Mythreya Hardur Madhukeshwara

hm.mythreya@gmail.com • +1 (240) 886-7232 • in/hmmythreya • github.com/hmMythreya
portfolio: hmmythreya.github.io • blog: medium.com/@hm.mythreya

TECHNICAL EXPERIENCE

SOC LAB WITH WAZUH, SHUFFLE, AND THEHIVE — Write Up

- Deployed **Wazuh** in the cloud, integrating with a Windows 10 client to monitor over **100 security events** daily.
- Developed custom Mimikatz detection rules, reducing incident response time by **50%** for credential theft threats.
- Integrated Wazuh with **Shuffle** to automate threat intelligence by sending Mimikatz alerts to **VirusTotal**
- Forwarded VirusTotal results to **TheHive**, enabling SOC teams to triage alerts in real-time for faster response

CYBERSECURITY INCIDENT RESPONSE PROJECT – HEXANET SOLUTIONS — Report

- Led incident response for a **simulated ransomware attack**, isolating infected systems and restoring operations within 72 hours using backups
- Analyzed the incident using the **NIST Cybersecurity Framework**, identifying gaps in phishing defenses, access control, and detection mechanisms
- Implemented post-incident improvements, including deploying Endpoint Detection and Response (**EDR**), enhancing **SIEM** capabilities, and conducting phishing awareness training

ELASTIC STACK SIEM CONFIGURATION IN HOME ENVIRONMENT — Write Up

- Configured elastic agents in kali and ubuntu, for **log collection** and **security event monitoring**
- Fabricated over **60 nmap alerts** to test the working of SIEM

AIG CYBERSECURITY VIRTUAL JOB SIMULATION - FORAGE — Cert

- Utilized **Python** to write a script for **bruteforcing** decryption keys
- Researched and understood reported vulnerabilities, showcasing analytical skills in cybersecurity.

TELSTRA CYBERSECURITY VIRTUAL JOB SIMULATION - FORAGE — Cert

- Engineered and implemented a **firewall** using a custom **Python** script to block malicious traffic

MALWARE DEV — Write Up

- Designed malware with memory usage of less than **100Kb** that can inject itself to any running process' memory address and **execute in under 10ms**
- Generated shellcode of length of just **232 bytes** using **metasploit** and **msfvenom**.

PROBEX - PORT SCANNER — Github Repo

- Built a lightweight CLI tool in python to scan a port on any host on the network in **less than 0.05s** sometimes up to **10 times faster than nmap**

EDUCATION

UNIVERSITY OF MARYLAND — **COLLEGE PARK, MD**
M.ENG IN CYBERSECURITY ENGINEERING — **EXPECTED 05/26**

PES UNIVERSITY — **BANGALORE, INDIA**
B.Tech in Computer Science Engineering - Specialization in Networks and Cybersecurity — **2020-2024**

SKILLS, CERTIFICATIONS AND TECHNOLOGIES

Certifications: CompTIA Security+ (2024), **Qualys VMDR** (2024), **OSCP** (expected jan 2025)
Skills and Technologies: Python, nmap, C++, metasploit, Raspberry Pi, Linux, Git, Kali