NCF #CyberChats Podcast Episode 002 - Transcript

00;00;00;02 - 00;00;09;23
Thomas Weeks:
The general concept is you harden in layers. Security is best when it's applied in layers, like an onion. And just like an onion, the deeper you get into it, the more it makes you cry.

00;00;14;26 - 00;00;47;08
Jen Langdon:
Hello and welcome to CyberChats, a podcast made by the National Cryptologic Foundation. I'm your host, Jen Langdon, and together we'll be demystifying the world of cybersecurity by talking with amazing cyber fanatics like you, as well as industry professionals.

Our conversations in this episode illuminate the seemingly dark arts of how hackers work and how training on cyber ranges and in real life challenges can help us learn how to defend ourselves.

00;00;47;19 - 00;01;13;28
I can't wait for you to hear our conversations with Ilana and Tweeks. After our talk with Ilana, she announced she just got accepted to the school of her choice. Congrats, Ilana!

And Mr. Weeks will have some great mantras and funny stories for you all about securing your devices.

Shout out to Cookie Monster, Cyber Viking, Gooseman, kind raccoon, Denise, Glitter bomb, Snoopy, and so many more listed on our leaderboard for doing our first week's episode challenge.

00;01;14;10 - 00;01;38;29
We'll have a grand prize at the end of our six-episode pilot and submitting to each challenge will increase your chances of winning. So if you haven't tried our bi-weekly challenge yet, it's not too late.

This episode's challenge is brought to you by the Virginia Cyber Range. We thank them for not keeping this challenge a secret. It's live on our website now at https://cryptologicfoundation.org/podcast.

00;01;39;16 - 00;02;04;19
You have until March 12th, 2023 at midnight to submit. So go and give it a try while you tune in here.

Also, if you're interested to see last week's answer, Eliot and I have a video for you with the solution. And it also includes many other professional OSINT tips.

Our student guest has a great story about how the pandemic affected her path in life.

00;02;04;19 - 00;02;20;12
I'm pleased to introduce you to this soon-to-be high school graduate, Ilana Payne. So, Ilana, you were featured on a student panel at NICE K-12 Cybersecurity Conference this past fall. What got you into cybersecurity to begin with?

00;02;20;27 - 00;02;41;06
Ilana Payne:

So my sophomore year, obviously it was COVID year. We were working on a hybrid schedule, and so I had just out of the blue kind of like decided, Oh, I'm going to take a cybersecurity class because it'll just it'll be, like, an easy class. The teacher is really fun. She's nice. And so I ended up being the only one in the classroom out of--

00;02;41;12 - 00;02;42;15
Jen:
Class in-person.

00;02;42;21 - 00;03;05;18
Ilana:
Yeah, in-person. Like, it was just me and my teacher Ms. Rice in this huge classroom with all these monitors and everything, and that was it. And so we spent, like, about half the year like that. Through that, I kind of got this really good relationship with her because doing virtual as a high schooler, really, it was really difficult to adjust to.

00;03;05;26 - 00;03;26;14
And so when I had it just that one-on-one time with her, I could create a bond that I wasn't having with anyone else because there was no one else in my classroom. So between that and then, the way that we did stuff in my classroom and how she-- even though it was a computer class because it was all virtual, we still got to try new things.

00;03;26;21 - 00;03;56;04
And so I learned a lot more from that first year. It's what got me into it. And so my junior year, I took her third year class because of scheduling conflicts and I got really involved with her CTF teams. And then we did something called Spotsy Hacks, and I got just really involved with doing cybersecurity and helping our community and teaching the kids around us and being able to compete in statewide and national competitions.

00;03;56;04 - 00;04;11;17
And I just figured that I was like, I'm obviously doing really good at this and I really enjoy spending my time on this. So I just figured that it was something that I wanted to do later in life because it came to me easily, but then also I was passionate about it.

00;04;12;09 - 00;04;33;03
Jen:
That's so funny that initially you were like, Oh, this will just be this easy class. I can just, you know, learn all this interesting stuff maybe. And now it's turned into, you know, it's a part of your life.

So eventually you became captain of the Cyber Knights Club at your school. Can you tell us about your role in that club, kind of what it is, and how did you become a leader?

00;04;33;12 - 00;04;56;10
Ilana:
My official title for the club is the Chief Security Officer. We came up with these really cool names and were like, Oh, this will be—like, I have my CTF name, but this is my club. Like, this is my position. And so it's about the equivalent of a secretary, I guess, in the normal roles. But with the club, I spend a lot of time working on the CTF.

