition, almost nobody had all of their services up
    - team 2 did for a while, but they quickly got pummelled and fell to 9th place

Helpful impacts

- simplified the scoring of availability/usability by collapsing the scoring to "does SSH work"
    - what would have happened if the scoring was more in-depth?

Chris's comments about hands-on material

First, I do apologize for not having more "traditional" homework with step-by-step guidance as you may have expected. Most years I've coached, the teams did not want, need, or ask for very much formal homework. This is because they followed along very well in class, doing all the things I was doing. That's on me. At the end of class for those other years, homework assignments would usually come down to, "why don't you see if you can (do this thing we're trying to do) this week or (fiddle around with some of the stuff we just did) and ask questions during the week if you have problems. They got hands-on experience because they did all the things I showed them.

This year turned into something more like lectures instead of guided hands-on sessions. That's a huge difference, and that's on me. At first it was partly deliberate because of wondering about pacing with a relatively inexperienced class, but then I just lost track of it.

If I have time, I hope to do more videos next year. However, it's not a given that I will have lots of time. Making traditional step-by-step homework for this topic is time-consuming and a little odd since you're typically summarizing things that are just a bit different from what's findable on Google. This is advanced content. It's not all high-school level material. My goal is to teach you material that is at least college-level at all times. So the type of homework I'd like to give you is very open-ended. I'd like to spend a session talking about what DNS does and then assign this:

```
"Install an instance of the BIND9 DNS server and figure out how to make your VM's
DNS resolver use it."
```

I'd tell you to discuss the things you don't understand in Slack and we'd go from there. Why? Because that's "the way it really works." Life isn't multiple choice, and the only `Step 1/2/3/...` instructions you'll find are in Google or ChatGPT. Even for those, once you find them, you have to be able to tell which answers are appropriate to your situation and are accurate. In other words, life is a really long open-book test, and it's all story problems. I've always tried to run my clubs in a way that helps people remember that.

However, I know I can't go that far, at least not with everybody. But if you are in this club, expecting everything to have `Step 1/2/3/...` instructions is more than I expect to give. If you all want instructions like that, please tell me. I can change my approach. My tendency would be to go to videos. While they also take a long time to produce, they also take less energy than writing because I try to write with a "professional author's habits, but I've found that I can just be me on video. I could even leave in the outtakes to save myself more time. :)

Also, remember my promise at the beginning of the year, at the kickoff event? It was that the best way to predict how much you would learn and grow was how much time and effort you put into the subject. I think that this held true this year. It basically always holds true. How you prioritize your time is up to you. I'm never going to turn this club into a program that says you must attend every session and you must put in four hours per week or you're dead to me. There were other homeschool programs that acted that way *many, many years ago* when we were a homeschool family, and I think there is probably still too much of that kind of thing, and I grieve over that.

I'm especially never going to tell you where Cyber Defense should fit into your family's priority's or your own priorities. I'm just going to say that if you want to get good at something, it takes time, and the same is true for cyber defense.

Malcolm Gladwell has said that it takes about 10,000 hours of effort to become an expert in something. That's about five years of full-time work. I don't think you automatically become an expert when you hit 10,000 hours. In fact, I'm pretty sure I work with some counter-examples. But it takes that long to have the opportunity to learn enough. Until that point, you really don't have enough experience to "know what you don't know."

My point is that no matter what, you won't go through three years of IT Club and come out a bona-fide expert. You have time to prioritize family, or music, or IT Club, or horticulture, or sports, or anything else. Eventually, you will probably specialize in something enough that you will have the 10,000-hour opportunity to become an expert in it. It only takes about five years. :-)

However, if you do decide to make our Cyber Defense club a priority, and put several hours a week into it, you will advance quite a bit beyond your current level. If you start off with a basic understanding of networks or programming, obviously your initial level is different than if you start off from scratch, but that's still the promise.

Back to the topic of "hands-on opportunities." Although I did not present these opportunities as clearly as I should have, I'd like to do something that we sometimes call a "true-up" at GoDaddy. A true-up is when you take inventory of what actually happened so that the context you have is as accurate as it can be. I looked back through the notes that are on our Github website, and found the following hands-on topics, all of which had notes that were more than adequate for doing walkthroughs of the material at home. I didn't look at the two videos I made, but I think they only covered material that is also on this list. I am not including material that we talked about that I never wrote decent notes for.

Here are the topics I found:

- Installing Virtualbox
- Installing Ubuntu
- Using `apt` to install and update apps and services
- Installing, configuring, and using `ssh` and `sshd`
- Managing services with `systemctl`
- Configuring `sudo` to protect root
- Object permissions (basic)
- Object permissions (intermediate)
- `find` command (basic)
- `find` command (finding files with specific attributes)
- Setting up and configuring a DNS server
- Identify listening processes with `netstat` and other tools
- Configuring the `ufw` firewall with `gufw`

In addition to this we also took a detour into HTB and THM, which was extended into three weeks by popular demand. You were specifically encouraged to continue experimenting with those sites if they had any content that interested you. THM in particular had courses that covered a wide range of material.

We also spent parts of a couple of weeks on the **Advent fo Code** so that we would at least discuss programming a tiny bit.

The point is that I identified 13 topics in our notes, two hacking web sites, one of which had a complete library of other topics that we looked at, and a coding challenge that we looked at.

If you want a bit more guidance in your homework, I can give you that. But I am going to ask you to meet in the middle. If I am giving you this much material to work with, don't wait for step-by-step instructions. When the competition happens, and most significantly, if you want to have a job with significant responsibility and autonomy, you will not get step-by-step instructions. You are at the age where the faster you learn to proceed without such instructions, or to write your own instructions or find GOOD ones on the Internet, the more you will begin to stand out among your peers. And helping you grow in that way is a very real goal of this program.

Please let me know what you disagree with! Also hit me up with any other questions or comments.