ERIC NUNES

1215 E. Lemon Street, Apt #105, Tempe, AZ-85281
Website: https://efnunes.github.io/

Email: enunes1@asu.edu
Contact: 315-439-3089

SUMMARY

Computer Engineering Graduate student with 3 years' experience in research and development of data analysis tools. Hands-on experience with Python, R, SQL, C++, and MATLAB. Knowledgeable in processes and tools related to Big Data and Data Science.

EDUCATION

PhD in Computer Engineering **Present**
Arizona State University, AZ GPA: 4.0

Master of Science in Electrical Engineering **May, 2012**
Syracuse University, NY

Bachelor of Science in Electronics and Telecommunication **June, 2010**
University of Mumbai, India

TECHNICAL SKILLS

- **Machine Learning**: Classification, regression, clustering, anomaly detection, feature engineering, online learning, Experience with deep learning.
- **Programming Languages**: Python, MATLAB, C++, Prolog, HTML, LaTeX. Familiar with C, R.
- **Libraries**: scikit-learn, ElasticSearch, Weka, Pandas, Theano, Caffe.
- **Databases:** SQL, PostgreSQL**,** MongoDB.
- **Big Data and Cloud:** Splunk, Spark, Familiar with Big Data Processing Platforms: Hadoop and Cloud tools: Amazon S3.

KEY PROFESSIONAL AND RESEARCH EXPERIENCE

Data Scientist, Cyber Reconnaissance Inc. (CYR3CON**)** **August 2016 - Present**
Tools: Python, PostgreSQL, MongoDB, Spark.

- Designed a system to store and mine data from darknet markets and forums.
- Leading a team of developers and analysts to build tools/products for security applications. In particular, leveraging threat intelligence to build learning models for predicting likelihood of exploitation of a vulnerability (vulnerability prioritization), providing intelligence on Mobile threats (both Android and iOS applications), active threat assessment on client systems, named-entity recognition (to determine vulnerable software) using RNN/LSTM seq2seq models.

Security Automation Intern (Data Science), PayPal **May 2017- August 2017**
Tools: Python, Splunk, Spark.

- Analyzed user login activity using Akamai logs and enriched it with other data feeds such as threat intelligence, merchant data, credential dumps.
- Implemented operational Anomaly detection models to detect Account Takeover (ATO) attacks to raise alerts for automated mitigation.
- Visualized ATO attacks in real time on a dashboard in Splunk to aid risk to flag fraudulent transactions.

Research Consultant, CYR3CON (Client: SiteLock) **June 2016 - August 2016**
Tools: Python.

- Analyzed large dataset of malicious web scripts (PHP/HTML) to generate features indicative of malicious activity.
- Developed classification models to classify web scripts as malicious or not using the generated features in Python.
- **Achieved malicious script detection rate of >90%.**

Graduate Research Assistant, CySIS Lab, Arizona State University **August 2014 - Present**
Tools: Python, PostgreSQL, Prolog, tcpflow.

- Modeling of threat actors: Identifying cyber adversaries using argumentation and machine learning models (knowledge base: 10 million attacks).
- Proactive Cyber-Threat Intelligence: Built a system to crawl and parse the Darknet (markets and forums) to extract cyber threat intelligence including zero-day exploits using data mining and machine learning techniques. Identifying targeted software through disclosed vulnerabilities on Darknet.
- Malware task identification: Identifying the tasks that a piece of malware was designed to perform on the system (adversarial intent) using cognitive learning models.

PATENTS

- Systems and Methods for Data Driven Malware Task Identification. Submitted, 2016. **Provisional: 62/182,006**.
- Intelligent darkweb crawling infrastructure for cyber threat intelligence collection. Licensed to CYR3CON. **Provisional: 62/409,291. Technology featured in Forbes, MIT Tech Review, ACM TechNews, Cisco Continuum.**

REFERRED PUBLICATIONS

https://efnunes.github.io/publication.html