KARTHIK JADALA

412-758-6771 | kaj98@pitt.edu | LinkedIn | Website | Pittsburgh, PA 15213

EDUCATION:

University of Pittsburgh, Pittsburgh PA **GPA-3.9** **Apr 2020**

Master of Science in Telecommunications majoring in **Cyber Security**

Relevant Courses: Network Security, Developing Secure Systems, Machine Learning, Cryptography, Computer Forensics, Information Security and Privacy, Data Structures, Application of Networks

Indian Institute of Technology Gandhinagar, India **May 2013**

Bachelor of Technology in Electrical Engineering

SKILLS:

- **Programming Languages:** Python, Shell Scripting, Javascript, C
- **Skills:** Penetration Testing, binary debugging and disassembly, x86 architecture, XSS, SQL injection, OWASP top 10, Network segmentation/ secure network design, Mitre Att&ck and Cyberkillchain frameworks, threat modelling in SDLC, Routing and switching technologies and protocols, TCP/IP, Open embedded/ Bitbake, CI/CD pipeline
- **Tools:** Nmap, Wireshark, AWS (EC2, S3, Cloudfront, Route53, IAM, GuardDuty), Burp Suite, radare2, IDA, SSH, SQL, Docker, Open VPN, Git, Nessus, Snort, Pandas, MATLAB
- **Certifications:** CompTIA Security + (in progress)

EXPERIENCE:

Security Engineer Intern, Intel Sports **May 2019 – Aug 2019**

- Performed penetration testing on web apps using **burp suite**, calculated **CVSS** scores of all issues found and developed POCs. Worked with development teams to mitigate these issues.
- Audited all the subdomains hosted on **cloudfront**/ **S3 buckets** and DNS entries in **Route53** to find the subdomains vulnerable to takeover attacks and mitigated them.
- Audited **EC2**s' security group policies, enumerated open ports, running services and their versions, SSL ciphers.
- Developed an in-house tool to perform security scans on EC2 instances using **python** and **boto3**
- Integrated opensource tools like **prowler** and **pacu** for benchmarking and finding configuration flaws
- Created REST APIs for using **flask** and **SQLite** and developed a web interface for the same using **react**
- Performed threat modeling and risk analysis at different phases of **SDLC**

Engineer, Qualcomm (Contract) **Jul 2014 – Aug 2018**

- Integrated static analysis tool **Klocwork** to find predefined vulnerabilities in the codebase, integrated patches for different **CVE** from upstream and delivered code to customers as per requirement
- Upgraded and optimized different user space daemons and startup scripts (**shell/ python**) to improve the boot up time (by more than **3** seconds) and key performance indicators (**KPI**) in Linux based IOT chipsets.

PROJECTS: **Aug 2018 - Present**

- Solved multiple CTF challenges on vulnhub, tryhackme, protostar - https://noobfrompitt.github.io/categories/
- Discovered privilege escalation vulnerability in virtual machines provided in course material and disclosed
- Designed a secure network segmentation for a mock company with specific requirements and constraints
- Executed ChopChop attack to exploit the known vulnerabilities in WEP networks using **aircrack-ng**
- Created and validated an analytical model of a network firewall under **DOS attack** using **Markov**

OTHER ACTIVITIES:

- Public relations manager for ANKUR, the Indian community at University of Pittsburgh **Apr 2019 – Apr 2020**