00;04;56;11 - 00;05;18;03
So when we're trying to recruit kids from the freshman and the sophomores and the younger classes, I'll sit there and I'll help them figure out how to use the different resources that they have to complete those challenges and everything. And then also I help tutor them when they need help in her class. But I came into that role because of my junior year.

00;05;18;17 - 00;05;36;19
So we had actually placed, I think, fifth at the Radford CTF, which was like a statewide thing that we had. And then we did NCL this year. But because that team had worked so well together and, like, even though it was-- for a lot of us, it was our first time competing. We worked so well.

00;05;36;27 - 00;05;57;06
And we placed, like, top five out of other colleges and were going against other high schools and everything. So we just kind of realized that we wanted to bring back the club. And so with COVID, it had made it harder to do our club stuff and everything, but really just trying to bring it back this year as kind of a unity thing within cybersecurity and our school.

00;05;57;07 - 00;06;13;23
And so I came into that because of that team that we had created, like that bond we had created. So we were doing a lot of stuff together last year, and then we came into it this year. We're like, We're going to start this. We're going to start our club back up again. Like, we're going to make it so that our school is like, known,

00;06;14;01 - 00;06;20;12
so that we can get the funding, and that we can get the recognition for all of our really good students that we have.

00;06;20;21 - 00;06;25;09
Jen:
You mentioned funding. Do you win money?

00;06;25;19 - 00;06;44;25
Ilana:
Yeah. With the Radford one, I know that the top-- they won, like, scholarships to go to Radford and everything. And then we're doing-- like NCL, that one is just kind of recognition. But then we'll do CyberStart and we'll work together on that and we'll work with her classes and we'll work with the kids that aren't even actually in cybersecurity.

00;06;44;25 - 00;07;08;00
So it's like the normal population of our school. And we want them to be able to try something new. Like, we'll give them a like a prize for it, but then also we're getting-- those numbers add up and we'll get funding for it. So Virginia has put forth this initiative for it so that the top ranking in CyberStart are given a bunch of money for their funding and their cybersecurity programs.

00;07;08;13 - 00;07;21;27
Jen:

Some people might see that as part of a problem, though, like getting more and more people into cybersecurity because they might have the perception that, you know, we're training all of these kids to be hackers, right? What do you say to that?

00;07;22;11 - 00;07;44;07
Ilana:
I think it's just plainly false. Like, a lot of cyber security-- we're not training them to be hackers. It's just like a cyber basics class. We're teaching them to be safe on the Internet. And so a lot of that has come in when kids are growing up with the Internet around them. And so it's something that we need to be taught to save ourselves and our identities and everything.

00;07;44;19 - 00;07;53;01
So I think it's not necessarily we're teaching them to be hackers. I think we're teaching them to be safe online.

00;07;53;10 - 00;08;22;14
Jen:
At NICE, your teacher, Ms. Rice, she was there teaching how to break locks. And Thomas Weeks, he was there from the Virginia Cyber Range and he had a challenge set up for the Capture the Flag event. And for this challenge you had to sniff a router, which doesn't involve using your nose, as many of you may know, but actually involves capturing the packets of data moving to and from the wireless router that he had set up.

00;08;22;19 - 00;08;24;29
And within those packets was--

00;08;25;04 - 00;08;26;03
Ilana:
The flag!

00;08;26;07 - 00;08;53;09
Jen:
The flag! So in order to do this challenge, you needed some knowledge of Kali Linux, which is the essential brand of Linux for any cyber novice, right? The command line. And also Wireshark, which is a program that helps really visually organize the overwhelming amount of information within the packets sent through the air and sent to the wire. So tell us about how you felt about this challenge and the CTF overall.

00;08;53;22 - 00;09;12;03
Ilana:
Since I had some experience with CTL, I obviously really wanted to try it when we got there, but I think the sniffing was like a really cool experience because as like a normal person in a normal day life, I'm not going to be able to just sniff some wi-fi and find data from it.

00;09;12;03 - 00;09;15;14
Jen:
It's not like you get permission to sniff somebody’s router.

00;09;15;14 - 00;09;16;17
Ilana:
No. That's not on my to-do list.

00;09;16;17 - 00;09;20;09
Jen:
Shouldn't be doing that in ordinary life. Let me just put that disclaimer out there.

