PRATINAV CHANDRA

pratinav.chandra1997@gmail.com | +1 (240) 927-9770 | College Park, MD

· inf0spec.medium.com · pratinavchandra.github.io · github.com/pratinavchandra · linkedin/in/pratinav-chandra ·

EDUCATION

University of Maryland | A. James Clark School of Engineering College Park, MD
Master of Engineering - Cybersecurity *Aug 2022 – Present*

Manipal University **Jaipur, India**
Bachelor of Technology - Computer Science & Engineering **GPA:** 8.4/10 *July 2015 – June 2019*

SKILLS

• **Domain:** Network Security, Security Monitoring, Automation, Packet & Log Analysis, Computer Networking & Design, Virtualization
• **Infrastructure:** Firewalls (Palo Alto Networks, Checkpoint, Sonicwall), Web proxies (Symantec), VPN (Palo Alto Networks - Global Protect), IDS, Routers (Cisco), Switches (Cisco, Ixia), Raspberry Pi, Arbor DDoS Protection
• **Tools:** Splunk, Wireshark, tcpdump, Burp Suite, MITRE ATT&CK, Solarwinds NPM, Firemon, Nmap, Metasploit, Yara, Snort, Security Onion, FlareVM, REMnux, Zeek, Scapy, Volatility, Prometheus, Grafana, Docker, Canary tokens, ServiceNow, etc.
• **Programming/Scripting Languages:** Python, C, Bash, Java, HTML, CSS, Javascript

WORK EXPERIENCE

Dell Technologies – *Senior Cybersecurity Analyst* *Bengaluru, India · July 2019 – July 2022*
• Served as part of a fast-paced global Cyber Defense team handling **high-priority network security incidents** and managed firewalls, web proxies, DDoS protection, and VPN technologies with a **98% customer satisfaction rating**.
• Implemented data center, lab, and DMZ security architectures and deployed and **configured network security solutions** for the segmentation of multiple sites globally, **reducing the attack surface by 80%.**
• Created monitoring alerts, built dashboards, and **extracted insights from network traffic** and network security device logs using Splunk, Solarwinds, and Firemon, **increasing visibility by 60%.**
• Spearheaded the development of tools for the **automation** of various processes and workflows and **reduced manual workload on the team by 70%** within four months.

Tecelec Engineers – *Software Development Intern* *Vadodara, India · Jan 2019 - April 2019 & June 2018 – July 2018*
• Developed web applications for the **automation** of earthing and cable sizing calculations using React JS, Node JS, and MongoDB Atlas.
• Built Python tools for the automation of electrical termination schedule generation and various technical processes that **reduced workload** on teams from days to seconds and also **decreased the cost of resources by 50%.**

PROJECTS

Home Cybersecurity Lab - *Independent Project* *December 2022*
• Designed and implemented a home cybersecurity lab from scratch to **test deployments, vulnerabilities, and open-source tools**.
• Deployed an **isolated malware analysis lab** consisting of FlareVM and REMnux and **configured a Raspberry Pi 4 to run ESXi ARM** and hosted multiple virtual machines to run services **to enhance the security of the lab and increase visibility on the network**.
• Established **edge defense** by deploying a Palo Alto **PA-220 firewall** to analyze and monitor traffic **between the lab and the internet**.
Technologies used: Python, Linux, Prometheus, Grafana, ESXi, Raspberry Pi, Pi-Hole, Palo Alto Firewall, FlareVM, REMnux, dnsmasq

Technical Content Writer - *InfoSec Write-ups* *September 2021 - Present*
• Published write-ups as part of the team at "InfoSec Write-ups'', which is the largest Cybersecurity publication on medium.com with over **23k followers**. My write-ups have been **recommended as reading resources** by a SANS instructor for Windows Forensics as well as **featured as walkthroughs** at leading blue team CTF platforms.
Topics covered: Home lab guides, Windows forensics, Blue Team CTF Walkthroughs, Analysis of Zero-Day vulnerabilities

IoC Miner - *Independent Project* *April 2021*
• Developed an automated tool that **analyzes a supplied packet capture file** and attempts to **find and collect all possible indicators of compromise** in the network traffic, runs reputation checks and creates an HTML **incident report**, which **saves time** and provides a good starting point while working on an incident.
Technologies used: Python, Scapy, Wireshark, VirusTotal, URLVoid

pxymon - *Dell Technologies, Bengaluru, India* *August 2020*
• Implemented a tool to **troubleshoot and identify issues** related to web proxies and **web-based traffic** automatically by parsing the security policy based on keywords and filtering through rules to **search through the configuration faster**.
• Designed modules to **perform various kinds of tests** on multiple proxies and URL lists **simultaneously** to **save time**.
Technologies used: Python, Splunk, Symantec Proxies, McAfee Web Gateways, Solarwinds NPM, Postman, Burp Suite

CERTIFICATIONS

Practical Malware Analysis and Triage - **TCM Security Academy** *November 2021*
Cyber Defense Path (Threat & Vulnerability Management, Security Operations & Monitoring, Threat Emulation, Incident Response & Forensics, and Malware Analysis) - **TryHackMe** *July 2021*
Palo Alto Networks Certified Network Security Administrator - **Palo Alto Networks** *February 2021*
Splunk Fundamentals - **Splunk** *August 2019*
Developing Ethical Hacking Tools with Python - **Cybrary** *July 2019*