Mythreya Hardur Madhukeshwara

240-886-7232 | hm.mythreya@gmail.com | linkedin.com/in/hmmythreya | github.com/hmMythreya | portfolio | blog

Education

University of Maryland — College Park, MD
Masters of Engineering in Cybersecurity — *Aug. 2024 - Present*

Coursework: Penetration Testing, Digital Forensics and Incidence Response
Hacking of C Programs and Unix Binaries

PES University — Bangalore, KA, India
Bachelor's in Computer Science Engineering — *Dec 2020 - May 2024*

Coursework: Computer Network Security, Information Security, Applied Cryptography
Cloud Security, Automotive Cybersecurity, Blockchain

Skills and Certifications

Certifications: CompTIA Security+, Qualys Certified Specialist, Linux Kernel Development LFD103, Cloud Computing 101, OSCP+ (expected feb 2025)

Languages: Python, SQL (Proficient), C/C++ (Intermediate), Java, Rust (Beginner)

Tools and Technologies: Nmap, metasploit, msfvenom, john the ripper, hashcat, netexec, gobuster, wireshark, burpsuite, gophish, mythic, Linux, Git, Raspberry Pi, Docker

Technical Experience

SOC Lab | ***Wazuh, TheHive, Shuffle*** — 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

Elastic Stack SIEM configuration — Write Up

- Configured elastic agents in Kali and Ubuntu, for log collection and security event monitoring
- Acquired skills for querying logs and setting up alerts for nmap activity for both agents
- Fabricated over 60 nmap alerts to test the working of SIEM
- Built dashboards to visualize security events and trends over time

Malware Dev | ***C++, msfvenom, Windows API*** — 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.
- Used Windows API (Windows.h in C++) and it's respective functions like VirtualAllocEx(), CreateRemoteThread() to inject malware to existing processes

Home Lab and VPN setup | ***Raspberry Pi 5, WireGuard, PIVPN***

- Installed, setup, and configured Ubuntu Server 24.04.1 LTS on a raspberry pi 5
- Configured router settings to allocate static IP to rpi5 and setup port forwarding rules
- Installed and configured a VPN server on rpi5 with pivpn, duckdns and wireguard, allowing secure access to home network from anywhere in the world

probeX | ***Python, Scapy*** — 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
- Implemented source IP spoofing and fragmentation to make it hard to be detected by a weak firewall
- Gained strong understanding of network protocols and packets (TCP, SYN packets) and port scanners
- Learnt how to construct raw packets from scratch using the scapy python module