April 2023 was my Crossing the Rubicon, the moment that changed my life forever. The journey of obtaining the PNPT. Invited to come out and volunteer at HackSpace Con, it was a 10 ½ hour drive down to the Kennedy Space Center in Florida. I had the honor of meeting Heath Adams and picking his brain for a while. I really wanted to know in his opinion what someone with no experience should do to get started.

Armed with the information that he passed on to me, I got to work. It took me four attempts. After not crushing the 1st attempt. I was a little deflated, but I knew I had to go at it again, so I went back to the drawing board, back to the material, back to the basics. I was pumped up and ready for the 2nd attempt, or so I thought. I failed the 2nd and the 3rd attempt. No more PTO, exhausted from taking the 2nd attempt on thanksgiving break, then immediately taking the 3rd attempt right after. Dealing with the entire house being sick and at the same time still going to work left me exhausted. I had one more shot at this before the closing of this year, which only allotted me the night of Friday after work and all day Saturday to complete the lab environment from start to finish. I paid the retake fee and got to work.

The most valuable thing I learned the fourth time around was something that was talked about many times, yet should be truly embodied. Methodology, one must really ask themselves what is my methodology? Methodology is what allowed me to capitalize with less time then on my first three attempts with the maximum allotted time on my end. The PNPT is a monster, it’s made specifically for you to think like a hacker, it is in no way a CTF. It took three attempts to break me of this mindset.

Open Source Intelligence (OSINT), a lot of people have got lost down this rabbit hole, and many more will continue to. Understanding that goal of the OSINT material is to understand that tactics will change, tools will break, yet the process or the **methodology is the same**. Enumeration is key, drill down, once you have what you need then go for it.

Okay we made it in, it’s easy to feel like we have all the time in the world. We don’t, this is a snapshot in time, that is why we go after Low-Hanging-Fruit (LHF). It’s easy to go down rabbit holes at this point. Just remember everything you need is in the course material, I will advise to start embracing a **metadata mindset**. The data is all there but, it is up to you to really understand it and expound upon any gaps that you might have that could affect you from truly digesting the material.

The metadata mindset was something that came to me after compromising the Domain Controller. It was that moment I realized I did it, I now owned the keys to the castle. It was euphoric and yet terrifying, this is how easy it is to gain remote code execution. Yet the ability to test for these common attack vectors, and assist companies with mitigating or atleast decreasing their attack surface started to become more of a moral fight then just another job.

After the final 44 page report was submitted I then had to pick a time to do the debrief. This was a 15 min scoped call. To explain findings, remediation, and recommendations. For anyone who is looking to really understand the pentest process from start to finish, I highly recommend going for the PJPT and PNPT.

Thank you for the opportunity and allowing me to participate by being an early adopter of PJPT and proud PNPT certificate holder. Special thanks to everyone at **TCM Security** for the amazing experience.