00;09;21;11 - 00;09;53;07
Ilana:
So I thought it was just a really cool experience because it was something where I could apply it—like, the stuff that I have learned. So when I used Wireshark in the past, I just used it to, like, analyze the data and see what was going through and everything, but using it with wi-fi and finding through that router and using all the packets to find the flag and seeing kind of like a real world purpose for it was really cool. Because in our classes we'll use VMs and those are virtual machines.

00;09;53;07 - 00;10;10;00
So that's, like, in a contained environment. But this you got to use it like in person, like I saw what people do, what hackers do in the real world, and they got to kind of use it. And it was a really cool experience for me to learn in a different way about cybersecurity.

00;10;10;19 - 00;10;29;28
Jen:
So also at NICE, you made a really amazing point at the end of the interview that gained a lot of applause, and I think a lot of people share this, which is that, you know, we don't need textbooks, right? We need all these experiences, these hands-on experiences in the classrooms. And that's really what we need to help move cybersecurity forward.

00;10;30;03 - 00;10;56;01
And I feel like the router sniffing challenge was empowering, like you mentioned, because it was really easy to see how hackers gain our information because they do the same things. And once you do it yourself, you're like, Oh my gosh, this this is how they do it. So with that in mind, you know, how do we use that knowledge to secure our own personal systems?

00;10;56;15 - 00;11;22;01
Ilana:
So obviously that taught me a lot about, like, just connecting to wi-fi and not being secure enough with, like-- not using a VPN and not keeping my own stuff together. And so it kind of just showed me how easily my data's accessible, like how easily I could just lose everything. And so realizing how influential that was-- like, it kind of scared me a bit because it was like, Oh my gosh, like these people just do this.

00;11;22;01 - 00;11;43;15
Like I could be at a coffee place and they could just steal my data. And so it kind of it taught me to be more careful about my connections and how I just connect to, like, the wi-fi just willy nilly. And so teaching a lot about that. But then also it kind of reminded me of what we learned with my Cyber Basics class about being safe on the Internet.

00;11;43;20 - 00;11;48;06

That kind of just reapplied that to my real world living a lot.

00;11;48;10 - 00;11;53;20
Jen:
Ilana, I want to thank you so much for giving your time. And we wish you luck on the next chapter in your life.

00;11;54;00 - 00;11;56;15
Ilana:
Thank you.

00;11;58;09 - 00;12;03;09
Charissa Kim:
There are two types of people: those that have been hacked and those that will be. Learn to stay safe online.

00;12;07;27 - 00;12;18;09
Jen:
This week, we'll be talking a little bit about system security with a man whose code name writes itself. Thomas Weeks or Tweeks has loads of adventures in cyber to share with us.

00;12;19;01 - 00;12;38;27
Thomas Weeks:
I'm a, I guess you could say, cloud engineer. My official job title at Virginia Tech is the director of Future Technologies and Communities. But I spend most of my time sitting here with the Cyber Range as a consulting engineer, so I work on cloud engineering problems and in relation to the Cyber Range.

00;12;39;07 - 00;12;49;05
Jen:
So tell us about your path to this field, because I know you started with electrical engineering in high school and it just kind of seems like this is a far way away from electrical engineering, if you know what I mean.

00;12;49;18 - 00;13;12;11
Thomas:
So I always loved electronics as a youth. And in junior high I got in and went to a technical high school, took electronics for three years, went directly into junior college, electrical engineering technologies, then transferred to Texas A&M and finished out my degree. Never changed my major. So always knew what I wanted to do. But along the way, I took-- at university, I specialized in telecommunications.

00;13;12;27 - 00;13;36;14
I loved computers, did computers on the side, and eventually doing computers kind of became my main thing. I was big into the BBS scene in the ‘80s and into the hacking magazines in the ‘90s and kind of loved security and kind of got sucked into IT as the main way I got into security kind of unofficially.

00;13;36;16 - 00;13;47;14
Once you get into it, you find you have to keep all your systems secure. And I really love doing that and worked for the DOD and Rackspace and other folks who would have me secure systems.

00;13;48;10 - 00;14;02;14
Jen:
So what does it mean to secure the systems or harden a network system? Like, how do you go about, you know, doing that? And particularly at the Virginia Cyber Range, what does that mean specifically for what you do there?

