Apurv Singh Gautam

apurv.gautam@gatech.edu apurvsinghgautam.me

Education

- **Georgia Institute of Technology** — Atlanta, US
  Master of Science in Cybersecurity (M.S.); GPA: 3.75 — *2019 - Expected 2021*
- **Symbiosis Institute of Technology** — Pune, India
  Bachelor of Technology in Information Tehcnology (B.TECH); CGPA: 8.63 — *2015 - 2019*

Experience

- **International Computer Science Institute, UC Berkeley** — Berkeley, US
  Security Research Intern — *May 2020 - Jul 2020*
  - **Area**: Threat Intelligence
  - Researched 5 dark web forums and marketplaces
  - Analyzed the data using advanced NLP algorithms (LDA, CatE)
  - Created 4-6 high-level threat intelligence metrics for the analyzed data
- **Georgia Institute of Technology** — Atlanta, US
  Graduate Teaching Assistant — *Aug 2019 - Apr 2020*
  - **Course**: CS 4235/6035 Intro to Information Security, CS 6250-O01 Computer Networks
- **Volon Cyber Security Pvt. Ltd.** — Pune, India
  Security Research Intern — *May 2018 - May 2019*
  - **Area**: Threat Hunting/Intelligence - Obtaining Intelligence from clear/dark web forums
  - Researched about 10-20 dark web forums and marketplaces
  - Performed Open Source Threat Hunting and stored the data into ELK
  - Scraped 1-2 GBs of dark web forum and marketplace data using Python Scrapy
  - Performed HUMINT on dark web forums

Skills

- **Programming**: Proficient in Python, Java, and Bash. Fundamentals of C, C++, PHP, JavaScript
- **Security**: Threat Intel/Hunting, OSINT, HUMINT, Security Analysis, Security Automation, Network Security, Red/Blue Teaming
- **Miscellaneous**: ELK, MITRE ATT&CK, NLP

Publications

- **Gautam A.S.**, Gahlot Y., Kamat P. (2020) Hacker Forum Exploit and Classification for Proactive Cyber Threat Intelligence. In: Smys S., Bestak R., Rocha A. (eds) Inventive Computation Technologies. ICICIT 2019. Lecture Notes in Networks and Systems, vol 98. Springer, Cham
- Kamat, Pooja, and **Apurv Singh Gautam**. "Recent Trends in the Era of Cybercrime and the Measures to Control Them." In Handbook of e-Business Security, pp. 243-258. Auerbach Publications, 2018. First Edition by CRC Press - Taylor & Francis Group

Projects

- **Crawling and Analyzing Top 1 Million Domains**: A research project that uses the top 1 million list of domains from three data sources namely Majestic, Alexa, and Tranco to apply a set of security metrics and visualize the results of that analysis along with a review of the change in popularity of domains for 30 days [Research Project]
  - Analyzed 1 million domains on 3 security metrics - HTTP/2.0 adoption, IPv6 adoption, and TLS adoption
  - Results were 27.16% of TLSv1.3 sites, 33.67% of TLSv1.2 sites, 31.36% of sites adopted HTTP/2.0, and 15.1% of sites adopting IPv6
  - Designed an efficient active scanning Sub Domain extraction tool using Python
  - Performed Trend Analysis on 20,000 domains and forecasted them as Top 100, 1000, and 10,000 in Kibana

- **Assess network reputation through multiple threat intelligence data feeds**: Research project that utilizes various threat intelligence feeds to assess network reputation and detecting & mitigating Volumetric anomalies using Machine Learning analysis using Python
  - Utilized PARAFAC tensor decomposition to decompose higher-order tensors in order-1 tensors
  - Consumed 12-13 ASes Netflow data to assess network reputation
  - Plotted several features to determine the behavior of these malicious infrastructures
  - Used the ARIMA model & Z score method to plot graphs and visualizations
- **Hacker Forum Exploit and Classification for Proactive Cyber Threat Intelligence**: Research project that utilizes hacker forum data for proactive cyber threat intelligence using Python. [Research Project]
  - One of the first few pieces of research talking about Threat Intelligence pertaining to dark web data in 2018
  - Used Python's Scrapy framework to scrape data from the dark web
  - Utilized ML & DL approaches in classifying data with precision above 95% for all the models used
  - Achieved 96.56% precision for the RNN GRU model
- **ForumScrapy**: Web Scraping application built on Flask that scrapes forum posts from the Bitshacking hack forum [Project]
  - Automated the scraping of Bitshacking forum posts
  - Utilizes several socks proxy in a chain to scrape the data
  - Utilizes ELK to store the data and visualize it
  - Created dashboard using Flask to view and interact with data with search capabilities
- **PastebinScrapy**: Threat Hunting tool built on Flask that scrapes IOCs, including IP addresses, hashes, and emails from Pastebin's latest pastes [Project]
  - Scrapes latest pastes from Pastebin using Pastebin's Scraping API
  - Collects IOCs like IP addresses, hashes, emails from the latest pastes
  - Utilizes ELK to store the data and visualize it
  - Created dashboard using Flask to view and interact with data with search capabilities

Community Involvement

- **DEFCON Red Team Vilage '20**: Delivered a talk on Automating Threat Hunting on the Dark Web and other nitty-gritty things
- **GRIMMCon 0x2 '20**: Delivered a talk on Threat Hunting on the Dark Web
- **Cybrary**: Volunteering as a Senior Teaching Assistant, managing security-fundamentals channel, creating materials for several security courses, including Intro to Threat Intelligence, Insider Threats, Intro to TOR, and many more
- **StationX**: Volunteering as a Teaching Assistant, moderating the discourse, engaging with the community, and solving course-related doubts
- **Cybercademy**: Volunteering as a Community Challenger, managing the discord and creating security challenges for students
- **SIT, Pune**: Presented two seminars on starting in cybersecurity for high-school students and cybersecurity certification batch students and conducted NS3(Network Simulator), Git, and Virtualization Buddy Session for third-year Computer Science and Information Technology students
- **MITCOE, Pune**: Conducted a Cyber Privacy Seminar on behalf of the Logout - Privacy Seminar
- **Null, Pune**: Delivered several talks including Introduction to VAPT, Bitcoin Forensics, and OSINT
- **TAIS, Varanasi**: Conveyed a two-day workshop on Cyber Security Awareness

Certifications

- **CompTIA Security+ ce by CompTIA**: (Feb 2019 - Feb 2022) [Link]
- **Computer Forensics by RITx**: (July 2017) [Link]
- **Cybersecurity Fundamentals by RITx**: (July 2017) [Link]

Significant Achievements

- **Best Outgoing Student Award - Symbiosis Institute of Technology, Pune, India**: Awarded as the Best Outgoing Student from B.Tech Information Technology 2015-19
- **DRDO Cyber Challenge - DRDO, Government of India**: Received Certificate of Achievement for securing 45th rank out of 1489 participants in the DRDO CTF challenge [Link]