

# Hamil Dimapanat

IT Professional | Full-Stack Developer

📍 Yonkers, NY    ✉ dimapanat.hamil@gmail.com    ☎ 914-410-1081    🔗 hamil-dimapanat.com    in hamil-d

## Education

**BS**    **State University of New York at New Paltz**, Computer Science    Completed - 2023

## Certifications

**AWS Certified Cloud Practitioner** [🔗](#)    Mar 2024  
**CompTIA Security+ SY0-701** [🔗](#)    Dec 2024  
**Cisco CCNA**    Expected-April 2025

## Experience

**Mount Sinai Health System**, IT Desktop Support Specialist    New York, NY  
August 2024 - Present

- Provided end-user support via ServiceNow, resolving hardware & software issues.
- Developed web app (**PSON IT**) for troubleshooting and deployed with Github Pages.
- Reimaged workstations, updated and patched drivers and softwares.
- Managed VoIPs, Laptops, Printers, Scanners, and Mobile Devices.
- Handled relocations, upgrades, and device provisioning.
- Configured access permissions and identity management (IAM) through SailPoint.
- Administered Google Workspace, SharePoint, Moodle LMS, Echo360, and Zoom.

**Code Nation**, Web Development TA    New York, NY  
August 2023 - Dec 2023

- Delivered web development instruction (HTML, CSS, JavaScript, React) to middle school students via hands-on projects.

## Projects & Labs

**SUNY New Paltz TicketSense** - (Spacy, FastText, Jupyter, Flask)    [github.com/hvmil](https://github.com/hvmil) [🔗](#)

- Used Python, SQL and a dataset of over 10,000 tickets to train a classifier model.
- Aimed at reducing resolution times by helping service desk escalate tickets.
- Deployed on Heroku and used Flask web framework.

**VMware Microsoft Windows Server 2019**

- Used VMware to host Windows Server 2019 and Active Directory Domain.
- Automated account creation and data processing with Powershell scripts.
- Managed user accounts, groups, and Group Policy Objects (GPOs) for security and user management.

**CCNA Packet Tracer Lab**

- Configured Cisco routers, switches, and VLANs using Cisco IOS.
- Managed routing protocols, access points, and basic network segmentation.
- Resolved connectivity issues and applied security measures with ACLs and firewalls.
- Gained a deep understanding of OSI layers 1-4 and protocols such as DHCP, DNS, and TCP/IP.

**Try Hack Me Lab**

- Configured firewall rules and monitored Splunk SIEM for threat detection.
- Executed buffer overflow attacks using Bash and Python.
- Performed network scans and vulnerability assessments with Nmap and Nessus.
- Analyzed logs, set IDS/IPS alerts, and implemented endpoint security.

## Technologies

**Languages/Scripting:** Python, Bash, Powershell, JavaScript/TS  
**Networking:** Cisco IOS, Routing & Switching, VLANs, Firewall Configuration  
**Cybersecurity:** SIEM (Splunk), IDS/IPS, Vulnerability Scanning (Nmap, Nessus)  
**Tools & Systems:** SIEM (Splunk), IDS/IPS, Vulnerability Scanning VMware, Active Directory, SailPoint, Linux, AWS  
**Databases & Development:** SQL, MongoDB, Full Stack (React, Node.js)