Logeshwar S

Email : logeshwar.0512@gmail.com
Information Security Analyst
Mobile : +91 8825759647
LinkedIn, Github, Medium

Projects

- **IDS Integration with SIEM for Intrusion Detection and Monitoring**:
  - Created and configured a virtual network environment including Kali Linux (attacker), Ubuntu Server (Splunk), Ubuntu PC (Snort and Splunk), and Metasploitable2 (vulnerable machine).
  - Installed and set up Snort on Ubuntu, writing and implementing custom intrusion detection rules.
  - Deployed Splunk on Ubuntu Server, configuring it to receive and monitor Snort alert logs.
  - Conducted attack simulations using Kali Linux to test and validate the intrusion detection system.
  - Utilized Splunk's Snort dashboard to analyze and monitor security events, effectively identifying potential threats.
- **Malware Analysis Sandbox** :
  - Installed and configured FlareVM and REMnux on VirtualBox for comprehensive malware analysis.
  - Secured and isolated the virtual environment using a host-only network adapter to prevent malware spread.
  - Conducted static malware analysis using tools like VirusTotal, FLOSS, PEview, PEiD, and PE Studio.
  - Performed dynamic malware analysis with Procmon, CFF Explorer, and TCPView.
  - Simulated a fake internet environment using INetSim, capturing and analyzing network traffic with Wireshark.
- **Network Traffic Analysis using Wireshark**:
  - Performed in-depth analysis of network traffic using Wireshark, focusing on protocol behavior and data flow.
  - Investigated and decoded various network protocols, including HTTP, TCP, UDP, DNS, and SSH.
  - Applied advanced display filters to examine specific traffic patterns in detail.
  - Compiled comprehensive analysis reports identifying network performance issues, security vulnerabilities and optimization opportunities.

Technical Skills

- **Programming Languages**: Python ,C++ ,Bash, SQL ,PowerShell
- **Technologies & Tools**: Git, GitHub, Hypervisor (VirtualBox) , Wireshark, IDS (Snort), SIEM (Splunk), Windows Firewall, Active Directory
- **Technical Concepts**: Linux System Administration, Networking Traffic Analysis, Network Security, Incident Response, Malware Analysis, Log analysis, Threat Intelligence, Vulnerability Assessment
- **Additional Skills**: Scripting, Automation, Cloud (AWS), Data Science, Web Development, API

Certifications

- **Google Cybersecurity Specialization**: Coursera
- **Comptia Security plus (In-progress)**: Comptia
- **Python for Data Science, AI & Development**: Coursera
- **Introduction to Linux LFS101**: The Linux Foundation

Education

- **PSG Institute of Technology and Applied Research** Tamil Nadu, India
  Bachelor of Engineering in Electrical and Electronics; CGPA: 8.21 *Oct. 2020 – Jun. 2024*
- **Delhi Public School** Tamil Nadu, India
  Higher Secondary Education; Percentage: 87% *Aug. 2018 – July. 2020*

Publications

- **Elephant Detection and Alarm System Using TensorFlow**: S. Ravikrishna, C. S. S. Kumar, V. Sharan, V. S. Kumar and S. Logeshwar, ”Elephant Detection and Alarm System Using TensorFlow” 2023 International Conference on Intelligent Technologies for Sustainable Electric and Communications Systems (iTech SECOM), Coimbatore, India, 2023