**Emmett Rushin**

[emmettrushin@gmail.com](mailto:emmettrushin@gmail.com)

919-500-1530

Looking to apply experience in a cybersecurity entry-level role such as cyber security analyst or malware forensics and reverse engineering. Open to obtaining a security clearance and supporting the public and private sector.

**Skills**

• Linux (6 years)

o I started learning Linux due to the terminal. It started as trying to learn as much as I could about the language and how it differs from Windows. My day to day operating system is Ubuntu so the familiarity comes from use.

• Metasploit (5 years)

o Implemented Metasploit as a tool to practice with. It offered a lot of different vulnerabilities and I wanted to learn how they affected different operating systems and how I could prevent them. I have also practiced with Metasploitable to have a lab to practice on. I practice daily with different scenarios using Metasploit.

• Microsoft Suite (7 years)

o Word is a program that has been used for many years now. It is my go-to word processer. Excel is also the spreadsheet program I choose and write in. I have used this suite through middle school, high school, and college.

• OWASP (5 years)

o OSWASP was something I was intrigued to learn due to the different web applications and exploits that were out there. I wanted to learn how to implement them along with how to protect against them. I implement different laps that incorporate OWASP to remain on top of the technology and changing exploits/vulnerabilities.

• Nessus (6 years)

o Started with Nessus because one of my mentors brought to my attention that I should start learning it. I feel it is very well-rounded and versatile. I have used it to practice vulnerability scans and how to report my findings. Nessus is my go-to when it comes to web-application scans and reporting.

• Reaver (2 years)

o I started using Reaver when I started learning cyber security and WPS attacks. I have used it personally when I have set up my own router to attack and see how a successful WPS attack looks. I set up laps weekly to practice WPS and wireless attacks.

• Arimitage (5 years)

o Armitage was also a program that was recommended to me by my mentor. I’ve used it as a suite that implements a lot of what Metasploit has to offer but provides a reporting suite from within. I find it very handy as a red team tool and use it during my labs weekly.

• Hydra (1 year)

o I used Hydra to practice brute force attacks. Especially when using wordlists containing passwords and usernames. Found it useful to use when attacking SSH as well.

• Burpsuite (1 year)

o Burpsuite is a program I just started learning to ease the ability for web application attacks. MITM is very easy to use and implement using this software.

• OS X (2 years)

o OS X is fairly new to me. I got into it because the terminal in OS X is one that I was familiar with in Linux. The memory management both in Linux and OS X (Unix) is heavily preferred over the memory management within Windows. My main laptop is a MacBook Pro so the familiarity with OS X only grows.

**Work Experience**

Concrete Technician / Data Entry

Froehling & Robertson, Inc.

Richmond, Virginia

May 2018 to April 2020

* Tested concrete and soils per regulation
* Assisted with data entry when needed

Server

Hometeam Grill

Richmond, Virginia

October 2017 to December 2017

* Accurately memorized a menu to provide necessary details for guest inquiries and kept up to date with changing menu trends
* Provided a great experience for each guest while constantly improving my service method

Shift Leader

Chili’s Bar and Grill

Holly Springs, North Carolina; Apex, North Carolina; Morrisville, North Carolina

October 2013 to August 2017

* Offered availability to substitute for co-workers where support was needed
* Took initiative to further serve with managerial training
* Kept a cool head under stressful situations to encourage team morale

Server Assembly

Dell Computer

January 2012 to May 2012

* Managed accuracy of all products being systematized and departing during active shifts
* Assisted in the support of building servers when the opportunity presented itself

**Education**

High School Diploma

2010

Fuquay Varina High School

Studied for an Associate in General Studies

Landmark College - Putney, VT

**Certifications**

Comptia Security+ (Pending)

**Additional Information**

* Experience in customer-relations
* Team player with the willingness to lead
* Problem solving skills
* Able to perform all tasks assigned promptly even under pressure
* Strives to keep up to date on all company products and procedures
* Effective sense of urgency
* Willing to learn and cross-train in other job positions and duties
* Technology Skills
* Troubleshooting and PC repair
* Experience with wireless vulnerability testing, server vulnerability and LAN/computer vulnerability
* Teacher assistant in high school technology class
  + Assisted students with technology skills on a daily basis
  + Asked by Administration to penetrate school network for vulnerability and resolution of security-related issues
  + Proved to the technology teacher that his password protected HDD was exploitable
  + 8 years' experience building/diagnosing computers
  + Rebuilding an unbootable laptop
  + Diagnosing, repairing, and maintaining computers for various family members and family friends