Heather:

Welcome to the Hurricane Labs Podcast. I'm Heather and in today's podcast, we're going to hear from two of Hurricane Labs, team members, Tom Kopchak, our director of technical operations and Meredith Kasper, one of our SOC architects, about their experience, red teaming for the Northeast regional of the Collegiate Cyber Defense Competition. In this yearly competition, students try to keep their system secure, maintain business operations, and complete various administration tasks while cybersecurity professionals like Tom and Meredith attack their systems. Tom, Meredith, thank you for taking the time to join me. I appreciate it. The theme for the regional was "The Hunt". So can you tell me a little bit about the premise for this year's competition?

Meredith:

So the overall premise, as you said, was "The Hunt", which is essentially the threat hunts that the student competing teams do and where they go through and hunt for the red team in their systems or on their network, or a bit of both actually, and sometimes physically in their rooms, which they may not have known about beforehand, but it did happen.

Tom:

So the idea of the CCDC event is to give students the experience of what it's like to defend their own corporate environment from a team of attackers. And Meredith and I got to spend the weekend being the two team of attackers or at least part of the team of attackers to make the student's lives more interesting–and interesting was definitely the result of that.

Meredith:

On that team we were on, we had a total of nine red teamers being those offensive attackers. One person was focused on Windows the entire time. We had one Splunk specialist. I'm sure you can guess who it was. There was one person doing social engineering and firewall stuff. One ESXi focused person looking solely at that virtualization and then five people just attacking all of the Linux machines and shenanigans that they can come up with for those hosts.

Tom:

Yeah. So the way we work together, it's really good the way we work together as a team, as opposed to one person focusing on a student's or a school's environment, we all try to work across the board. So like, just if someone that I know well was working on Splunk, for example, we'd make sure that we maintain the Splunk systems or the Splunk components that are being used for fun at all the student environments. Your friendly social engineer, firewall administrator Meredith would be responsible for tracking firewall rules. And if someone on the Linux team, for example, realized that something that they were doing was blocked by a firewall Meredith would be responsible for resolving that firewall issue.

Heather:

What sort of tools were you given to make all of this happen?

Meredith:

So from the red team perspective, we basically had carte blanche to design what we wanted to design or to bring what we wanted to bring. And the teams actually got a really nice base set of tools, including

Wazuh and they were able to start off with some things that could easily help identify red team and suspicious activity on their network that the red team had to learn to work around and evade detection in while we were deploying our things across all of the teams and trying to evade that detection ahead of the competition, which was pretty cool.

Tom:

Yeah. And a lot of times teams don't have a ton of visibility into what red team's doing, but giving the students a little bit more opportunities to see what we're doing and what activities are happening, I think it makes our job harder, but it's more realistic too. And if the students don't have visibility of what we're doing or the ability to see things, it makes it really hard for them to get us out. So the battle I think, between blue and red is really a key component of this event.

Heather:

What sort of strategies did you guys use?

Tom:

So I think we kind of broke down into a couple categories. Meredith focused on firewalls and social engineering and I tag teamed with her on the social engineering side and also used Splunk as well. So maybe we want to cover social engineering first since that was the teamwork aspect.

Meredith:

Yeah. So from a social engineering perspective, my goal was essentially to establish trust early on and thanks to the wonderful marketing team at Hurricane Labs, we had a bunch of swag to give away to students. And you want to know what students love? Free stuff. So I started off my red team experience, firewalls and wireless and all that fun aside by establishing some trust with the students, asking if I could take some photos of their teams, just some really awesome action shots, which you can check out in the awesome video. But I asked for that permission. And once I was given that, I also offered some free stuff and those free things did come into play later on just for fun and games. But at that point I was essentially a trusted entity as somebody who wasn't on the red team, wasn't doing anything malicious to them, just going around, taking some awesome action shots of their team. So I was able to come back time and time again and take some photos of the team, maybe of their screens, potentially of their password lists and questionable things they had written on the whiteboards, and bring that back so that the rest of the red team could have those passwords if we were having trouble getting into a system.

