Noam Yakar

My Portfolio Site

Education

Arizona State University, Tempe 2021 – 2025

BSc Computer Science, BSc Mathematics (Statistics Focus) GPA 4.0

- **Coursework:** Real Analysis, Advanced Linear Algebra, Mathematical Statistics, DSA, OS, Stochastic Processes, Cryptography, Networks, Network Security, Systems Security, Digital Forensics

Technical Skills

Languages/Database: Python, R, SAS, C, C++, SQL, PowerBI
Relevant Libraries: TensorFlow, Keras, PyTorch, Scikit Learn, Shiny, GGplot, Pwntools
Software & Tools: GATK, DeepVariant, BWA-Mem, Snakemake, Databricks, AWS
Cybersecurity Competencies: Buffer Overflow Attacks, Return-Oriented Programming, Shellcode Injection, Race Conditions, Kernel Security Exploitation, Sandboxing, Dynamic Allocator Misuse, MicroArch. Exploitation

Experience

Nike - Data Engineering Intern (Oregon) Jun 2024 – Aug 2024

- Contributed to the development and optimization of data pipelines, ensuring efficient data flow and integration across various systems.
- Collaborated with cross-functional teams to support data-driven decision-making processes, leveraging advanced analytics and machine learning techniques.
- Implemented data validation and quality assurance protocols to maintain the integrity and reliability of large datasets.

ASU - Statistical Modeling Analyst (Arizona) Aug 2023 – May 2024

- Developed and implemented robust time series modeling techniques to forecast financial data, providing critical insights for informed decision-making.
- Applied time series forecasting methods, including ARIMA, Simple Exponential Smoothing, Holt-Winters Forecasting, to capture complex temporal dependencies in financial data.

Radware Inc. - Cybersecurity Data Intern (Tel Aviv) June 2023 – Aug 2023

- Developed a robust testing framework for validating a client alerts REST API through meticulous unit testing.
- Utilized a combination of cutting-edge dimensionality reduction techniques, including linear (PCA), non-linear (Kernel PCA), and manifold-based approaches (t-SNE, UMAP), to create low-dimensional representations of cyber attacks, enabling efficient clustering and analysis.
- Skillfully optimized and fine-tuned prominent tree-based machine learning models, such as XGBoost, Adaboost, and RandomForest, for accurate cyber-attack cluster characterization and improved classification.

Projects

Privacy Preserving Tool (Private Repo) | *Vega-Lite, Flask, Data Anonymization* **Aug 2024 - Present**

- Developed a Flask-based Vega-Lite editor enabling privacy-preserving visualization using *k-anonymity, l-diversity, t-closeness, and differential privacy.*
- Integrated real-time privacy metric computation and dataset transformation to balance data utility with protection.
- Implemented security measures to defend against statistical attacks and cyber threats, ensuring robust data privacy.

Pwn College - System Security Competitive CTF (Arizona) **Aug 2024 - Dec 2024**

- Ranked top 10 among over a thousand participants in the Pwn College Program and System Security Track.
- Excelled in Program Security modules such as *Shellcode Injection*, *Reverse Engineering*, *Intermediate Memory Errors*, *Return-Oriented Programming*, *Dynamic Allocator Misuse*, and *Program Exploitation* (All Time 151/6800).
- Developed exploits for System Security modules including *Sandboxing*, *Race Conditions*, *Kernel Security*, *Microarchitecture Exploitation*, and *System Exploitation* (All Time 168/2211).

WarGames: Secure Gradebook System | *Ethical Hacking, Python, Format String Exploit* **Feb 2025**

- Built a WarGames-inspired hacking simulation featuring admin credential cracking, format string exploits, and a DEFCON-based alert system (Educational CTF tool for students to exploit).
- Simulated real-world vulnerabilities, teaching exploitation techniques through gameplay-driven cybersecurity concepts.

SneakyPixel - Hack the Pixels, Hide Your Secrets | *Steganography, Cryptography, Flask* **Jan 2025**

- Developed a steganography tool to hide/extract encrypted messages in images using custom cryptographic keys.
- Ensured secure encoding/decoding while preserving image integrity, emphasizing privacy and secure communication.