#InfoSec N00bs

Do I REALLY need to learn those PenTesting tools?

3: What happened to updates?

4: Red vs. Blue

5: Why can't we all just get along?

6: Do I REALLY need to learn [whichever] PenTesting Tool?

What happened to updates?

Well, 2020 was a crazy year, right? But seriously, things got all sorts of crazy for me…to the point that I haven't actually been applying for InfoSec jobs lately. It's been all that I can do to stay up to date. The day-job, which is a necessity for us, has been really big into training and the like lately, which I really, really can't object to. Besides, it's fun!

That being said, are updates to this something that will be happening in the future?

Maybe? I hope so? I have a lot on my plate at this point, and I'm going through and refreshing a lot of old skills that I let fall by the wayside. If I can remember, I may chronicle some of that through new releases of InfoSec Noobs. I let a lot of my programming and scripting skills lag behind as a I focused more on networking hardware and software, and overall security concepts.

Imagine my (lack of) surprise when I realized that these skills would not only be valuable, but would let me understand InfoSec more fully if I could get them back up to speed.

And so that's one of the main things that I'm doing at this point. I haven't built web pages or anything resembling a web app for years, and so now I'm returning to the good old days of HTML, CSS, and (yech) JavaScript. And Python. Oh, and I think that I'll learn Go. So…yeah. There's a lot going on.

Red vs. Blue

It's one of the first things that a lot of us hear: "Red or Blue team?" Is this something so incredibly important that we have to make a choice "right out of the box," so to speak? Short answer: no. Long answer: no, but…

So these labels are more intended to notate what sort of work that you do. One thing that many of the people who are so intent on the "teams" fail to grasp, however, is that there's only one team. And it's essentially purple, to extend the metaphor.

Blue team activities are typically considered defensive activities. You'll find a lot of people labelling it the "boring" side of InfoSec. Of course, DFIR and incident response falls under this "Blue Team" heading just as easily as the policy and procedures bunch.

Red team activities are considered offensive activities. This includes active and passive testing of security on sites and applications, and really anywhere else. Done legally, this is tightly bounded by an inflexible scope that is set ahead of time. Done illegally, this is what most Blue Team groups attempt to prevent. The thing is…the Red Teamers generate the data that the Blue Teamers use to update defenses and re-write those policies and procedures. By the same token, Red Teamers need to study what the Blue Team is doing to be able to work out a way of circumventing it.

Both groups are 100% necessary. Don't pay so much attention to labels. Learn anything that is available. Anything can be useful, but anything under either of these labels is something that will be immediately and directly useful to you in your InfoSec career.

Why Can't We All Just Get Along?

If you have followed InfoSec personalities and trends for long enough, you will have noticed a (or several) disturbing trends. People get mad at one another. Like, really, REALLY, mad. Sometimes unethical things (like doxing) transpire. Other times, there's just hurt feelings and rough words. Still, these people were friends last week...why does this keep happening?

Think of it this way: This is a large profession. There are massive differences in the way that various people see things. Some people come from a corporate background, others are virtually stereotypical iconoclasts. Add to that the fact that most people in this field are either used to being the smartest person in the room...or else thinks that they are. We tend to think that we're right. Probably moreso than a lot of other groups.

Add to this fun stew of ours a heaping helping of anxiety and imposter syndrome, meaning that things typically get pushed under the rug until they explode. This isn't everyone, of course, but it's probably descriptive of more than a few of the people that I've met. And me, of course.

That all being said, I haven't found a community that, as a whole, is more welcoming or inclusive than the InfoSec community. It's big enough that the fringes are sort of dark and weird, but it's varied and changing all of the time.

Do I REALLY need to learn [whichever] PenTesting Tool?

I've asked this question. A lot. Like, a WHOLE lot. Why? Well, I wanted to be "Blue Team." (And now we see the theme of this #InfoSec N00bs come together…) I wanted to play with networks. I wanted to get into DFIR and yes, even policy and procedures. I enjoy training, and all of the other typically "blue team" activities. I actually look forward to being a SOC/NOC Analyst.

So naturally, I didn't learn these tools, like BurpSuite. (This is something else that I'm working on.) One of the places that I have looked at working uses BurpSuite and similar tools a lot. All of them. Evaluating a client in a quick and dirty way is integral to the workflow in lots of places. Sure, you're "Blue Team" or whatever, but you aren't expected to be as proficient as the hardcore console jockeys. You're there to check for obvious things, and then make sure that the main bases are covered. Your friends across the aisle on Red will let you know what else needs to be worked out. But you can get a start without waiting for them…which typically takes quite a while.

So do you need to learn that pentesting tool? If you are asking the question, the question is likely yes. The absolute worst case is that you learn something new that you rarely, if ever, use. I consider that a good day. In the best case, you learn something new that you'll use all the time, and possibly a new skill that may change or expand your interests.

You'll likely find that I will rarely, if ever, discourage an opportunity for learning. It's something that I've preached all of my life, and all of my son's life. He's only just now learning that I really mean it: learn everything that you can. It's all useful somewhere.

Credits

Brian Petty
bwpetty@protonmail.com
@BPetty_InfoSec

All pictures and images are royalty and attribution free, found on the site https://pixabay.com.