Taejeong Kim

667-240-6721 | tj11564@gmail.com | linkedin.com/in/taejeong-kim03

Education

University of Maryland College Park, MD
B.S. Information Science *Aug 2022 – May 2026*

Projects

Home Lab SIEM Setup | *Splunk, ELK Stack, Wazuh* 2025

- Installed and configured SIEM tools for centralized log collection and real-time analysis.
- Forwarded logs from host machine, router, and virtual machines for endpoint visibility.
- Built dashboards to detect suspicious activity including brute-force attempts and port scans.

Multithreaded TCP Port Scanner | *Python, Socket Programming, Networking* 2025

- Developed a multithreaded TCP scanner supporting CIDR targets and custom port ranges (1–65535).
- Implemented concurrency with ThreadPoolExecutor to optimize scan performance.
- Integrated service detection and banner grabbing for reconnaissance analysis.
- Generated structured JSON output for automated parsing and reporting.

Network Packet Sniffer & Traffic Analyzer | *Python, Scapy, Network Protocol Analysis* 2026

- Built packet capture tool to classify live traffic across TCP, UDP, DNS, ICMP, and IP protocols.
- Extracted DNS queries and protocol statistics for lightweight anomaly monitoring.
- Identified top source/destination IPs and network flows for behavioral analysis.
- Implemented BPF filtering for targeted inspection of specific traffic types.

Automated Log Threat Detection System | *Python, Regex, SIEM Concepts* 2026

- Built a log analysis tool that parses system and authentication logs to detect suspicious activity patterns.
- Implemented rule-based detection for brute-force attempts, failed logins, and privilege escalation indicators.
- Used pattern matching and statistical thresholds to flag anomalies in login frequency and source IP behavior.
- Generated structured alerts and summaries to simulate lightweight SIEM-style threat monitoring.

Technical Skills

Languages: Python, Java, SQL (MySQL), JavaScript, HTML/CSS, Bash, PowerShell, Git

Security & Networking: Splunk, Sysmon, Nmap, Wireshark, Metasploit, Hydra, Mimikatz, Kali Linux, Packet Tracer

Tools: VSCode, Jupyter Notebook, VirtualBox, Linux CLI

Relevant Coursework

Computer Networking, Database Design, Object-Oriented Programming, Information Security Concepts, Data Structures, Systems Fundamentals

Additional

Languages: Fluent in Korean

Certifications: Studying for Comptia Security+ Exam