**SUMMARY OF EXPERIENCE**

After graduating high school, I worked as a nail technician for several years without a clear idea of what I wanted to pursue in college. Instead, I decided to work full-time and live with relatives to save money. During that time, I purchased my first personal computer, which led to my interest in cybersecurity. I pursued self-study using many different resources such as OverTheWire, OpenSecurityTraining, TryHackMe, and HackTheBox, eventually ranking in the top 1% on TryHackMe and the top 500 globally on HackTheBox. Since then, I have earned several industry certifications and am currently pursuing a Bachelor's degree in cybersecurity. I'm passionate about continuous learning and am looking for a work environment that will allow me to contribute to the field in a meaningful way and grow as a cybersecurity professional.

**EDUCATION & CERTIFICATIONS**

**Western Governors University** December 2022 – (expected) November 2023  
***Bachelor’s of Science, Cybersecurity and Information Assurance***

**eCPPTv2** eLearnSecurity June 2022  
***eLearnSecurity Certified Professional Penetration Tester***

**Security+** CompTIA March 2022

**PROFESSIONAL EXPERIENCE**

**Huntr.dev**, Remote June 2022 – December 2022  
***Freelance Security Researcher***  
• Performed white-box security testing on open-source software  
• Performed code review on php, golang and c# applications  
• Discovered and reported OWASP Top 10 vulnerabilities  
• Performed dynamic analysis on command-line utilities

**Modern Nails of Tampa**, 10067 W Hillsborough Ave May 2018 – March 2022  
Nail Technician

**COMPUTER LANGUAGES AND SKILLS**

**Languages**  
• Limited but improving: Bash, Golang, Python, and Powershell  
• I have reverse engineered applications written in C using a working knowledge of x86 ASM

**Skills**• Web application testing and OWASP Top 10 2021  
• Network testing and exploitation  
• Custom exploit development  
• Routing, pivoting and tunneling  
• Windows and Linux privilege escalation  
• Fuzzing with coverage-guided fuzzers such as AFL++

**PROJECTS AND OTHER SECURITY EXPERIENCE**

**Web Presence**   
• **Website**: <https://eli2k.com>  
• **Github**: <https://github.com/Eli2k765>  
• **HackTheBox:** [Eli2k765](https://app.hackthebox.com/profile/688988)  
• **Tryhackme**: <https://tryhackme.com/p/Eli2k765>

**OS and Tools**  
• **OS**: Linux(Arch, Kali, NixOS, Android), Windows(XP, 7, 10, 11)  
• **Network exploitation tools**: Metasploit, nmap, dig, nslookup  
• **Web tools**: Burp Suite, Owasp ZAP, sqlmap, gobuster, dirbuster, feroxbuster, httprobe, assetfinder, waybackurls, and amass  
• **Tunneling tools:** proxychains-ng, chisel, and sshuttle  
• **Reversing tools**: gdb-peda, Ghidra, Immunity, pwntools, AFL++, and valgrind  
• **Virtualization tools**: VirtualBox, VMWare, WSL, Android Studio, Genymotion  
• **and more**...

**CVEs**  
• [**CVE-2022-3135**](https://huntr.dev/bounties/68331124-620d-48bc-a8fa-cd947b26270a/) - Null Dereference in vim

**Additional Certs**  
• **CompTIA**: A+, Network+, Project+   
• **ITIL**: ITILv4 Foundations

**Certs In-Progress**  
• **Portswigger:** Burp Suite Certified Practitioner   
• **Offensive Security**: Offensive Security Certified Expert