Tom:

And this is something I think that took the students a little bit by surprise, just since the last two of these events were remote. So the thought of auditing who came into your room and maybe assuming that some of the individuals who come into your room are not necessarily trusted, was something that came into play. Then we kind of took it to the next level a little bit where I became official red team photographer with proper credentials saying that I was red team and a camera with a very, very, very, obviously large zoom lens that I walked around and tried to see what the teams noticed for that. And it was a really interesting pattern. Some teams obviously identified me as someone that they didn't want in their room taking pictures of everything that I could get a picture of, including whiteboards, passwords, screens and those sorts of things. And they took action to remove me from the room or make my life difficult. That was sometimes accomplished using the aforementioned Hurricane Labs swag, which happened to shoot things at someone because that's what we do with our swag. But one of

the interesting things was probably that first time through, more than half of the teams didn't really give me a hard time at all. I just walked around, talked to them, snapped photos of things, or didn't even necessarily talk to them in some cases. And I made no effort at all to hide my identity. It was blatantly obvious that I was red team, including we have the photo that you took Meredith of me just standing there while the team is just kind of not paying any attention, holding my red team badge with the camera. So that was fun.

Meredith:

Yeah, that was a good photo.

Tom:

So after the evening of the first day, the morning debrief for Saturday, we did kind of communicate to teams that pay attention to who comes in your room and who they might be, and the teams responded, I think fairly well by that, at least in the case of me, by noticing that I was a red team person. But the side effect with that, me wandering into the room, them all paying attention to me allowed you basically unrestricted access to everything that was going on in the room because of figuring you were a trusted entity. So the social engineering was very strong there.

Meredith:

Correct. And what we ended up seeing was students would not only ignore me and allow me to continue on, but they would physically go towards Tom, leaving their machines unlocked and papers out that had their updated password list through the day before, from when they believed they were compromised. And I was able to get some very good shots of those credentials, whether they were on the board, on a paper, I was even turning over notebooks and things. And I think that at one point Tom, some team accidentally gave you a notebook where they had been doing discreet math, but on the other side was the password list.

Tom:

Yeah. So that team, they were handing me the notebook. So I just start reading discreet math to them to start wasting their time and provide more distraction to Meredith. But I flipped to the back page like, Hmm, these are all passwords.

Heather:

So the moral of the story is don't write your passwords down on paper. Don't leave your screen unlocked. Don't trust Meredith.

Tom:

I think the third is the most important point, never trust Meredith.

Meredith:

I am friendly. Thank you very much.

Heather:

You want to talk about Splunk or do you want to talk about firewalls with this doll story next?

Tom:

Yeah. We can talk about Splunk real quick and then we'll talk about the firewall side of things. But so one of the things that the organizers asked us to do as red teamers was to ensure that the students had the opportunity to experience a ransomware attack, which as red teamers, we were more than happy to do that. However, there are some challenges that we ran into as red teamers because Windows Defender was actually killing the approach that we were looking to use to originally deploy the ransomware. So a couple team members on the red team went through a couple different approaches, either using Log4j or potentially sending it via other access that we had to Windows and everything was failing. So they were actually worried that we weren't going to be able to get ransomware out to all the teams. So I happened to be using Splunk as kind of a command and control mechanism on many of the team systems that we deployed ahead of time. And actually went ahead and with the help of some of the other members just kind of spot checking what I was doing with PowerShell, basically pushing out a Splunk config to ransomware all the team systems that I had access to, which was nine of the 10 teams. So I know everyone right now running Splunk is a little bit scared, but I do have a write up we can link up to in this document as well. It's something I've talked about, used several years in the past too, about how you can use Splunk for an offensive tool and what you can do to secure it. But basically just using Splunk for evil while wearing my Splunk for good shirt.

Meredith:

That was delightfully ironic. And I do support that.

Tom:

Yeah. And we knew pretty quickly when it worked. When our Discord chat that had all of the communication from the room, noticed that some team member was aware of that working. So it's always good to know when something functions when you're just on the remote end of things.

