Intro
Hello, I’m Dana Fellows. I currently work for TestOut Corp as an Instructional Designer and Content Developer but the focus of this talk is more about my time teaching high school kids when I lived in Illinois.

Career Center
I was hired to teach at this career center and my students were high school juniors and seniors. The students were able to take a variety of courses but mostly A+, Network+, Security+.

Network Admin
In addition to teaching, I was also the schools network administrator and took care of every single aspect of the schools technology. So being a brand new teacher along with taking care of all of the technology, I had my hands full.

Old Stuff
One of the first things I discovered is that the network was very old. This was in 2007. There was maybe one Cisco switch but the rest of the network was connected with hubs. To make things worse, I didn’t have passwords for many of the things such as the wireless access points, many of the PC’s had admin accounts but I did not know the password to those accounts, only the limited student accounts.

Students Know Password
And finally, many weeks later, I found out that several of the students actually knew the admin password for the school. It was about two months into the school year before I found out that some of the students knew the admin password.

Cain and Abel
During that time one student had installed the program Cain & Able on one of the computers in the classroom. I found out later that he would install it at the beginning of the class, capture traffic for the entire 100 minutes of class, and then uninstall it at the end of class. I was able to figure this out by looking at the event logs. So once I figured this out he was questioned by our schools director and once she found out the potential severity of this, called in the school resource officer from the neighboring school. The student confessed to everything and was actually put up to this by a former student of the school. Their plan was to find out passwords and to use them with malicious intent.

Student Arrested
So to wrap this up, the student was arrested for computer tampering. He lost his high school credits for the class. Since this was dual credit he failed the class for college purposes which messed up his college GPA. I actually felt a bit bad for the kid because he was talked into this from the ex-student, who by the way denied everything and didn’t get into any trouble. The local states attorney ended up mishandling something with the case and the judge dismissed the case but I was Okay with this since the kid certainly did receive enough discipline from the school and lost his credits.

Confused
So, where are you going with this story?
My point of telling this story is to explain what happened next.

At that point on, I really started locking down everything. The school spent money for switches, some new computers, better servers, and things in general to make my life easier. However something negative happened also.

Cut Back On Teaching
I actually cut back on what I was teaching students. Anything that I felt the students could use maliciously, I cut out and did not teach. If you think about it that could potentially be a very long list.

But, things started to turn around. It was like a year or so later that a few students came to me and asked if they could try to crack a password on QuickBooks. The one student’s mom used QuickBooks for her business and I guess he was curious to see if it could be cracked. I allowed them to set up a standalone system and mess around with it. I can’t remember what program they used but they had me set a password in QuickBooks and were able to crack it in a matter of a few minutes. They said they were curious and wanted to see if they could crack the password. Both were very good students and were just those types of kids you know that are going to do well, and both have. This was over ten years ago.

So besides the students being curious about being able to hack into things, I started becoming curious on how easy it is to hack into things. It was about then that I started introducing more activities but was still pretty cautious.

Curious Students
This brings up a good question. Why do students try hacking things? Are they trying to steal passwords to be used for malicious use? Are they just trying to sharpen their skills for career purposes? Are they just bored and looking for a challenge? I’m leaning toward that fact that they are bored and looking for a challenge more than the other reasons but that is not always the case.

Scan Tool
In a small town near where I lived in Illinois a high school senior used a network scanning tool to scan the schools network. This tool showed all connected devices and shared folders. There was a network drive that was shared with no password assigned. In that folder were dozens of files that the schools secretary had put in there.

Spreadsheet
One file was a spreadsheet that contained all the students’ personal information, social security numbers, address, phone numbers, parents names, and so on. Over time that student would do things such as ask girls if their phone number was such and such, or ask other students if their social security number ended a certain way. Eventually this info got back to school administrators and they questioned the student confessed to what he found. The student stated that he meant no harm and did not use any of the information for anything malicious. He was arrested but charges were dropped. Discipline included him not being able to participate in graduation ceremonies at the school. He stated he did not inform the school about the files because he was afraid that he would get into trouble.

Retired Teacher
The tech person at the school was a retired school teacher who had returned to the district and had very limited tech skills. The district actually attempted to keep this from getting out and it wasn’t until some parents contacted the press that it got out.

Erie Bypass Filter Nuclear Plant
There was another small district in my area. The district had a lot of money due to a nuclear plant being in the tax district so they were one of the first districts to have a one to one program. That is each students had a device that they got to take home and use. That district was part of the career center where I taught and some of their students were in my classes. The district filtered student’s internet by using a proxy.

School Proxy Graphic
Basically the student’s internet would connect back to the school, when they were at home, and then the internet would get filtered by the schools filtering system. I found out that some of the students that were in my class had figured out how to modify the proxy settings and bypass their schools filtering.

