Apurv Singh Gautam

apurv.gautam@gatech.edu

+1 (470) 439-1527

LinkedIn

Portfolio

EDUCATION

Georgia Institute of Technology   Atlanta, US
Master of Science in Cybersecurity (M.S.); GPA: 4.00   2019 - Expected 2021

Symbiosis Institute of Technology   Pune, India
Bachelor of Technology in Information Tehcnology (B.TECH); CGPA: 8.63   2015 - 2019

EXPERIENCE

Georgia Institute of Technology   Atlanta, US
Graduate Teaching Assistant   Aug 2019 - Present

- **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 Intelligence - Obtaining Intelligence from hack forums and dump shops
- **Work**: Scraped 5-10 GBs of dark web forum and dump shops data, constructed data collect systems for threat indicators in Elasticsearch and automated the collection process using Scrapy.

I-Medita, Pune   Pune, India
Trainee   Feb 2018 - May 2018

- **Area**: Cisco Networking
- **Learning**: Training for Cisco Certified Networking Associate (CCNA) with 90% practical approach including Router configuration, Switch configuration, and ACL configuration.

Lucideus Cyber Space   Delhi, India
Security Trainee   Dec 2014 and Dec 2016

- **Area**: Security Basics, Networking, Pentesting
- **Learning**: Networking Basics, Digital Footprinting, Email Security, System Security, Wireless Security, WAPT, and Network Pentesting.

SKILLS

- **Programming**: Proficient in Python, Java, and Bash. Fundamentals of C, C++, PHP, JavaScript
- **Security**: Threat Intelligence, Threat Hunting, Security Analysis, Security Automation, Network Security, Penetration Testing, Red Teaming, Blue Teaming

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

- **Assess network reputation through multiple threat intelligence data feed**: Research project that utilizes multiple threat intelligence feeds to assess network reputation and detecting & mitigating Volumetric anomalies using Machine Learning analysis using Python.
    - Uses PARAFAC tensor decomposition to decompose higher-order tensors in r order-1 tensors
    - Used 12-13 ASes Netflow data to asses network reputation.
    - Plotted several feature to determine the behavior of the these malicious infrastructures.
    - Used 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 research talking about Threat Intelligence with respect to Dark Web data in 2018.
  - Used Python's Scrapy framework to scrape data from dark web
  - Utilized ML & DL approaches in classifying data with precision above 95% for all the models used
  - Final result gave 96.56% precision for RNN GRU model
- **Anonymous Traffic Network**: A research paper describing the Onion routing concept, its working, and security issues. [Paper]
- **Question Mark**: Python web application that aims to serve as a platform where people can ask questions, share valuable knowledge and devise reliable solutions by answering the queries. The idea is to bring the knowledge from peoples head to a far-reaching platform where they can share and others can learn. **Flask Python Framework** is used. [Project]
- **Unnati (SPEP)**: Skilled People Emplyment Portal is a responsive Java web application that provides employment to skilled village people. HTML, CSS, JavaScript and Bootstrap is used for front end. Java Servlets and JSP is used for back end. [Project]
- **UserCred Hack**: Combination of several python application that grabs user credentials. Contains clipboard hijacking, keylogger and chrome password hijacking. Pyperclip, win32crypt, pythoncomm & pyHook modules are used. [Project]
- **Reverse HTTP Shell**: Python application that is used to get connection of client to the server using HTTP protocol. BaseHTTPServer module is used. [Project]

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, Governemnt of India**: Received Certificate of Achievement for securing 45th rank out of 1489 participants in 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 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 - creating security challenges for students.
- Successfully completed many trekking & mountaineering expeditions in different Himalayan ranges of India.
- Conducted Git & Virtualization Buddy Session for third year Computer Science students of SIT.
- Conducted NS3(Network Simulator) Buddy Session for third year Information Technology students of SIT.
- Conducted a Cyber Privacy Seminar at MITCOE Pune on behalf on Logout - Privacy Seminar. [Link]
- Delivered a talk on Bitcoin Forensics at Null Pune chapter meet. [Link]
- Delivered a talk on OSINT at Null Pune chapter meet. [Link]
- Delivered a talk on Intorduction to VAPT at Null Pune chapter meet. [Link]
- Delivered a small talk on Security News at Null Pune chapter meet. [Link]
- Conducted a one day workshop on Cyber Security Awareness at Symbiosis Institute of Technology, Pune, India.
- Conducted a two day workshop on Cyber Security Awareness at The Aryan International School, Varanasi, India.