MATTHEW YAMAMOTO

IT Professional

Los Angeles
☎ +1 424-237-6641
@ mlyhoops@gmail.com
github.com/mlyhoops
in matthewyamamoto1197

OBJECTIVE

Seeking a challenging and rewarding position in Linux System Administration, leveraging my extensive knowledge of Linux-based operating systems, server management, and cybersecurity to contribute effectively to an organization's IT infrastructure, ensuring optimal performance, security, and scalability. My goal is to apply my skills and passion for problem-solving to enhance system stability, streamline operations, and support the growth and success of the company.

SKILLS

- Python and SQL
- Oracle VirtualBox/VMWare/Hyper-V
- Linux (CentOS and Ubuntu)
- OpenLDAP
- Shell Scripting
- NAS Drive/RAID
- HTML/CSS
- Microsoft Active Directory
- Windows Server 2019

EDUCATION/CERTIFICATION

Security+ SY0-601: (Click for Certificate) — **COMPTIA**
Passed the COMPTIA Security+ Exam. Verification code: 9M93JTK5PBFEQ2SL

Linux Administration in CentOS — **Udemy Courses and Labs**
Hands on labs learning advanced Linux systems administration skills with a deep understanding of Linux fundamentals and concepts. Topics include: Virtual Machine Management, System Administration, Shell Scripting, Linux Fundamentals, Networking, Services, System Updates, Disk Management, and Run Levels.

Windows Server 2019 Administration — **Udemy Courses and Labs**
Hands on labs creating Windows Servers on virtual machines. Key topics include Windows Server Administrative tools, PowerShell, Group Policy, DNS, DHCP, file server management, creating and managing virtual machines, implementing failover clustering, disaster recovery using Windows Backup, Windows Server Security, monitoring performance, managing Active Directory Users, Computers, Groups and more.

Google Cybersecurity Professional Certificate: (Click for Certificate) — **Coursera - Google Career Certificates**
Learned Cybersecurity practices, common risks, threats, and vulnerabilites, and how to protect networks, devices, and people from unauthorized access and cyberattacks. Related labs included tools such as Wireshark, tcpdump, Splunk, Linux, Python, SQL, and the NIST RMF.

Master's Degree in Computer Science — **California State University Dominguez Hills**
Currently pursuing my masters in Computer Science but taking a year break due to course availabilty and schedule conflicts with work. Finished 1 year and need to complete 1 more year.

Bachelor's Degree in Computer Science — **California State University Dominguez Hills**
Completed my Bachelors of Science in Computer Science.
Courses include: Data Management, Probability and Statistics, Data Structures, and AI.

WORK EXPERIENCE

IT Operations Support: 2020-Present — **Cogo Systems**
- Used Crystal Reports/SQL/CCTV/Logs to research and report incidents to save the terminal thousands.
- Tested Terminal OS to make sure upgrades worked seamlessly and tested for issues that operations had.
- Documented Service Desk tickets and tasks completed for each shift.
- Worked with labor union/ops management/3rd parties regarding the terminal OS and automation.
- Created Python scripts and Excel macros in my own time to save me time on daily tasks.

PROJECTS

Media Server — **Ubuntu**
- Installed Ubuntu Server on an old PC to create a private cloud with NextCloud.
- Ran tailscale as T-Mobile Home internet did not allow for port forwarding due to Carrier-Grade NAT.

Virtual Backup — **Windows 10**
- Converted my XPS13 laptop into a virtual machine as it was getting old and taking up space.
- Utilized Disk2vhd to convert the physical disk into a VHDX file then converted the VHDX file into a VDI file
- Used the VDI file in Virtual Box to run Windows with the full backup of the laptop.

Analyze Network Traffic with TCPDump: (Click for Project Certificate) — **Coursera Project Network**
- Utilized tcpdump to capture and analyze TCP packets in a virtual linux environment

Wireshark Packet Capture: (Click for Project Certificate) — **Coursera Project Network**
- Installed and set up Wireshark on Ubuntu
- Utilized a display filter to analyze HTTP/S traffic and detect IP Addresses in packets