00;14;02;27 - 00;14;22;04
Thomas:
Well, what I do here is a little bit different than what I would do for a corporation for hardening systems. But the general concept is you harden in layers. I like to tell people security is like layers. It's best once applied in layers, like an onion. And just like an onion, the deeper you get into it, the more it makes you cry.

00;14;23;13 - 00;14;47;27
But the point there being you address things at the network layer and then on your devices, in the outer layer of your digital devices, then the services layer of your devices, then the file system and permissions all the way down to the user and data on the file system. So you have to do it at all levels because you can't just rely on a firewall.

00;14;47;27 - 00;15;06;08
For example, if you have a vulnerable Web server, they're going to drill right through your firewall and penetrate your Web server and then you’re owned. So you have to do it in layers. Now, for doing things here at the Cyber Range, our infrastructure is a little different. It's all cloud based. In fact, our entire front end and even our website is serverless.

00;15;06;15 - 00;15;35;05
There's no physical or even virtual machines involved. It's all what's called Lambdas or API calls to AWS systems that are all decentralized and load balanced. So hardening those systems is a little bit different. But the virtual machines inside the Cyber Range that people log into and actually use are actual VMs and those are restricted. The Cyber Range keeps packets on the range.

00;15;35;05 - 00;15;53;05
So each one of these virtual machines that students use, they're quarantined off into their own little network bubble that they can't get out of or into any damage to anybody else on the range or off the range on the Internet. So some systems, we purposely don't harden on the Cyber Range because they're targets. They're hacker targets.

00;15;53;05 - 00;16;03;24
And so we teach the students how to attack and then how to defend, how to patch, how to make things secure. So hardening happens at the network layers and at the operating systems and services layers themselves.

00;16;04;23 - 00;16;25;28
Jen:
So in trying to, I guess, describe to people what a cyber range is who may not have heard, I was thinking about this. One of my close friends, she used to work for a guy whose business was developing

models of legs, which at first I thought was kind of weird. But then, you know, you looked at them, they look like real legs, and they were for surgeons, you know, to cut and practice on.

00;16;26;12 - 00;16;40;19
And, you know, many people may be more familiar with, like, the mannequins that we practice CPR with. So it's really common, you know, in the medical community to not use real people. How is a cyber range similar in that regard?

00;16;41;10 - 00;17;02;02
Thomas:
In the same way, you want to practice. Just like doctors have a practice. They call it a practice because they're practicing. At least, that's what the doctors I talk to you like to say. But in the same way, you don't want to be learning in the middle of a hack-- a hacker attack or an incident, a security incident.

00;17;03;04 - 00;17;25;16
So I like to tell people-- you know, parents, sometimes, people who are new to the concept of the cyber range in cybersecurity, teaching in cybersecurity, are afraid and dismayed that-- why are you teaching kids how to hack? Oh my gosh, that's terrible. No, first of all, we cover ethics. We talk about what you should and shouldn't be doing, what's acceptable, unacceptable.

00;17;25;22 - 00;17;52;21
And then we get into the hacker tools in the same way that a football team has to learn both offense and defense to play the full game, to be a good team. Right? And just like I like to tell kids, Harry Potter, the Defense Against the Dark Arts class, they take that class to learn the bad tools so that the kids can learn to defend and take care of their own systems in the cyber range.

00;17;52;24 - 00;18;00;14
The term range, of course, is a safe place to play with dangerous things. So that's just the environment in which we do it.

00;18;00;14 - 00;18;20;02
Jen:
And talking about the cyber range, I know this month that the Virginia cyber range is hosting the Commonwealth Cyber Cup, which is a CTF challenge that's really just available to Virginia schools and a lot of kids, I'm sure, and maybe teachers are like, Wow, this is cool. Why can't the other states compete?

00;18;21;08 - 00;18;46;24
Thomas:
Right, right. Well, in this specific case, the Virginia Cyber Range was brought into existence through the Virginia legislature, using Virginia taxpayers' money. So that's the main reason. But after we had launched back in back in 2016 and became very popular in 2017, '18, we had a lot of requests. "Hey, can you guys open this up to other people?"

00;18;46;24 - 00;19;10;28
Like, no, but we got the authorization to create the U.S. Cyber Range, which is a separate 501c3 nonprofit that allows other states to come on board. But they have to pay. But since we're nonprofit,

it’s pay just to break even, basically. So we're not making a profit on that and then they can get accounts on the U.S. Cyber Range.

00;19;11;23 - 00;19;26;22
Jen:
We talked a while back about uncovering vulnerable systems on a network and you mentioned the shodan.io and finding something on the printer in your office. Could you explain what that tool is and what was happening with your printer?

