Greetings all! My name is Joseph Clay. I am 27 years old. I am a professional Penetration Tester. I am passionate about IT and have always been interested in learning about devices, networks, and other gadgets. I like to think outside of the box. I prefer to not even be trapped in a box, ideally.

A career in cybersecurity has been a dream of mine since the first time my iPod was hacked, back when I was 15 years old. I used to jailbreak and root all my mobile devices, and I grew to understand a lot about IT from these personal experiences. For as long as I can remember, I have been taking things apart and putting them back together to learn how they work. Learning how things function is one of my greatest skills.

I have an adventurous soul and love to explore things I’ve never encountered before. Technology is fascinating and it has captivated me since I played Carmen Sandiego on my first computer. I remember my first laptop. It was a Compaq Presario with Windows XP SP2 installed.

My machine of choice now differs quite a bit. I usually prefer a machine with a dual boot of Windows and Linux, and on the Windows partition, I have to have some kind of Virtual Machine manager. I use both VirtualBox and VMWare quite often. Kali Linux is my distribution of choice for all the fun stuff.

My love for technology has only grown through the years. I tried to move into other avenues in life because I thought the deeper concepts in tech would elude me. My educational background is in Psychology because at one point in my life I was planning to become a counselor. I have a BA in Psychology, and even completed the first semester of graduate school for clinical mental health counseling. I believe this understanding of the human psyche enhances my ability to dive into the mindset of hackers.

I lost the passion for counseling, but I never lost my love for IT and gadgets. Regardless of what I am doing in my personal life and professional life, my fascination with and appreciation for technology always remains. I tried my hand at working a trade after deciding counseling was not for me. Locksmithing seemed like a noble and lucrative venture. I became an apprentice locksmith and enjoyed what I was doing; I mean, I got to legally break into cars, businesses, and homes. That was awesome!

The long work hours on-call with no free time is what finally caused me to look at my life and reassess whether I wanted to continue locksmithing. Not only was I mentally exhausted; I was also physically drained. Locksmithing requires a lot of manual labor. I didn’t think my knees would make it until I was ready to retire. This caused me to look back at things I enjoy doing and try to decide on a suitable career path.

Searching deep, I realized that no matter what field I was in, technology would be a dominant force in the coming years. I decided to go all-out and started studying web development on my own. I started by refreshing myself on HTML and CSS. Right as I was transitioning into learning Javascript, I began to narrow down fields that interested me in IT. Cybersecurity, and specifically, penetration testing checked all my boxes.

I would get to break into things legally again, but I wouldn’t be physically exerting myself all the time. I could also study material that interests me and be faced with an ever-changing industry. The prospect of continual growth and learning, as well as the team spirit and challenges present in the security industry, called out to me. I immediately began searching for programs, degrees, and certifications I could obtain to further my knowledge.

Due to working full-time in retail at this point, I opted for a Bootcamp experience. I found a part-time Bootcamp at UNC Charlotte for Cybersecurity. The program boasted many topics relevant to the security sphere today, as well as training for the Security+ exam. This seemed like a great path to head down, so I threw myself into it head-first.

I started the UNC Charlotte Cybersecurity Bootcamp in September of 2019, put in countless hours of self-study and work on assignments, in addition to the tri-weekly classes. I made it out of the program with my certificate of completion in February of 2020 and a lifelong passion for security. I applied for several positions throughout this journey, and finally got a bite with a company for the position of NOC Technician. Networking was one of the areas in the program that I learned I had room to improve in, so I jumped at the chance to challenge myself and solidify my knowledge in this discipline.

I started working as a NOC tech in January of 2020, and I was over the moon. I finally made it into my first role in IT! My second role came a few months later in the form of a part-time position. Seeing how well I worked with others and how willing I was to help my classmates out in the Cybersecurity program, my professor recommended me for a TA position. I applied, interviewed, and was offered a job as a TA for the same Cybersecurity Bootcamp I completed.

Working a full-time and a part-time job can be tough, but I managed it well for a month. Then, another opportunity struck when one of the other TAs in my class told me that he worked as a tutor for the bootcamp, and they were looking for more tutors. I applied for this position as well and was offered the job. It had flexible hours, and I could determine my own schedule.

