Cybersecurity Home Lab - Summary

This is a self-directed, enterprise-grade cybersecurity home lab built to simulate real-world attack and defense scenarios.

The lab is fully modular, virtualized, and cloud-integrated, allowing for deep hands-on practice across red, blue, and purple team disciplines.

Lab Stack

- Proxmox VE / VMware
- Ubuntu, Kali, Mint, Fedora, Windows Server, Security Onion
- AWS (EC2, S3), Terraform, Tailscale
- pfSense/OPNsense, VLANs, NAT, DNS, DHCP

Security Tools

- Splunk, Wazuh, Zeek, Suricata, ELK Stack
- Ghidra, x64dbg, radare2, Sysinternals
- Wireshark, Sysmon, Fail2Ban, CrowdSec

Key Projects

- Active Directory Lab with GPOs and Windows Clients
- Threat Detection with Security Onion + Wazuh
- Cloud Lab with Terraform & Tailscale Subnet Router
- Malware RE with Ghidra and isolated sandboxes
- Honeypot telemetry and alerting via ELK stack

Objectives

- Simulate attacks & defenses in an enterprise-like network
- Practice log analysis, SIEM tuning, and threat hunting

- Develop cloud security and infrastructure automation skills

- Reverse engineer malware samples in a secure environment

Contact

GitHub: github.com/mchyasn

LinkedIn: linkedin.com/in/mchyasn