AKSHAY GALGALI

Houston, TX | +1 469-922-8892 | agalgali@cougarnet.uh.edu | GitHub | LinkedIn | Portfolio

EXPERIENCE

5G Software Engineer (Co-op), ***Simnovus, Cary, North Carolina*** **Jan 2023 - Present**

- Created a network containing multiple VLANs and TUN interfaces supporting nested network namespaces for simulating more than 1000 UEs and PDNs.
- Aided in testing the new application features in the UE simulator to minimize vulnerabilities by implementing secure coding standards, security policies, and best cybersecurity practices against security risk parameters before release.
- Delivering the highest quality of service, working with a multidisciplinary team (QA, Engineering, Sales) to debug and rectify faults discovered during testing with the assistance of the Sales team, and putting proactive measures in place to address customer concerns.

Wi-Fi Engineer (IA), ***University Information Technology, University of Houston*** **Sept 2022 - Jan 2023**

- Led a team to maintain and monitor traffic that entered the campus Wi-Fi network, using Aruba Central, which helped in the authentication and implementation of security policies for 6500 Aruba access points on campus.
- Reviewed and analyzed security architecture & policies that was built on 500 acres of campus which comprised two data centers and 6500 APs which resulted in efficiently gathering evidence and assisting in the deployment of the NIST (SP) 800-207 Zero-Trust Architecture framework.
- Aided in the migration to the newest 802.11ax Wi-Fi technology on-campus locations, which included anything from a big basketball arena, more than 6,000 dorm rooms, 500-person auditoriums, and extremely high-density library/study facilities.
- Developed and conducted network and security audit to monitor all access points on campus, using Ekahau data capture files and running them on Aruba central tool, which enabled our team to find 40 rouge access points and rest them to work effectively.

SKILLS

Skills: Network Security, Vulnerability Assessment, Penetration Testing, Privilege Escalation, Control System Security.
Programming Languages and Scripting: Proficient in Python, C, C++, Bash scripting, Shell Scripting, PowerShell.
Operating System: Kali Linux, Windows, Linux, Macintosh, Security Onion.
Networking and Routing: NAT, DNS, DHCP, ICMP, VoIP, VLAN, TUN/TAP, Network Namespace, IP Subnetting, Network Slicing, OSPF, IDS, Firewall (Cisco, Azure, Sophos).
Networking Devices: Routers, Switches, Access Points, Bridges, Gateway, Hubs. (Cisco, Aruba, Tplink).
Information Security Techniques: OWASP Top 10, OSINT, CIA Triad.
Tools*:* Wireshark, Nmap, Burp Suite, Metasploit, Snort, Cobalt Strike, Nessus, Kibana, Docker, MobaXterm, VMWare, VirtualBox, Putty, WinSCP, PyCharm, Git.
Standards, Frameworks, Certifications: NIST Cybersecurity Framework, SOC2, ISO 27001/2.
Wi-Fi Standards: 802.11ax (Wi-Fi 6) 802.11ac.
Software Development Life Cycle Models: Agile SDLC, Waterfall model, DevOps.
Interpersonal Skills: Teamwork, Active Listening, Analytical thinking, Leadership, Conflict Management, Problem solving, Motivation.

EDUCATION

University of Houston, TX **Aug 2021 - May 2023**
Master of Science in Cybersecurity **| GPA: 3.9/4**

University of Mumbai, India **May 2018 - June 2021**
Bachelors of Engineering in Information Technology | ***CGPA*****: 8.76/10**

PROJECTS

MODBUS Attack & Packet Injection Lab | *Modsak Simulator, VMs, Shell Scripting* **|** GitHub, Report

- Simulated a MODBUS attack & Packet Injection attack in Industrial Control System in a Master-Slave environment using Modsak Simulator to assess the vulnerabilities and risks in Industrial Control System and how to mitigate and prevent the attack.

Keystroke Logger | *Python Scripts, VMs, Python Libraries* **|** GitHub

- Developed a keystroke logger in an active browser using python scripting and libraries, to retrieve sensitive information and credentials of a user like a username, passwords, card details, this credentials and URL information is sent via email to the attacker.

Log and Network Traffic Analysis Lab | *Kibana, VMs, Incident Response Plan* **|** GitHub, Report

- Implemented incident response plan when an alert was generated where a system operated by a user from HR behaves maliciously as if another person is controlling it, performed investigation on alert using Kibana, analyzed windows logs and network traffic, and reported mitigation and prevention methods.

RESEARCH/TECHNICAL PAPERS

- SOC - Setup, Responsibilities and Accomplishments | Read
- Mitigating Cybersecurity threats to Industrial Control Systems: SCADA | Read
- Cybersecurity Risk Management - Risk Management Plan for an IT Firm | Read
- Database Cryptography in Today's Enterprise | Read
- Analysis of Advance Persistence Threat Group And its Impact on the Organization | Read