I was working my fingers to the bone and gave up much of my free time during this period of my life. It was a chance to dive into new technologies headfirst and focus on self-study even more. I spent my time studying for Security+ certification, setting up a VPN with a friend so we could practice hacking together, and studying Python programming.

It was in October of 2020 that another opportunity presented itself. A recruiter reached out to me on behalf of a company, looking for a passionate individual interested in hacking, cybersecurity, and education. The role he was trying to fill was for an information security engineer on the content development team. Researching the company, I stumbled upon Project Ares, which is the platform for which content development builds scenarios. I applied, interviewed, and secured the role.

I have had to revise this document many times over as I am moving much more quickly through the world of IT and closer to my goals every day. I was presented with an opportunity to interview for a penetration tester position just shy of a year after accepting the information security role. Thanks to all the studying done in my free time, I felt ready to attempt to land my dream job of penetration tester. Sadly, I was not offered this position, but I viewed it as a learning experience and threw myself into studying even harder.

I referred to questions I was asked in the interview to determine the path I should take in my studies. This process showed me I had a lot to learn about Windows Active Directory, so I enrolled in a course provided by TCM Security called Practical Ethical Hacking. This course emphasizes the importance of a penetration testing methodology as well as the importance of Active Directory knowledge. I learned that Active Directory makes up a huge portion of the enterprise infrastructure, so it became imperative that I focus on this skill gap.

I went through the course which taught me how to set up and Active Directory environment in my personal home lab. I began practicing techniques for compromising Active Directory and took detailed notes along the way. I was presented with another opportunity to interview for a penetration tester position at a new company about a month after the initial interview where my application was denied.

This time I knew I was ready. The interviewers agreed and I started working here about a month later. It was an amazing experience to land my dream job, knowing full-well I had earned it. I knew I was only going to continue to learn and grow from here. I accepted the offer and started my first job as a penetration tester on September 1st, 2021, roughly 2 years after I started the Cybersecurity Bootcamp program back in 2019. Moving from no experience in IT to penetration tester in two years’ time is no easy feat, but I’m a very dedicated individual.

I have been in this position for three months now at the time of this document’s revision. The team lead that interviewed me left about 3 weeks after I started, and I had to step up to the plate. I decided to pursue TCM Security’s Practical Network Penetration Tester certification. Leveraging the Practical Ethical Hacking course, as well as the External Pentest Playbook and Open-Source Intelligence Fundamentals courses by TCM Security, I began to study for the PNPT exam.

I studied for about 2 weeks in my free time to fill in any gaps I had in knowledge that may pose a challenge for me on this exam. I registered for the exam in October of 2021, and ultimately passed. This exam tested abilities in external pentesting, pivoting into an internal network from the outside, compromising an Active Directory domain, establishing persistence in the internal network, writing a detailed report of all findings, and presenting the report to an industry professional.

Passing the PNPT exam and adding it to my list of certifications inspired confidence. I knew I could handle anything this new job could throw at me. I had not performed too much pentesting before my team lead left, and he did not have the time to train me in the way I was expecting, so I decided to train myself, and to learn by doing. I threw myself into the work, began performing testing as much as my coworker. We divided the load evenly and managed all the tasks assigned to our team, since it was just him and I left on the team.

I even began communicating with our client’s during kickoff calls, writing reports, and presenting the findings in the reports for our report review calls. November came around and I even led an entire internal penetration test on my own, from start to finish.

It’s been a long journey so far for me in a little more than 2 years since coming from working in a vape shop and starting a cybersecurity bootcamp. Now my career is Cybersecurity, and I’m becoming a better penetration tester every day. Responsibilities keep getting piled onto me, and I’m managing them all well and delivering quality results to our customers. I even took some time to revamp the process we used for connecting to the machines we send customers to add to their network for internal testing.

I know I add value to my team, all my teammates agree with that. I am no longer a bootcamp student. I am no longer a cybersecurity engineer. I am no longer even simply a junior penetration tester. I am a penetration tester on the way to becoming a seasoned veteran, and I am learning and growing more by the day. Keep your systems locked down because I am coming for you (if you hire my company to test your infrastructure)!