

Luke Taliercio

(571)-585-6028 | lukert@vt.edu | [linkedin.com/in/luke-taliercio](https://www.linkedin.com/in/luke-taliercio) | Vienna, VA

EDUCATION

Virginia Tech

August 2019 – May 2023

B.S Computer Science, Minor in Mathematics (In-major GPA: 3.72)

Blacksburg, VA

Coursework: Data Structures & Algorithms, Operating Systems, Computer Architecture, Cryptography,
Principles of Computer Security, Quantum Computing, Network Architecture & Programming

EXPERIENCE

Cyber Systems Engineering, Intern

May 2022 – Present

Northrop Grumman, Space Systems

Warp Drive, VA

- Co-developed a vulnerability identification program that queries the NVD REST API to create a database of at-risk products with corresponding CVE records
- Used Fortify to conduct static code analysis to identify and remedy vulnerabilities
- Created shell scripts to automate 75% of the Fortify scanning pipeline

Undergraduate Research Assistant

October 2021 – June 2022

VT Hume Center for National Security and Technology

Blacksburg, VA

- Mentored a team of 5 members in the creation of PowerShell scripts to remotely collect information from Windows-based systems and successfully presented our work at the Hume research symposium
- Designed a command line interface from which the scripts were remotely deployed
- Incorporated Elasticsearch and Kibana dashboards to correlate and display the information collected

Incident Response Analyst, Intern

May 2021 – August 2021

Leidos

Gaithersburg, MD

- Tuned a set of Suricata rules related to WannaCry ransomware to reduce the false positive rate by over 90%
- Analyzed malware samples using dynamic and static analysis to build out detection and prevention rules
- Authored a set of fully scalable API health checks that would alert on failure of vital scanning/search API's, resulting in roughly a 70% reduction in the need for re-scanning
- Created and modified Suricata and YARA signatures as well as Splunk alerts to detect malicious activity in various stages of the Cyber Kill Chain

PROJECTS/EXPERIENCE

Rubber Ducky

- Created a "Rubbery Ducky" device from scratch capable of rapid keystroke injection attacks, disguised as a harmless USB
- Developed and modified code to create various payloads for the Ducky, one of which included a reverse shell capable of discretely executing in 3 seconds

Deltamath.com web app pentesting

- Used Burp Suite to discover a vulnerability in deltamath.com that would result in the evaluation of any answer to return correct
- Analyzed JavaScript code in browser requests to determine that the site was performing client-side validation and successfully demonstrated an exploit to this vulnerability

ACCOMPLISHMENTS/AWARDS

- **Cybercorps SFS scholarship:** Three-year full tuition scholarship along with an annual \$30,000 stipend
- **2nd place** in the Lockheed Martin CTF invitational
- **2x Platinum**(highest) tier competitor in the CyberPatriots competition with a focus on Linux system hardening

TECHNICAL SKILLS

Languages: Java, Python, C, Powershell, Bash, Assembly

Tools: Burp Suite, WireShark, Nmap, Cuckoo, Suricata, Splunk, Hashcat, Google Cloud Platform, Metasploit, Git