Manoj Vignesh **K M**

Security engineer · Automation Expert

www.kmmanoj.me | kmmanoj | @kmmanojv96

Education

Georgia Institute of Technology
Atlanta, Georgia, US

M.S. in Computer Science — *Aug 2021 - Dec 2023*

- Computing Systems Specialization

PES Institute of Technology
Bengaluru, Karnataka, India

B.E. in Computer Science and Engineering — *Aug 2014 - Aug 2018*

- Gold medalist with a grade score of **9.69** and rank **5**

Industry Experience

Juniper Networks
Sunnyvale, California, US

Security Engineering Intern — *May 2023 - Aug 2023*

- **Monitoring for Supply chain attack**: Developed a web application that communicates with build tools, and CVE databases (such as NVD, CVEdetails) to monitor CVEs of packages in Juniper software products.
- **Penetration testing**: Contributed to threat modeling, designing test cases and performing VA/PT for Juniper products to find 3 medium or higher vulnerabilities.
- **CTF user training**: Contributed to development of CTF challenges around web, systems and cryptography. The CTF saw 97% registration and the top 5 teams scored close to 90% with average distance between them at 0.8%.

Georgia Institute of Technology
Atlanta, Georgia, US

Graudate Research Assistant — *Aug 2022 - Present*

- **Pirvacy leak due to browser extensions**: Contributed to the research by developing system that taints web elements to track their access and usage by browser extensions.

Georgia Institute of Technology
Atlanta, Georgia, US

Graudate Teaching Assistant — *Aug 2022 - Present*

- **Module lead for SDN**: Presented content and walkthrough project requirements for SDN module of CS 6211: System Design for cloud computing course.
- **Course design**: Improved project evaluations by providing PyTests and better documentation that left room for more deeper interaction during live grading of student's projects.
- **Office hours**: Conducted office hours to nudge students to find answers and answer conceptual questions that students had.
- **Grading**: Live grading of student's work to test student's understand of the subject.

Postman
Bengaluru, Karnataka, India

Security Engineer — *Aug 2021 - Aug 2022*

- **CSPM/CWPM Vendor Assessment**: Assessed multiple CSPM/CWPM vendors against Postman's cloud security requirements. The assessment and the deal improved the visibility of the cloud infrastructure by 3x (based on number of actionable alerts), reduced the cost by about 250% and reduced the maintenance efforts by about 200%.
- **Custom Security Controls**: Developed custom security controls using AWS lambda, Python, Node JS for Postman's AWS environment. This improved the visibility by a further 20%.
- **Threat modelling**: Performed threat modelling at multiple layers of Postman cloud and web application infrastructure. This established a framework to measure security testing coverage and improved the efficiency of VA/PT process.
- **Security Regression testing systems**: Built and improved 7+ automated security regression testing systems to continuously monitor releases of critical services.
- **Vulnerability Assessment and Penetration Testing**: Assessed 50+ releases and 7+ major releases off security vulnerabilities in Identity, Billing and other micro services. Found 5+ security vulnerabilities with CVSS score above 7.
- **Incident Response**: On call support for 100+ hours on web application security and cloud security incidents.
- **Tech Talks**: Presented multiple technology talks on API security - OWASP top 10 security in action themed around a vulnerable demo bank server, Postman as automatic security regression testing platform.

Intuit Inc.
Bengaluru, Karnataka, India

Identity and Access Management Engineer — *Nov 2020 - Aug 2021*

- **Authorization data schema**: Strategized and performed migration of live authorization data to a new schema with zero service downtime.
- **Tech Talks**: Presented multiple technology talks on systems security - Docker container security, AWS resources and infrastructure, threat modelling authorization data access infrastructure.

Intuit Inc.
Bengaluru, Karnataka, India

Network Automation Engineer
Aug 2018 - Nov 2020

- **Experimenting FIDO2**: Contributed to experiment of rolling out FIDO2 based multi-factor authentication on the enterprise endpoint systems. Windows hello with Active directory was used for the proof of concept. The security of systems and sign-in user experience of the beta users was observed to have improved.
- **Enterprise Infrastructure Monitoring**: Architected a secure and scalable data pipeline using AWS ECS and AWS lambda and secured with SNMP ACLs and encrypted credentials, from network and video conferencing devices to a monitoring and alerting tool, thereby reducing the MTTD issues by 50%.
- **Chatbot**: Designed, threat modelled and implemented a slack bot using python Django and various AWS services that provides a natural language conversational interface for the automation scripts to the users. Zero security incidents reported till date. It also improved user experience and reduced the learning curve required to understand an automation software.
- **Event Correlation Engine**: Developed a curious and intelligent SIEM like system using python Django in AWS ECS that correlates different network alerts to present an aggregate analysis, thereby further reducing the MTTD by 20%.
- **Infrastructure QA Automation**: Automation of pre-checks and post-checks of the network, video conferencing, and security devices before and after a change. This removed human errors and standardized the test series.
- **Asset Management**: Built a data pipeline using python Django in AWS ECS and AWS lambda for various network and video conferencing orchestration tools to ensure a single source of truth for the asset inventory.
- **Leadership**: Lead a team of 3 engineers to consistently deliver at least 70% of sprint task points. Taught, guided, and advised network engineers on python and AWS that grafted DevOps mindset and enabled the team to write scripts that automate at least 10% of their routine work.
- **Incident response**: On call support for 120+ hours on network and network automation software incidents.

