Nisanth Nadimpalli

(518)362-6879 | nisanth@nisanth.net | linkedin.com/in/nisanthn | github.com/astrophysx | blog.nisanth.net

Education

University at Albany, State University of New York Albany, NY
Bachelor of Science (BS) in Informatics (conc. Cybersecurity), Minor in Computer Science *Expected May 2024*

Experience

Security Operations Center Intern August 2023 – Present
New York State Office of Information Technology Services (ITS) *Albany, NY*

- Contributed to cybersecurity incident investigation and response activities, leveraging enterprise host and network-based security tools such as CrowdStrike Falcon, IBM QRadar, and CP4S.
- Utilized Splunk to analyze, collect, and visualize network traffic indices from New York State county offices, establishing a comprehensive network baseline and delivering actionable insights to the SOC team.
- Created Python and PowerShell scripts to streamline SOC procedures, automating repetitive tasks, improving operational efficiency, and expediting event response times.

Security Engineering Intern June 2023 – August 2023
IAT Insurance Group *Raleigh, NC*

- Orchestrated zero trust network and application security principles using Akamai Guardicore, contributing to the design of granular policies, network segmentation, and fortified access controls.
- Elevated threat response efficiency by crafting custom CrowdStrike Falcon Fusion Workflows against various threat types, significantly reducing manual triage times and optimizing incident resolution.
- Conducted comprehensive testing & contributed to the implementation of Duo multi-factor authentication (MFA) & user and entity behavior analytics (UEBA).

Security Research Intern March 2023 – June 2023
Pacific Northwest National Laboratory (PNNL) *Remote*

- Supported research for a PNNL project under the guidance of Dr. Terry Merz (senior research scientist), identifying emerging cyber-attack vectors targeting power & industrial control systems (ICS), focusing efforts on network edge intrusions at Layer 5 (Internet DMZ) of the Purdue Model.
- Analyzed tactics, techniques & procedures (TTPs) pertaining to threat actor APT29 and the SUNBURST malware family, utilizing the MITRE ATT&CK Framework to assist in the creation of adversarial emulation strategies.

Projects

Active Directory Home Lab | *DNS, DHCP, LDAP, TCP/IP*

- Configured and deployed an Active Directory environment utilizing various Windows Server technologies to simulate enterprise infrastructure.
- Created custom Group Policies to manage user access, software deployment, and system configurations within Group Policy Management Console (GPMC).

Cloud Deployed Honeypot | *Google Cloud (GCP), JSON, MHN*

- Engineered a low-interaction, network-accessible honeypot server utilizing Modern Honey Network (MHN) and Dionaea over HTTP (a honeypot used to trap malware samples) within Google Cloud.
- Created an attack surface vulnerable to network-based intrusions, logging attacks in real-time and capturing attacker information.

Leadership & Activities

UAlbany Cyber Defense Organization | Executive Board & Red Team Captain September 2021 - Present

- Conducted weekly presentations and workshops on offensive security topics for a diverse audience.
- Competed in the Collegiate Cyber Defense Competition (CCDC), Collegiate Penetration Testing Competiton (CPTC), CNY Hackathon & UB Lockdown.

Skills

Programming: Python, Java, C/C++, PowerShell, HTML/CSS, JavaScript, SQL, Go
Platforms: Linux, Windows, MacOS, pfSense, Amazon Web Services (AWS), Microsoft Azure
Software: Docker, Proxmox, VMware, Ghidra, Microsoft Office 365
Security Tools: CrowdStrike Falcon, Splunk, Metasploit, Burp Suite, Snort, Wireshark, Nmap