Adrian Necaj

an9905@rit.edu || (347)-XXX-XXXX || Queens, NY
https://www.linkedin.com/in/anecaj/ || https://an9905.github.io/

EDUCATION:

Rochester Institute of Technology | Rochester, NY | *Bachelor of Science, Computer Security '24* | *Major GPA: 3.42*
Minor in Web Development | Immersion in Economics

Relevant Coursework: Programming for Info Security • Risk Management for Information Security • Cyber Security Policy & Law • Web Application Security • Systems Administration • Network Services • Disaster Recovery • Reverse Engineering Fundamentals • Penetration Testing • Intro to Cryptography • Computer System Security • Network Security and Forensics

- Member of Honors Society
- Deans List Recipient
- RIT Founders Scholarship Recipient
- RITSEC member

Certifications:

Google - IT Support Specialization Certification

SKILLS & ABILITIES:

Programming Languages: Python, C, Java, HTML, CSS, x86 Assembly, MySQL, C#
Scripting Languages: PowerShell, Python, Bash, JavaScript, PHP, JSON
Operating Systems: Windows, Mac OSX, Linux, UNIX, Kali Linux
Frameworks/Protocols: NIST, OWASP, MITRE & STRIDE, CSF, TCP/IP, FTP, SSH, DNS, DHCP, HTTP, SIEM, SOC, HIPAA
Software & Tools: Nmap, Wireshark, VirusTotal, Strings & FLOSS, PEiD, Dependency Walker, PEview, Resource Hacker, Regshot, Procman, Process Explorer, ApateDNS, Netcat, IDA Pro, x32dbg, Microsoft Office Suite, Word, PowerPoint, Excel
Other: Virtualization (VMWare), VPN, Active Directory, Blockchain, ServiceNow

EMPLOYMENT:

Jr. Application Administrator Intern | Rochester Institute of Technology | August 2022 – April 2023

- Applied ServiceNow application administration skills, proficiently implementing software updates, and leveraging ServiceNow "building blocks" to enhance system functionality.
- Evaluated and refined design approaches to align with specific requirements, consistently choosing the most suitable option for each request.
- Developed, rigorously tested, and seamlessly implemented enhancements, bug fixes, and projects in adherence to established standards, ensuring optimal system performance.
- Collaborated with cross-functional teams, including SecOps and ProCard, to integrate ServiceNow applications seamlessly into existing workflows.
- Crafted and optimized customized workflows tailored to the unique needs of various departments, streamlining operational processes, and improving efficiency.
- Demonstrated strong skills in Information Security and effective communication, contributing to a collaborative and secure IT environment.

PROJECTS:

AdrianHub - Personal Portfolio Actively Upkept

- Incorporated dynamic content to keep the portfolio updated and relevant, reflecting ongoing projects and skill advancements.
- Highlighted a diverse set of skills, technologies, and tools used across various projects, showcasing versatility and expertise in full-stack web development.
- Implemented Google Analytics to gather insights into website traffic, user behavior, and interactions.
- Utilized analytics data to refine the website's content, improve user experience, and track the performance of various projects.
- Leveraged Git for version control, allowing for the tracking of changes and maintaining a history of project iterations.

Malware Analysis - WannaCry, Academic Project Spring 2022

- Conducted in-depth analysis of live malware, specifically WannaCry, utilizing the MalwareDB (theZoo)
- Employed a combination of tools and techniques to execute both Static and Dynamic Analysis
- Established a controlled lab environment to facilitate a secure and controlled analysis process
- Leveraged a diverse set of software applications and tools, including Wireshark, x32dbg, VirusTotal, and more, to augment the analysis process and extract valuable insights from malicious code.

Risk Management, Academic Paper Fall 2021

- Conducted a comprehensive risk management analysis for a teaching hospital, involving the assessment of information and non-information assets in a specific security scenario.
- Utilized the FIPS 199 categorization to quantify the impact of potential threats on different information assets
- Employed industry-standard frameworks, including MITRE ATT&CK and STRIDE, to identify and analyze potential vulnerabilities in the hospital's security posture
- Utilized risk assessment methodologies to quantify and qualify potential risks, providing a structured foundation for the development of effective risk mitigation strategies.
- Developed comprehensive risk mitigations, ensuring a proactive approach to addressing identified vulnerabilities and reducing the overall risk exposure of the organization.