Mouli Kesavan

moulikesavan07@gmail.com | https://www.linkedin.com/in/mouli-kesavan | Github

Technical Skills

Operating Systems & Software: Windows, Linux, Mac OS, Active Directory, Microsoft Server, Office 365.
Programming & Tools Python, Bash, C, Metasploit, Burp Suite, Nessus, OWASP ZAP, Wireshark, Nessus, Splunk, Elastic Search, Kibana, Threat Intelligence, Malware Analysis, Digital Forensics, Reverse Engineering
Web Application Security: SQL injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), security testing methodologies
Network Security & Assessment: Vulnerability Assessment, Network Scanning, Risk Assessment, Firewall Configuration, IDS / IPS
Malware Analysis & Reverse Engineering: Ghidra, IDA Pro, Volatility, static and dynamic analysis.
Cybersecurity Frameworks: NIST CSF, ISO 27001, CIS
Soft Skills: Problem-solving, Critical Thinking, Communication, Attention to Detail, Team Collaboration

Experience

IT Systems Analyst SPAN Associates, Bangalore, IN Sep 2019 – Aug 2022

- Managed and implemented internal IT infrastructure projects, enhancing overall architectural team efficiency by 30% through effective software installations, network management, and strategic resource allocation.
- Established and maintained vendor relationships, negotiating software and hardware procurements, resulting in a 15% reduction in overall technology procurement costs.
- Trained and provided ongoing technical support to staff on newly implemented software solutions, significantly improving user proficiency and boosting software adoption rates across the company.
- Developed and implemented a statistical framework to measure IT support performance, achieving a 20% increase in employee satisfaction related to technical support services.
- Led the installation, configuration, and maintenance of computer hardware, including desktops, laptops, printers, and networking equipment, ensuring 100% uptime and minimizing disruptions to architectural project deadlines.

IT Associate Block Educational Office, Bhavani, IN May 2017 – Aug 2018

- Handled Windows updates on 20+ desktop computers, ensuring a secure and consistent IT environment for faculty and administrative staff.
- Linked and configured computer networks, improving overall efficiency in daily administrative tasks.
- Installed and updated educational and office software, reducing downtime by 30%.
- Provided on-demand technical support, resolving software issues and clarifying user doubts to maintain smooth departmental operations.

Projects

SOC lab project on Google Cloud| *ELK, osTicket, Google Cloud*

- Engineered a full-scale SOC lab on Google Cloud Platform, integrating the ELK Stack, Elastic Defend EDR, and osTicket for end-to-end detection, alerting, and automated incident response workflows—emulating real-world threats like SSH/RDP brute force and C2 attacks using Mythic C2.

- Simulated advanced attack scenarios and implemented defense mechanisms, including endpoint isolation, custom detection rules, and threat intelligence validation—achieving real-time mitigation of malware and command-and-control activity across Windows and Linux environments.

False Data Injection Attack Detection Using Federated Deep Learning| *Numpy, CNN, Tensorflow*

- Developed a secure system leveraging Federated Deep Learning to dynamically detect, classify, and mitigate False Data Injection Attacks, enhancing system state estimation and control signal retrieval.

- Conducted performance evaluation of multiple machine learning models, with Random Forest achieving the highest accuracy of 79%, outperforming other algorithms like Logistic Regression, Decision Trees, and Gaussian Naive Bayes.

IoT Security Device Scanner with LLM Integration | *Python, Nmap, NVD, Pyshark, GeminiAI*
- Built a scanner for identifying vulnerabilities in IoT devices in smart home environments.
- Integrated a Large Language Model for customized security advice and natural language interpretation of vulnerability data

Malware Analysis and Decryption Tool Development(Coursework)| *IDA Pro, Ghidra*
- Led a team of 6 to analyze a ransomware sample within 48 hours. Utilized reverse engineering tools (IDA Pro, Ghidra) to identify targeted files and recover the decryption key.
- Developed a decryption tool to restore encrypted files.

Security Assessment of Amazon Alexa Device(Coursework)| *MobSF, JADX, Drozer*
- Discovered 6 medium and 1 low-severity vulnerabilities and developed a detailed report with actionable risk mitigation recommendations.
- Identified and exploited vulnerabilities, including SSL pinning bypass, weak encryption, and insecure network protocols.

Reversed and emulated Raspberry Pi Pico firmware)| *Ghidra, Unicorn, Pyhton*
- Reverse engineered and emulated ARM-based Raspberry Pi Pico firmware using Ghidra and Unicorn, bypassing hardware limitations by rehosting ELF binaries, intercepting I/O functions, and automating memory inspection for successful PIN extraction.
- Developed a full Unicorn-based emulation pipeline in Python, mapping ROM/SRAM regions, implementing memory hooks, and simulating SPI/UART protocols to identify a 4-digit authentication PIN from 10,000 possibilities, achieving firmware rehosting and multiprotocol flag retrieval.

Designing and Configuring a Large University Network)| *Cisco Packet Tracer*
- Designed and configured a scalable multi-campus university network, implementing VLAN segmentation, DHCP services, inter-VLAN routing, and RIPv2 to ensure efficient, isolated, and dynamic IP-based communication across 10+ departments.
- Established inter-campus and cloud connectivity via router and multilayer switch configuration, integrating a cloud-based email server and verifying full network operability through systematic layer-by-layer testing and troubleshooting.

Education

University of Birmingham(NCSC) Birmingham,UK Sep 2024
MSc in Cybersecurity
- *Graduate with Merit*

SRM University Chennai,IN Jul 2023
B.Tech in Computer Science and Engineering
- *Graduate with First Class*

Certifications

Comptia Security+ (In Progress)
ISC2 CC
Google Cybersecurity Professional Certificate
Certified Ethical Hacker (CEH v11) | EC Council
SOC Essentials | Splunk