Ansh Chandnani

✉ ansh.chandnani@gmail.com | in LinkedIn | github.com/mrdebator | Blog | anshc.me

Academics

Drexel University June 2023

B.S. in Computing & Security Technology, minor in Computer Science GPA: 3.91/4.0

Selected Coursework: Virtual Environments & Cloud Security, Network Security, Operating Systems, Computer Forensics, Ethical Hacking, Disaster Recovery, Systems Architecture, Database Management Systems, Server Management

Publications:

⇒ " Malware Detection in Cloud Native Environments ↗ ", **ACM AICCC 2024** ↗

⇒ " Finding Balance - Looking Towards the Future, in Media Literacy for Justice ↗ ", **American Library Association**

⇒ " Ontology Modeling of Industrial Control System Ethical Hacking ↗ ", **ICCWS 2021** ↗

Work Experience

Google **Sunnyvale, CA**

- *Security Engineer, Offensive Security* *July 2023 - Present*
  - Designing and executing realistic **red team exercises** using novel Tools, Techniques, & Procedures (TTPs) against several **client-centric** and **enterprise products** to improve Google's security posture.
  - Architecting and developing tools to **support penetration tests** through the **reconnaissance** and **post-exploitation** phases resulting in **increased operator convenience** and **stealthier attacks.**
  - Collaborating across teams on **security reviews**, **vulnerability taxonomies**, and helping organize community events such as the **BSidesSF CTF**, **Red Team Summit**, and HackTheCity at SaferWithGoogle.
- *Security Engineering Intern, Offensive Security* *June 2022 - September 2022*
  - Conducted extensive **Open Source Intelligence (OSINT)** investigations to identify **foothold vectors** on Google's **production** & **corporate** environments.
  - Introduced **query-capable knowledge graphs**, and through subsequent automation, **saved** operators **2+ weeks of reconnaissance time**.
  - Collaborated on a specialized **penetration test**, safely simulating **insider risks**, that targeted critical production infrastructure, resulting in a broader push for **healthier credential habits**.
- *Security Engineering Intern, Detection Team* *June 2021 - September 2021*
  - Designed & built a **platform and OS agnostic** Zeek script validation tool using **Go** and the **Google Cloud Platform** to provide a standardized testing environment for threat detection automation.
  - Implemented the tool as an **on-demand** utility with a custom **Docker** image, reducing the **testing time** to **60 seconds.**
  - Assisted the **Corp Task Force** in threat detection and analysis to prevent **insider threats** and **permission creep**.

Susquehanna International Group **Bala Cynwyd, PA**

- *Cybersecurity Coop, Firewall Services* *September 2020 - March 2021*
  - Designed & built a **Rule Lookup** tool using **Python3** and custom APIs, **automating** manual **firewall rule lookup** operations across all firewalls.
  - Configured & managed firewall rules to facilitate **secure network access** for various services & workstations across **global offices and exchanges**.
  - Collaborated on automation projects for firewall **health checks**, status **alerts**, and data-aggregating operations to **guarantee up-time** during trading hours.

STAR Scholars, Drexel University **Philadelphia, PA**

- *Cybersecurity Research Scholar* *July 2020 - September 2020*
  - Conducted research on leveraging **ontologies** & **semantic graphs**, with **SPARQL** queries, to create contextual representations of security information for **Industrial Control Systems (ICS)**.
  - Developed an ontology using **Protege** to model **threats, vulnerabilities, exploits**, and critical security information.

Other Experiences: Cybersecurity Intern at Kyrion Technologies ↗ , Fellowship at Young Leaders' for Active Citizenship ↗

Select Projects

- **eBPF Sysmonitor -** Developed a **kernel-level** system monitor using the **extended Berkeley Packet Filter (eBPF)** to log events and detect threats in **distributed computing environments**.
- **Claros -** Architected a **graph-based** cybersecurity **search engine** that takes an NMap scan and aggregates relevant port, service, vulnerability, and exploit information to **streamline attack surface enumeration**.
- **Malware Analysis with Machine Learning -** Built parameterized **malware** and **exploits** to train **n-gram** based models in **system call-based anomaly detection**.
- **Cybersecurity Training Lab -** Constructed a cybersecurity lab using **Proxmox**, Kali Linux, and vulnerable machines on recycled servers to provide a **learning environment for 500+ students**.
- **BabyRSA -** A cryptography tool built in python that **decodes RSA Encryption based on the public key.**
- **OfflineCaesar -** A nifty python script to **brute force Caesar Ciphers**; a useful tool in **Capture The Flag** competitions.
- **Oracle SQLizer -** Python **automation** that creates Oracle SQL INSERT statements from a given CSV file, using **regex** to handle various data types.

Certifications & Trainings

- Creative Red Teaming, Mandiant
- Security Fundamentals, Microsoft Training Association
- OSINT Corporate Recon, HackTheBox Academy

Involvements & Achievements

- Collaborated & organized the **BSides San Francisco CTF** 2024.
- **President** of Drexel Cyberdragons (Cybersecurity club), 2022-23
- **Vice-President** of Drexel Cyberdragons (Cybersecurity club), 2021-22
- **Won** the Central Regional **Collegiate Penetration Testing Competition 2021**.
- Awarded 'Best Poster Presentation' at the **Stanford Research Conference 2021**.
- **Ranked 4th out of 113 teams** in the CyberSEED Capture-the-Flag (CTF) competition 2021.
- Presented research at the **Harvard National Collegiate Research Conference 2021**.
- Competed in HTBxUNI CTF 2021, National Cyber League, CPTC 2022, CCDC 2022, & CCDC 2020.