225-505-3542
Baton Rouge, LA
saugat_ghimire@outlook.com

Saugat Ghimire

My Website
GitHub: sghimi
LinkedIn: sghimi

Education

Bachelor of Computer Science; concentration in Cybersecurity **August 2020 - May 2024**
Louisiana State University (GPA: 3.5)

Relevant Coursework: Data Structures and Algorithms, Digital Forensics, Mobile Security and Cryptography, Operating Systems, Reverse Engineering and Malware Analysis, Computer Networks, and Software Vulnerabilities and Exploitation

Awards: TOPS scholarship recipient, Dean's list (Fall 2020, Spring 2021, Spring 2022, Spring 2024)

Work Experience

IT Technician **Feb 2023 - current**
MMR Group *Baton Rouge,LA*

- Utilized PowerShell scripting to automate routine IT tasks, including user management in Azure AD, mailbox management in Microsoft Exchange, and other administrative processes.
- Continuously monitored and identified insecure systems, contributing to the security team's efforts by reporting and mitigating vulnerabilities like local admin usage or missing EDR solution.
- Tools used: Active Directory, Microsoft Teams, PowerShell

IOT Forensics Researcher **Jan 2023 - May 2023**
LSU *Baton Rouge,LA*

- Solo project in the analysis of iRobot app's HTTP/S traffic to understand data exchange between app and Roomba vacuum cleaner.
- Developed a tool for forensic investigators to use to gather iRobot cloud data that could be used in criminal investigations.
- Tools used: Burp Suite, MITMProxy, Wireshark, Python, Frida, Apktool

---

Projects

The Phish Initiative **2022**

- Aimed to help system administrators test the susceptibility of their employees to phishing scams.
- Assisted in the implementation of the server-side code using Java and AWS services, which included configuring and integrating the backend with the frontend website.

Home Lab Environment **2024**

- A comprehensive home lab environment to simulate enterprise-level infrastructure and for security testing.
- Configured a Windows 2016 Domain Controller with GPOs for WEF server configuration, Powershell logging, and enhanced Windows auditing policy.
- Established Windows Event Forwarder server on Windows 2016 Server, integrating Microsoft Advanced Threat Analytics.
- Implemented a logging server on Ubuntu 16.04 with Splunk, Fleet for endpoint visibility and tools like Suricata (IDS/IPS), Zeek (network monitoring), and Velociraptor (DFIR)

Skills

Languages	Python, C, SQL, JavaScript, Bash, Assembly
Tools	Linux, Wireshark, Autopsy, Splunk, Nmap
Frameworks	NIST, ISO, MITRE ATT&CK, CIS
Cetifications	CompTIA Security (2023) +, CySA + (pursuing)