Bypassing Google Results
If it wasn’t bad enough they knew how to do this, they actually configured nearly every laptop in the high school to bypass the districts filters. I think am not sure how long this went unnoticed but I think it was nearly the entire school year.

EdTech News Article
I could stand up here all day but these are just a few examples that happened locally to where I taught. I’m sure of a few things. Most school districts have had students hacking their systems. Many districts have known about their systems being hacked but have kept it hush, hush. And many districts have had their systems hacked and no one has ever found out about it.

Students Interested in Ethical Hacking
So what do we do with students who are interested in cybersecurity? You can pretend they don’t exist and just avoid the subject or you can get them involved and encourage them to use and practice those skills for good. But how do you do that?

Cyber Laws
There are a lot of grey areas between what is legal and what is not legal. Laws vary between countries, states, locally. Not only that, companies have their own policies. It might be legal to use a program to scan a network for example. Doing so might not violate any laws at all.

Cloud Providers
But what if that network is hosted on a cloud provider?
What if that cloud provider has an acceptable use policy that prohibits scanning?

AWS Terms of Use
And further, what if that cloud provider decides you violated their terms of use and bans you from using their system forever? And, what if this cloud provider is Microsoft or AWS and the person that has been banned is an 18 year old students who really didn’t mean any harm and really didn’t know they were doing anything to violate the cloud provider terms. Now what does that do for their career? I know that is a lot of what ifs but the thing is, it’s really hard to learn ethical hacking, pretesting, and cybersecurity skills without potentially getting into trouble. So how do you teach offer these classes? Well you have a few options.

Virtual Machine
One possibility is using virtual machines locally. This is probably not a good option because of what it would take to set up. This list of disadvantages could go on and on such as the possibility of the student getting the virtual machine onto the live network. My opinion is that for K-12, this is not a very good option.

Hosted Virtual Labs
There are virtual labs hosted on remote systems. There are some advantages, students are working on real systems so they have realistic issues, good and bad. There seems to be several disadvantages. You have to have great internet speed, Sometimes navigating them is a skill by itself, some have time limits that you can be logged in, with some if you get disconnected, the systems reboot and the systems reset themselves, as a teacher you will need to rely on students to take screen shots of their progress for grading, and finally the cost for high schools is prohibitive.

Simulated Labs
You have simulated systems. These are not virtual machines but rather realistic simulated machines. The disadvantage is that they are not real machines.

The advantages includes flexible access for students.

Simulations are usually web based and can be accessed from anywhere you have an internet connection.

They are typically device agnostic, meaning you can use different devices, such as Windows, macOS, or Chromebooks to complete the labs.

They can be used in shorter chunks of time, meaning you don’t have to spend an hour or so just getting thing set up. In a classroom time is pretty precious.

Students can get instant feedback from the simulated labs, no waiting days, weeks, or longer for teachers to catch up grading. When such a long period of time has elapsed, students will not remember really what they did wrong or right.

Students can redo and practice labs over and over in a short period of time. No one shot at it and you’re done.

No software license to worry about. No equipment to maintain. No outdated machines. Simulated infrastructure can replicated tens of thousands of dollars of real equipment.

If real equipment is available, having students do simulated labs will prepare them and when they do labs on real equipment, their time is better spent. This I what I use to do as an instructor. Students will have been exposed to the tasks.

Testout Homepage
I’ve talking about how to create a safe and legal environment for students here. It is true that I work for TestOut and TestOut’s business is creating curriculum and simulations. However I would be doing the exact same presentation even if I did not work for Testout. I was a customer of TestOut for over ten years and was very impressed with the product from the first time I saw it and used it. A few of the courses that are my favorite is the Security Pro and the Ethical Hacker Pro. It won’t take long for students to get bored with curriculum, not matter what type it is. If the students are like most tech students, they have a love for games and challenges. I had the pleasure of being one of the lead designers on the Ethical Hacker Pro course and when I was working on this, I did so as if I was going to use this in the classroom. First, we mapped it to the Certified Ethical Hacker objectives but second, I tried to design many of the demonstrations and simulations to also help students learn skills that they can use for various capture the flag websites.

Capture the Flag
Capture the Flag websites and competitions come in all shapes and sizes. One of my favorites is the site, Hack This Site. The site is divided up into missions that you complete. Many of the missions are basically the same sort of things you end up learning in courses that teach cybersecurity but when students are doing this missions, to them it is a game or competition, not homework. There are dozens of these capture the flag sites to choice from.

The End
OK, that wraps up what I have to talk about today. I’ll be around the rest of the day and if you haven’t already done so, please stop by and see Travis, Cole, or myself at the TestOut booth. I’ll be roaming around and also attending other sessions but I’m easy to find on LinkedIn or email.

Thanks for your time today.