Intuit Inc.
Bengaluru, Karnataka, India

Network Automation Co-op
Jan 2018 - Jun 2018

- **Video Conference troubleshooting**: Developed a web application using React JS and python Django that presents the hop-by-hop network health of each participant of a VC call, which reduced MTTD issues by almost 3 times.

Intuit Inc.
Bengaluru, Karnataka, India

Network Automation Intern
May 2017 - Jul 2017

- **VPN troubleshooting**: A CLI utility that gathers VPN client machine data and generates a report that is used by engineers to quickly identify the issue. This reduced the MTTD from 20 minutes to less than a minute

Research & Personal works

Applied Research
https://blog.kmmanoj.me

Blogger on medium.com
Nov 2018 - Present

- Article on "How complex can Authorization get?"
- ARP Spoofing custom exploit using ScaPy
- Man-in-the-middle via hoax DHCP
- DHCP starvation attack without making any DHCP requests
- Experiment to setup and learn internal network pivoting using Port forwarding
- Burpsuite plugin to capture and query proxy data from a database.
- Learning behavior of exploits and recon using SSH honeypot with cowrie.

Academic Research

Independent Researcher
Nov 2018 - Present

- **Modelling Trust Frameworks for Network-IDS (INCET 2021 - IEEE)**
  Mathematically modelling human instinctive trust among systems to communicate security based trust reduction and redemption messages. [https://doi.org/10.1109/INCET51464.2021.9456381]
- **Tamper Detection and Correction of ELF Binaries by Remote Parties via Merkle Trees (ICCISoT 2020 - Springer)**
  Efficiently identifying and patching malicious software using merkle trees before the first execution by the user. [https://doi.org/10.1007/978-3-030-66763-4_14]

Center for Cloud computing & Big Data, PES Institute of Technology
Bengaluru, Karnataka, India

Research Intern
Jun 2016 - Dec 2017

- **Green Cloud**: Energy Efficient datacenter management under availability constraints. To design a VM allocation, migration, and scheduling policy to ensure high availability while optimizing the amount of energy consumed by the data center.
- **Digital Swachh Bharat**: Digital initiative to clean India. To research strategic placement of garbage bins and efficient track for garbage truck based on multiple parameters such as size of truck, location and volume of garbage dumps.

Skills

SecOps	Penetration testing, Web Application Security, Cloud Security, Network Security
DevSecOps	AWS, Docker, Kubernetes, Snyk, CodeQL, Burpsuite plugin
Technology	AWS, Azure, GCP, Dockers, Kubernetes, Linux
Techniques	Threat modeling, Design Patterns, Source code review, Secure Design, Secure coding
Tools	Burpsuite, Wireshark, GNS3, Metasploit, Snort
Database	PostreSQL, MySQL, SQLite3, MongoDB, Neo4j, AWS Aurora, AWS Neptune
Backend	Python Django, Python Flask, Golang Gin, SailsJS, NodeJS, ExpressJS, Java Spring Boot
Frontend	ReactJS, HTML5, CSS3
Programming	Python, Javascript, Java, C/C++, Golang

Extracurricular Activity

Active	**Security Blogger**, on Medium
Currently	**Ranked top 1%**, in TryHackMe Pentesting Lab
Organized	**Guest lectures**, with my alma mater on advanced subjects
Was	**Project lead**, OSINT platform at Null India
Was	**an Active member**, of Intuit's NextGenNetwork
Was	**a Representative**, of Intuit's Community Service Group

Honors & Awards

2021	**11/100+ rank**, Intuit Redcon CTF 2021
2020	**178/5000+ rank**, NahamSecCon CTF 2020
2020	**13/600+ rank**, June'gle CTF 2020
2020	**4/30+ rank**, Intuit Redcon CTF 2020
2019	**NextGenNetwork Champion**, at Intuit's NextGenNetwork
2018	**Gold Medalist**, in Computer Science and Engineering, batch 2018 of PES Institute of Technology
2014-18	**Professor CNR Rao Merit Scholarhsip award winner**, in undergraduate

Certifications

CompTIA Security+

SY0-501 *October 2020*

AWS Solutions Architect Associate

AWS SAA-C01 *May 2019*