00;19;27;25 - 00;19;50;05
Thomas:
So I knew about Shodan. Shodan is an OSINT tool that basically does a lot of the constant security scanning of the internet for you. So now, like any tool can be used for good or for evil, it's all how you use it. So the same thing here. Shodan scans the internet looking for vulnerable systems.

00;19;51;14 - 00;20;13;19
I saw a printer spewing out reams and reams of paper every week and I'm like, What's going on? I looked at the paper and I saw, Oh, look, this is an nmap scan. Oh, look, this is an open email proxy scan. This system is being scanned for you know, all the time.

00;20;13;19 - 00;20;30;22
So I said, I wonder if it's on Shodan. So I go to Shodan and sure enough, our printer, Virginia Tech printer is on Shodan. Because Virginia Tech, by the way, we’re called a research network, we’re wide open. There aren't any firewalls, really. So when you turn on your desktop, you better have that thing locked down because you're going to start getting scanned.

00;20;31;19 - 00;20;50;22
Speaker 1
So that's part of it. And I respect that. So I saw that it was on Shodan. I'm like, Oh my gosh, our printer’s on Shodan. So I asked for administrative access to that printer and went in there and locked down its own firewall so that it wouldn't allow all these scans and stuff. So, yeah, that was fun.

00;20;51;05 - 00;20;58;20
Jen:
So what other types of maybe common hardware or software vulnerabilities have you uncovered? Would you say that was like a vulnerability?

00;20;59;10 - 00;21;26;27
Thomas:
It was not a vulnerability, it was a configuration error. So vulnerability would actually be, you know, a known or unknown piece of code that is vulnerable to being exploited or attacked and leveraged. So I'm sure with the age of that printer, because it's an IoT device and no one patches IoT-- I like to tell people, the S in IoT stands for security.

00;21;27;29 - 00;21;50;04
So people put printers online and they don't think about them again. They put their routers online. They don't think about them again. So I know it hadn't been patched. And so chances are—I know it's running embedded Linux. There's most probably a vulnerability in there. So you definitely want to lock

those things down. If you can't patch them, you should, you know, annually, at least annually, check for firmware updates and stuff like that.

00;21;50;18 - 00;22;16;05
Besides the printer, which was a configuration issue, when I worked for both the DOD and Rackspace-- I actually worked for Rackspace for 17 years, which is a major Internet hoster or were until recently. We would have, you know, thousands and thousands of hosts, servers and data centers all over the world. And we'd have several thousand customers running Web servers and DNS servers and things like that.

00;22;16;16 - 00;22;35;02
And so we would regularly scan our customers to make sure that they were keeping their stuff safe and because that was their job. And oftentimes they wouldn't. And so one case was we scanned our networks, we saw some unusual traffic, so we scanned our networks for vulnerable DNS servers-- BIND is the DNS server of the Internet.

00;22;35;11 - 00;23;02;10
And so we saw, wow, we’ve got thousands of vulnerable DNS servers, we really need to proactively take care of this for our customers or our networks are going to turn into a hacker playground. And so we sent notifications to customers. And me and a team of other engineers wrote a set of SSH Python automation scripts for scanning and patching each one of those DNS servers.

00;23;02;26 - 00;23;25;03
And so we have to communicate with customers and schedule all this stuff and then separate the ones we're patching now from the ones that we're doing later, and then automate that using a combination of Bash and Python for patching systems. So patching is, of course, one of those essential things, you know, secure passwords, patching, you know, the things you hear over and over.

00;23;25;09 - 00;23;41;01
Those are the most common weak links - other than humans - the most common technological weak links in the chain. And so when other people don't do it, we would have to do it at Rackspace. But we own this network, so we're responsible for everything on the network here at the Cyber Range.

00;23;41;16 - 00;24;00;06
Jen:
Right. I mean, those are the things you should always do, you know, patching - in terms of securing your network. So how does someone listening to this podcast, you know, do what you do at your work, maybe at their home, besides patching different things? How do they make sure their systems are secure?

00;24;00;06 - 00;24;19;11
Thomas:
Before you can secure your systems, you have to know what you have. A good way of doing that is to audit your home network. We teach kids to - once we get them to take our ethics class - we teach them how to scan their own home network using nmap, for example.

