AAKASH RAMAN

aakashr93@gmail.com | +1(240) 921-7770 | LinkedIn| Medium| GitHub | College Park, MD (Willing to Relocate)

EDUCATION

UNIVERSITY OF MARYLAND, COLLEGE PARK — College Park, MD, USA
*Master of Engineering in Cybersecurity; CGPA: **3.77*** — Aug '22 - May '24

VELLORE INSTITUTE OF TECHNOLOGY — Vellore, TN, INDIA
*Bachelor of Technology – Computer Science Engineering with Information Security; CGPA: 9.37 **(3.8)*** — Jul '17 - Jul '21

KEY SKILLS

Programming/Scripting Languages: Python, C, C++, Java, HTML, CSS, JavaScript, Bash, PowerShell, SQL.
Operating System/Virtualization Technologies: Windows, Kali Linux, Ubuntu Linux, VMware, Docker, Basic Kubernetes
OSINT/Offensive Security Tools: Burp Suite, OWASP ZAP, Nessus, Nmap, Metasploit, SQLMap, Hydra, John The Ripper, Bloodhound, Ffuz, Gobuster/Dirbuster, Responder, Mimikatz, Nikto, GoPhish.
Malware Analysis/Reverse Engineering Tools: Ghidra, IDA Pro, gDB, ProcMon, Process Explorer, Regshot, PE-Bear, Cuckoo Sandbox, VirusTotal.
Digital Forensics/Incident Response Tools: Elastic SIEM (ELK), Splunk, AlienVault, Basics of CrowdStrike Falcon, IBM QRadar, Suricata, Snort, Yara, Velociraptor, VeraCrypt, FTK Imager, Autopsy, Volatility, Wireshark, E-Mail Security Tools, Microsoft 365 Defender, Microsoft Azure Sentinel.
Cloud Security Technologies: AWS EC2, S3, IAM, Cloudwatch/Cloudtrail, Basics of Azure & GCP.
Risk & Compliance Frameworks: Threat Modelling, NIST Cybersecurity Framework, Microsoft Office Suite, Technical Content Writing, ISO 27001, PCI-DSS, HIPAA, SOC 2, GDPR, Risk Management, Business Continuity Planning, Root Cause Analysis, STIX, TAXII.
DevSecOps Tools: Basics of Git, Jenkins, Synk, Ansible, SonarQube.

EXPERIENCE

IBM (X-Force Incident Response) — Austin, (TX, USA)
Cybersecurity Consultant Intern — May '23- Aug '23

- Participated in Purple Teaming bootcamps covering Web Application Penetration Testing, Disk, Network & Memory Forensics, and Malware Analysis. Shadowed multiple Digital Forensic Analysts & Incident Responders on multiple incidents, threat assessments and forensic investigations increasing Incident Response actions by **95%**.
- Conducted research on visualizing lateral movement using Velociraptor JSON Logs, improving IR capabilities by **20%**.
- Presented research findings to IBM Executives, improving communication of technical findings to both technical and non-technical professionals.

HEVO DATA INC — Bangalore, (KA, INDIA)
Cybersecurity Associate & Content Lead — Jul '21- May '22

- Led a team to monitor and analyze security events, developing technical blogs on threat detection and incident response, increasing the company's online presence by **30%**.
- Conducted keyword research and utilized SIEM tools to enhance content visibility and ensure data integrity, improving strategic cybersecurity decisions.
- Improved the company's security posture by refining risk management methodologies, and reducing potential risks by **15%**.

HEVO DATA INC — Bangalore, (KA, INDIA)
Cybersecurity Research Analyst Intern — Jan '21- Jul '21

- Monitored security alerts and conducted incident investigations, integrating network and E-Mail security protocols across various endpoints & networks.
- Authored technical blogs on Cybersecurity & Data Analytics trends, threat analysis, and best practices.
- Identified and analyzed vulnerabilities in the company's cloud infrastructure and compliance frameworks, proposing actionable solutions, and leveraging advanced analytics for robust security protocols.

RAMCO CEMENTS LTD — Chennai, (TN, INDIA)
Security Consultant Intern — Apr '20 – May '20

- Enhanced the company's Risk Management, Business Continuity & Disaster Recovery Plans, reducing downtime by **25%**.
- Utilized OSINT and SIEM solutions like Recon-Ng, Nmap and AlienVault for security monitoring and Incident Response.
- Conducted a Digital Forensic investigation using tools like Autopsy, X-Ways, Encase & Veracrypt to discover Insider Threats improving security procedures by **75%**.

PROJECTS

- **Visualizing Lateral Movement with Velociraptor JSON Logs:** Developed a prototype tool named "Velocigrapher" to detect lateral movement visualization using Python's "igraph" library. It uses Velociraptor EDR's artifacts along with Windows Authentication Logs thereby improving Incident Report Quality by **85%**.
- **Android Malware Analysis Research Paper**: Published a research paper on the trends of various Android malware and their mitigation techniques in JESTR Journal. The paper extensively covers both the technical and business impacts of each Android sample, their interactions with a C2C Server and their appropriate mitigations.
- **Penetration Testing and Incident Response for Horizon Inc:** Conducted penetration testing using the MITRE ATT&CK Framework and Cyber Kill Chain, and implemented defensive measures with the Diamond Model of Intrusion Analysis.
- **Designing a Secure Cloud Security Architecture for Cobra Kai**: Designed and implemented a secure AWS Cloud architecture, migrating on-premise infrastructure of Horizon Inc and ensuring robust security with tools like EC2, Lambda, and CloudWatch.

CERTIFICATIONS

CompTIA Security+, CySA+, PenTest+, CASP+
AWS Solutions Architect Associate
Certified CyberDefender (Pursuing PJPT & CISSP)

CTFS

- UMD CTF'24: Ranked 51 overall, solved Forensics, Web, Privilege Escalation, Cryptography, Log Analysis and Threat Hunting challenges.
- Level Effect's Cyber Defense Analyst CTF: Ranked #14 globally, solving Forensics, Incident Response, Scripting, OSINT challenges.
- TryHackMe - Currently in the Top 1% with 100+ rooms complete.
- HackTheBox: Currently Pursuing Pwning Boxes and Defensive Sherlocks.
- CyberDefenders: Participated in Blue Team CTFs covering Threat Intelligence, Malware Analysis, Cloud Forensics, Threat Hunting, Endpoint Forensics, Network Forensics, and Memory Forensics.