RAVI BUDDI

https://ravibuddi.com
ravi@ravibuddi.com

EDUCATION

- **Rochester Institute of Technology, Rochester, New York**
  Master of Science in Computing Security — May 2017
  GPA: 4.0/4.0

EXPERIENCE

- **Information Security Engineer** — December 2018 – Present
  Indeed
  - ➔ Working with other teams to identify, resolve, and mitigate vulnerabilities
  - ➔ Deployment and administration of endpoint security tooling
  - ➔ Building operationalized workflows for various tools.
  - ➔ Creating and maintaining documentation for new and existing processes and deployments

- **Advisor, IT Security** — July 2018 – November 2018
  Secureworks
  - ➔ Provided in-depth analysis of security incidents
  - ➔ Developed and deployed counter measures to detect threats

- **Sr. Analyst, IT Security** — June 2017 – June 2018
  Secureworks
  - ➔ Performed accurate and precise real-time analysis of logs/alerts
  - ➔ Analyzed and assessed security incidents

- **Information Security Intern** — May 2016 – May 2017
  Wegmans Food Markets
  - ➔ Investigated and Resolved the Security offenses generated by SIEM
  - ➔ Tuned the SIEM ruleset to make it more efficient and useful
  - ➔ Processed intake tickets for SOC

- **Information Security Intern** — January 2016 – May 2016
  Southwest Airlines
  - ➔ Structured and processed information security policy exceptions
  - ➔ Assisted in the regulation compliance of PCI DSS

CERTIFICATIONS

- Offensive Security Certified Professional (OSCP)
- CompTIA Security+ – *Expires February 2021*
- CCNA Cyber Ops – *Expires February 2021*
- CCNA Routing and Switching – *Expires February 2021*

PROJECTS

- **Threat Detection with osquery and Elastic Stack**
  Utilized osquery daemon as an endpoint protection agent to monitor system security. Modified the existing query packs to effectively query the operating system. Used Elasticsearch to store all the logs, Logstash for parsing the logs and Kibana as a front end graphical user interface.
- **Implementation of GRR**
  Deployed Google Rapid Response and presented its advantages for incident response at scale.

SKILLS

- **Operating Systems**

  Microsoft Windows (7-10, Server 2012, 2016) – network configuration, active directory management, system security, firewall configuration.

  Linux/Unix based systems (Debian, RedHat)-network configuration, terminal knowledge, firewall configuration.
- **Programming/Scripting Languages**

  Python, C
- **Tools**

  Nmap, Metasploit, Wireshark, Burp Proxy, QRadar, Palo Alto
- **Other skills**

  Networking (Cisco devices), virtualization (VMware Workstation/Fusion & ESXi), database (MySQL)

ACTIVITIES

- Member- RIT Competitive Cyber Security Club; SPARSA (Security Practices and Research Student Association)