00;24;19;11 - 00;24;29;04
So we'll show an nmap scan of your /24 worth of IP space. By the way, if you don't know what /24 is, take some networking classes.

00;24;29;04 - 00;24;30;07
Jen:
You need a networking class. Yes.

00;24;30;15 - 00;24;54;20
Thomas:
Cybersecurity is great, but it's built on top of IT knowledge. So that's operating systems, networks. and general IT knowledge. So have kids go home and run nmap command, you know, boot up Kali, scan their own home network so they can see, Wow, I can see, oh, there's a Blu ray player on my network and my sister's iPad and my parents' laptop.

00;24;54;20 - 00;25;08;13
And what's this strange device? You'll often see things that you have no idea what they are. And so it's very important to first know what's there, and then you can look at each system and make sure it's getting updates. And that it's being patched.

00;25;08;13 - 00;25;19;27
Jen:
What skills do you think you need to be successful, to keep moving forward in the cyber pathway or that make you, you know, just be successful in it in general?

00;25;21;11 - 00;25;43;03
Thomas:
People sometimes introduce me as an expert, but I never introduce myself-- I'm not an expert. I'm always learning. I tell kids, especially, the more-- tell college students, because they're-- "I took this class, I know this." It's like, dude, the more you learn, the dumber you should feel. So it really is because the more you learn, the more you realize you're just scratching the surface.

00;25;43;11 - 00;26;03;12
And so I guess the more surfaces you can scratch, the wider your knowledge pool gets. But you need to go deeper, too. And that's where the intimate knowledge of IT and networking and operating systems are kind of the underpinnings. You can take your Security+ certification, but it's just a bunch of acronyms if you don't know what's really underneath it.

00;26;03;23 - 00;26;26;24
And so knowing what's underneath it is more experience-- more important. I would tell students that are going for interviews, Certs are okay, but it's like one leg of a three-legged stool. It's like, you have certs. Experience is what I look for first. Experience, degree, and certs. If you have all three of those, you're a perfect candidate.

00;26;27;03 - 00;26;42;28
If you have one of them, okay, you can kind of wobble around. If you have two of them, that's better than three. If you have three, then you're rock solid. But that experience should be in, like, you know, set up a home network, you know, set up some Raspberry Pis if you can find them on the market now.

00;26;43;16 - 00;27;04;04

Set up a Linux box. You know, dual boot from Windows and Ubuntu or something. Or make Linux your daily driver operating system so you're in it and learning it. And it's that edgy thing that's, like, “Ooh, I’m afraid of that.” Hey, you can still run Windows in a virtual machine and run your Outlook and other tools.

00;27;04;25 - 00;27;21;13
So jump into it. I remember my first day at Rackspace, they gave me-- “you want to run Red Hat Linux or you want to run Windows 98?” I'm like, Oh, I can probably be more productive on Windows 98. I'll take 98. And I put the CD-ROM in and pulled it out at the wrong time.

00;27;21;13 - 00;27;39;26
This was back when they had CDs, right? And I pulled it out and I broke the disc in half. And I was like, Oh, no. And that was very kind of foreshadowing of my future that I was done with Windows, basically. I was like, you know what? It’s time for me to jump into Linux, anyway. And they were like, “That was our only install media. So you're running Red Hat.” And I was like, that's fine.

00;27;40;11 - 00;27;52;22
And that was really telling for me. That was really good for me because it forced me to jump into what I really wanted to do anyway, which was get away from the Windows world. No ding on windows, but, you know, it kind of sucks.

00;27;52;23 - 00;28;04;13
Jen:
Yeah, I'm going to, you know, definitely snap and clap about running Linux and trying Linux, though, because I feel like that's definitely helped me. I hope we will evangelize future generations to try the same thing.

00;28;07;20 - 00;28;10;00
Thomas:
I’ll wave that flag on occasion, yeah.

00;28;11;09 - 00;28;35;16
Jen:
Thank you so much for your time, Thomas. We had so much fun talking today

Thomas:
Sure, Jen.

Jen:
That's our show! Thanks so much for being a part of our community. We can't wait to see how you do with this week's episode Challenge. Go to the Cyber Chats podcast page on our website at https://www.cryptologicfoundation.org to find this week's challenge, submit a question, and join our focus group to help improve the podcast.

00;28;36;17 - 00;29;02;27
You can watch more of this podcast on YouTube. Be sure to like and subscribe to hear more. And check out the show notes for more details and links. This podcast is made possible by the Chilton Foundation.