
PROFESSIONAL SUMMARY:

Cybersecurity Analyst with a Master's in Cybersecurity (GPA 3.9) and hands-on experience in penetration testing, threat detection, SharePoint automation, and Power Platform development. Proven ability to reduce manual effort by up to 95% and improve system security using tools like Metasploit, Wireshark, Splunk, and Nessus. Seeking a full-time role to apply my skills in cybersecurity operations and secure infrastructure development.

EDUCATION:

Saint Louis University

Master of Science Cybersecurity | GPA: 3.9

May 2025

SKILLS:

Cybersecurity

- Metasploit
- Nmap
- BurpSuite
- Nessus
- Wireshark
- Splunk
- PfSense
- Aircrack-ng
- SDR
- Social Engineering
- SQLMap

Security Skills

- Vulnerability Assessment
- Penetration Testing
- Incident Response and Protocols
- Data Administration
- Incident Response and Mitigation
- Cloud Security
- Network Security
- Digital Investigation
- Intrusion Detection and Analysis
- Cyber threat and Defense
- MITM Attack Framework

Skills

- Python
- Java
- PHP
- SQL
- JavaScript
- Scripting
- SharePoint
- Power Tools

WORK EXPERIENCE:

PhD Student Worker (IT and SharePoint Support)

MARCH 2025 – MAY 2025

School of Social Work, SLU | Saint Louis, MO

- Built and deployed a SharePoint site for the PhD program, streamlining resource access and improving team collaboration efficiency by 40% — gained hands-on experience with SharePoint architecture and user permissions.
- Developed a two-way sync between Outlook Calendar and SharePoint using Power Automate, reducing manual updates by 95% and eliminating duplicate entries through conditional logic and EventID checks.
- Designed and implemented customized SharePoint calendar tiles with JSON formatting, improving readability and UI consistency by 70%.
- Optimized Power Automate flow structure to reduce API call volume by 40%, maintaining full 31-day event visibility while avoiding throttling.
- Managed backend systems and supported SLU's web infrastructure, improving IT issue resolution time by 30% and enhancing data security and file accessibility by 35%.

CYBERSECURITY ANALYST INTERN

APRIL 2022 – JULY 2022

TechTwins Technologies | Jaipur, India

- Conducted vulnerability assessments and penetration testing using Metasploit, Nmap, and Nessus, identifying and mitigating CVE vulnerabilities such as CVE-2020-0796 and CVE-2021-34527, reducing security risks by 40%.
- Performed Wireshark-based network traffic analysis to detect anomalies, improving incident response effectiveness and system security by 30%.
- Developed an automated security compliance tracking system in Google Sheets to streamline risk assessment and reporting, improving efficiency by 25%.
- Implemented privilege escalation techniques and secure remote access protocols on Windows Server 2006, 2019, and Active Directory, enhancing system security.
- Delivered technical reports and security findings to cross-functional teams and non-technical stakeholders, driving discussions on regulatory compliance and security best practices.

PROJECTS:

Autonomous Vehicle Cybersecurity Project – Master's Research Project 2025

- Developed an automated compliance monitoring tool to detect unauthorized access and improve vendor security assessments in in-vehicle systems.
- Performed penetration testing on third-party communication protocols using Burp Suite and Metasploit to identify supply chain vulnerabilities.
- Integrated Splunk for real-time security logging and analysis, improving threat detection capabilities.
- Assessed risk analysis and compliance tracking using ServiceNow and Google Sheets to enhance regulatory compliance with ISO 21434 and GDPR.

Wi-Fi Security & Penetration Testing Tool - Present

- Designed a custom cybersecurity tool for Wi-Fi network analysis and penetration testing, utilizing Aircrack-ng, Nmap, and Wireshark.
- Captured and analyzed 4-way handshake traffic to identify weak encryption protocols and simulate real-world third-party security breaches.
- Integrated automated reporting features with Microsoft Excel & Office Suite, enabling network risk assessment visualization.

GUI Packet Sniffer - 2024

- Developed a Python-based GUI tool for packet sniffing and network monitoring, capturing over 10,000 network packets and improving data analysis efficiency by 40%.
- Implemented Nmap-based scanning features for real-time network mapping and anomaly detection.
- Reduced troubleshooting time by 30% through advanced packet filtering and analysis similar to Wireshark.

Image Steganography Tool - 2024

- Achieved a 98% success rate in encoding and retrieving hidden messages, validated through testing on 1,000+ images, ensuring robust and reliable data concealment.
- Enhanced user accessibility by integrating both CLI and GUI interfaces, boosting user adoption by 50%.
- Documented the project's methodology and presented the findings to peers and mentors, showcasing clear communication and technical writing proficiency.

Password Cracker - 2024

- Achieved a 95% success rate in cracking passwords using SHA-256 hash-based dictionary attacks, processing each password in under 2 seconds on average.
- Improved recovery efficiency by 25% compared to baseline tools through performance optimization.

Cybersecurity Audit & Live Assessment - 2023

- Conducted a 7-day live cybersecurity audit across multiple locations, assessing critical systems and internal security controls. Led a 3-day technical training program, equipping teams with Lansweeper, Pcaudit, and web hacking techniques, resulting in a 20% reduction in system vulnerabilities.
- Collaborated with the Chief Security Analyst, gaining hands-on experience in risk assessment, penetration testing, and compliance auditing.
- Evaluated and strengthened the security posture of examination systems, ensuring data integrity and regulatory compliance.

Keylogger Program - 2023

- Logged and transmitted 1,000+ keystroke sequences during testing, demonstrating the program's accuracy and reliability.
- Reduced user setup time by 20% with streamlined email reporting integration and stealth functionalities.

CERTIFICATIONS:

- Microsoft Az-900
- AWS Educate Getting Started with Networking
- AWS Educate Introduction to Cloud 101
- AWS Educate Getting Started with Cloud Operations
- EC-Council Ethical Hacking Essentials
- EC-Council Digital Forensics Essentials
- EC-Council Network Defense Essentials
- Website Hacking Techniques
- Wireshark
- Modern Web Application Hacking