Thanh Pham

Security Analyst - SOC Analyst

408-389-9606 | jonathanphamw22@gmail.com |

Graduating from FullStack Academy's CyberSecurity Analyst program equipped me with strong skills and interest in security infrastructure that allow for excellent identification and analysis of suspicious events. Extensive experience using a range of security tools has honed my skills in log and packet analysis. The project GoldenFin automated the extraction of SMTP data, IP addresses, images, and HTTP requests from Pcap files using scripting languages and TShark. The desire to remain up-to-date with emerging technologies enables staying current with industry developments.

TECHNICAL SKILLS

Proficient: *Linux, Python, Bash Scripting, Metasploit, Burp Suite, Nmap, OSINT, Snort, Splunk, Wireshark, Firewalls, Tshark*
Knowledgeable: *Powershell, Network Security, SIEM, EDR, IDS/IPS*

Certifications:
CompTIA CySA+ (In Progress - Expected: Feb 2023)
CompTIA Security+ (In Progress - Expected: March 2023)

TECHNICAL PROJECTS

TheGoldenFin | **Script Developer** | Jan/2023.

- Automated the process of extracting useful information such as SMTP data, IP addresses, images, and HTTP requests using the GoldenFin script, making the log and packet analysis process more efficient.
- Used scripting languages like Bash to automate the extraction process and parse data.
- Utilized network protocol analysis tools such as TShark to capture and analyze network packets.
- Used regular expressions for pattern matching and data extraction from packets.

EXPERIENCE

Assembler | Enovix | Fremont CA June/2021 to November/2021

- Assembled over 50 anode lithium-ion batteries per day, contributing to the company's success in the industry with high efficiency and precision.
- Operated laser cutting machines on anode materials to ensure the efficient and accurate production of batteries.
- Operated Vision Measurement Machines on anode materials and separators, ensuring that the products meet quality standards.

Supervisor | Boiling Point Restaurant | San Jose CA December/2021 to current

- Oversaw the activities of restaurant staff, ensuring smooth and efficient operations, and providing a high-quality dining experience for customers.
- Expedited customer orders as needed, resulting in increased customer satisfaction and repeat business.
- Maintained good working relationships with suppliers, resulting in reliable and timely deliveries of high-quality products and cost savings for the restaurant.

EDUCATION

San Jose State University Cyber Bootcamp October/2022 - Jan/2023

Powered by Fullstack Academy |Cybersecurity Analyst Bootcamp

- Three-month immersive program designed to train in advanced red team/blue team skills and use of security toolsFormed a solid foundation of computer knowledge; including Windows OS and Linux OS.
- Mastered common CLI for Linux through Fullstack's CTF challenges.
- Learned Python basics and scripting; Bash scripting and used replit to write Python code, Python scripts, and Bash scripts with given parameters.
- Practiced offensive techniques and how to mitigate these threats using industry blue team tools to align with cybersecurity frameworks such as NIST, ISO-27001 and MITRE ATT&CK.
- Wrote and modified rules for IPS, IDS such as Snort and ACLs for firewalls/routers based on parameters provided.
- Used packet capture tools such as Wireshark and TCPDump to investigate traffic for IOCs (Indicators of Compromise).
- Executed basic incident response procedures and gained familiarity with forensics tools, PCI-DSS and FISMA.
- Performed simulated threat hunting by analyzing logs in the SIEM Splunk
- Gained familiarity with a variety of tools including Snort, Splunk, Wireshark, Burpsuite, Metasploit, Nessus, Nmap.