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 - Present*
  - **Area**: Threat Intelligence
  - Researching about 5-10 dark web forums and marketplaces.
  - Analyzing the data using advanced NLP algorithms (LDA, BERT, GPT).
  - Creating 4-6 high-level threat intelligence metrics for the analyzed data.
- **Georgia Institute of Technology** Atlanta, US
  Graduate Teaching Assistant *Aug 2019 - April 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 Intelligence, Threat Hunting, OSINT, HUMINT, Security Analysis, Security Automation, Network Security, Penetration Testing, Red Teaming, 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]
  - Crawled 1 million domains for 30 days from Majestic, Alexa, and Tranco and stored in Elasticsearch.
  - Analyzed domains on 3 security metrics - HTTP/2.0 adoption, IPv6 adoption, and TLS adoption.
  - 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 concerning 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.

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]

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]

Extra-Curricular

- Volunteering as a Teaching Assistant for StationX - moderating the discourse and engaging with the community along with solving course-related doubts.
- Volunteering as a Teaching Assistant for Cybrary - creating materials for several security courses, including Intro to Threat Intelligence, Insider Threats, Intro to TOR, and many more.
- Volunteering as a Community Challenger at Cybercademy - managing the discord and creating security challenges for students.
- Completed many trekking & mountaineering expeditions in different Himalayan ranges of India.
- Presented a seminar on Cybersecurity for MS for cybersecurity certification batch students of SIT.
- Presented a seminar on Cyber Security for high school students during the SIT Summer School program.
- Conducted NS3(Network Simulator), Git, and Virtualization Buddy Session for third-year Computer Science and Information Technology students of SIT.
- Conducted a Cyber Privacy Seminar at MITCOE Pune on behalf of the Logout - Privacy Seminar.
- Delivered several talks including Introduction to VAPT, Bitcoin Forensics, OSINT at Null Pune chapter meets.
- Conveyed a one day workshop on Cyber Security Awareness at Symbiosis Institute of Technology, Pune, India.
- Conveyed a two-day workshop on Cyber Security Awareness at The Aryan International School, Varanasi, India.