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*

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

Skills and Certifications

Certifications: **OSCP+**, **CompTIA Security+**, **Dante HTB-PROLAB**, **Qualys VMDR** (Vulnerability Management, Detection and Response), Cloud Computing 101

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, Linux, Git, Raspberry Pi, Docker

Technical Experience

SOC Lab | *Wazuh, TheHive, Shuffle* Write Up

- Deployed and configured Wazuh, a **host-based intrusion detection system** (HIDS), in a cloud environment, integrating it with a local Windows 10 endpoint to monitor and analyze over **100** daily security events across multiple sources including system logs, application logs, and security alerts.
- Designed and implemented custom Mimikatz **detection rules**, reducing incident response time by **50%** and enhancing the SOC's threat mitigation capabilities.
- Streamlined incident response operations by integrating VirusTotal scan results with TheHive, allowing SOC teams to efficiently triage alerts, correlate them with other events, and conduct faster forensic analysis to prioritize and mitigate emerging security threats.

Elastic Stack SIEM configuration Write Up

- Configured and deployed Elastic Stack agents on Kali Linux and Ubuntu to effectively collect, process, and analyze security event logs from multiple endpoints, ensuring comprehensive network visibility and **incident detection**.
- Gained expertise in querying logs for patterns of suspicious activities, such as Nmap scans, enabling enhanced threat hunting capabilities and early detection of potential security breaches.
- Fabricated over **60 Nmap scans** to test alerts, improving the SIEM's rule accuracy and ensuring that critical security events, like port scanning and network reconnaissance, were accurately detected and flagged for immediate investigation.
- Created custom Kibana dashboards that visualized trends in security events, attack patterns, and system anomalies, providing the team with actionable insights and historical data for improved incident investigation and decision-making.

Malware Dev | *C++, msfvenom, Windows API* Write Up

- Developed a highly efficient, memory-optimized malware sample (under **100KB**) capable of self-injecting into the memory space of existing processes, enabling it to execute without triggering common detection mechanisms. The malware can execute under **10ms**, demonstrating significant performance optimization in real-world scenarios.
- Employed Windows API functions, specifically VirtualAllocEx and CreateRemoteThread, to perform process injection into target applications, effectively evading basic security mechanisms and enabling deeper exploration of exploitation strategies in a Windows environment.

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

- Successfully installed, configured, and secured Ubuntu Server 24.04.1 LTS on a Raspberry Pi 5
- Configured static IP addressing for the Raspberry Pi 5 and established port forwarding rules on the home router, enabling secure remote access for management, testing, and penetration testing activities.
- Installed and configured Damn Vulnerable Web Application (**DVWA**) and **Metasploitable 3** in the home lab environment, allowing for hands-on practice with **penetration testing** techniques and tools, such as **Metasploit, Nmap, Burp Suite, and Nessus**, within a safe and isolated environment.