Kevin Medina

kevinmedina26@live.com | Los Angeles, CA | (323)360-7127

SUMMARY: Recently obtained a Master of Computer Science with a Cybersecurity concentration due to influence from the US Air Force while in a co-op PAQ program. Proficient in network security using tools such as WireShark, Nessus, and Nmap. Intermediate in vulnerability analysis and reverse engineering using tools such as Burp Suite for web applications, Ghidra and IDAPro for compiled binary programs. Beginner but quickly learning cloud infrastructure using AWS and GCP. Seeking cybersecurity focused role to leverage my academic experience to apply frameworks such as NIST, Cyber Kill Chain, and OWASP.

EDUCATION

California State Polytechnic University, Pomona, Pomona, CA June 2021

Bachelor of Science in Aerospace Engineering, Materials Engineering Minor

Arizona State University, Phoenix, AZ May 2024

Master of Computer Science, Cybersecurity Concentration

EXPERIENCE

Nuclear Surety Intern Engineer, **US Air Force Civilian Service**– Hill AFB, Utah Sep 2021 – Jan 2023

- Certification at Engineer I Level – DAU; Required Secret Clearance
- Understand the Minuteman III ICBM system and how updating it is completed through various companies' work
- Assisted in secure management and certification of updating of critical systems components; Collaborated on risk management processes aligned with federal cybersecurity standards

SOFTWARE PROJECTS

- **Cyber Security –** Became familiar with Splunk SIEM, vulnerability scanners such as Nessus; created a simple IDS on a virtualized network that searched for specific IP addresses within external requests all by using VMs, Docker, the command line terminal, Bash, and Python
- **SQL Data Visualization** – Used old United States Consensus data, SQLite and matplotlib with Python, and Jupyter Notebook IDE to create an advertisement campaign for a community college based on data graphics created from the data; the data graphics had to be cleaned up visually to accurately create an advertisement story
- **Reverse Engineering** – Utilized Ghidra and IDAPro, with C/C++ to reverse engineer compiled binary programs to attempt to crash them; used GDB to debug and step through the binary programs to read, understand, and manipulate the assembly code to find exact memory addresses that stored desired functions/objects that had to be extracted to complete a capture the flag style project; created a string fuzzer in C++ that crashed programs that used input from the command line in Linux and Windows Powershell terminals
- **Network System LAN –** Used Docker and Virtual Machines(Linux kali and Linux ubuntu) to simulate a LAN and customize the default gateway to only accept certain protocols(TCP only from a specified IP address for security), used Wireshark to inspect ARP packets to verify spoofing attack within the LAN, performed network troubleshooting by using the command line tools such as netstat, nmap, ping, hping3, and traceroute

TECHNICAL SKILLS

- *Programming Language*s: Proficient in Python, Bash shell scripting, C++ and C; Familiar with C#, Golang, Solidity, and SQLite; Exposed to JavaScript
- *IDEs*: Visual Studio Code, PyCharm, Jupyter Notebook, Remix, and Linux Ubuntu command line terminal
- *Software*: Proficient with Microsoft Word/Excel/PowerPoint, Linux Ubuntu Virtual Machines, Oracle VM; Intermediate with MATLAB, Ghidra, gdb debugger, .NET; Docker; Beginner with Android Studio, Burp Suite
- *Writing*: Able to articulate and communicate ideas at the graduate level using IEEE standardized reports
- *Cloud Software*: Beginner in AWS and GCP, basic understanding of Infrastructure as code

Skills & Traits

- Familiarity with NIST RMF, SOC 2 compliance, HIPAA compliance, and ISO frameworks; MITR ATT&CK and Cyber Kill Chain models
- Understanding of DevOps using git for software project management from the terminal
- Knowledge of OWASP and MITR CVEs and how to use it to research information on latest top vulnerabilities
- Knowledge of commonly used protocols such as DNS, TCP/IP, UDP, etc
- Excellent writing skills due to researching and writing multiple IEEE reports on technical software topics
- Familiarity with federal government risk management processes
- Technically independent – able to quickly research, learn and utilize a new technical concept
- Bilingual in Spanish
- Interested in and used (ethically) hacking tools such as a Flipper Zero, Rubber Ducky, and software defined radio