Meredith:

Between that and walking around and hearing some of the screams of, "oh no", wonderful combination.

Tom:

Exactly. Speaking of oh no, though the firewall, that was a really key component of our attack and US pfSense administrator for all red team activities was glorious.

Meredith:

So as a social engineer who was the official red team photographer who appeared to be the official blue team photographer, I didn't have much time to sit at my computer and actually stay in the firewalls via a persistent session and do anything crazy. So once again, we went a bit of a social engineering route to maintain access, which is slightly less technical than we would typically see. But it did help the students realize that one of the very important things that you need to do, similar to seeing an unauthorized application like Splunk on your hosts, is verify that all the users on the firewall are authorized and should be there as well. We had two accounts on the firewalls that had descriptions that at first glance to the teams meant that they shouldn't touch them. So we got to see them say, "oh, this is the CIO of the scenario. We shouldn't interact with this account." And "oh, this account might be used for scoring." We shouldn't interact with this account. And that helped me when I was wandering around taking those wonderful photos, because I was sitting there, logged in from my phone, watching teams change their

firewall rules and asking them about it. And as they were making that change, I was immediately undoing that change at the same time. However, to them, it merely looked like I was just texting.

Tom:

Yeah, you were just texting your firewall. No big deal.

Meredith:

Texting my firewall to improve things.

Tom:

And then I think we need to talk about the wifi doll.

Meredith:

So, okay. There seems to be this interesting stigma in society about people wandering around with dolls, that nobody wants to go talk to the creepy person wandering around with a doll. And if there is somebody wandering around with a doll, you don't ask them about the doll. So that means that if you've got something where you can fill some space, you could hypothetically stick a computer and a battery pack inside it and just carry it around and have it make some fun. The first day we did not receive credentials to any of the access points that the teams were given. So one of the things that I was doing was looking for those credentials so I could script out attempting to connect to those access points to see if they had allowed some random device on their network who was named my evil twin, because I was wandering around with a doll that was my evil twin. And there were no incident reports filed interestingly about the fact that there was a doll popping on and off their network, not doing anything, but just there. She could have been used if we needed, but she'll probably make another appearance. I can't say much more than that.

Tom:

Yeah. So the moral of the story there is, if you see someone wandering around with a doll that just happens to be connecting to your wifi, you probably should be concerned.

Heather:

And of course the other moral is don't trust Meredith, especially if she has a doll. Were there any strategies that you saw the students use that were pretty cool?

Tom:

What they were doing with Wazuh and identifying network traffic. Some students also use some third party tools to look for connections outside of their network and what software is making those connections. And when you think about it, anything that is malware is going to make a connection outbound. So being able to identify those connections is going to make a big difference in finding threats.

Meredith:

It was also great to see students go through and start combing through the logs, both in and out of Wazuh to see exactly what traffic was expected and they should be seeing on their networks and what they shouldn't and starting to selectively permit what they know is clean white listed traffic or traffic

that would give them points on the scoreboard and start blocking what they believe to be the red team. And teams usually did a very good job at identifying the few known malicious IP addresses that were the red team. Their only problem was figuring out how to block it, where the red team couldn't undo that block.

Heather:

What do you enjoy most about working with these competitions? You guys do quite a lot with helping students. So what is it that you enjoy about student competitions?

Tom:

For me, it's kind of giving back to the community because this event, CCDC is what brought me into the industry and being able to support the thing that kind of got me interested in the field has been something that I think is really important. And also just having realistic experience outside of the classroom, maybe learning how to do something that you don't necessarily know how to do under pressure is a valuable skill and helping students get that experience before they go into industry is really important.

Meredith:

Yeah. And from my perspective, it's just seeing the amount of time and effort that the students put in and watching them learn from year to year because we do see repeat phases. And it's nice to see them improve and have all that prep work and do things well.

Heather:

All right. Well that's all for today. Keep an eye out for their blogs on this experience, which you can expect later this month. And until next time, stay safe.