DONATUS JUNIOR NWAOYIBO

+49 160 4077150 | newdonatusjnr22@proton.me
Berlin, Germany | GitHub: Privitjay

Mechanical Engineer | IT Support Specialist | Cybersecurity Analyst
Technical Project Coordinator | Infrastructure & Systems Admin | Customer Support Professional| Project Management

---

Professional Summary

I'm a versatile and tech-savvy professional with a Bachelor's in Mechanical Engineering and a Master's in Global Production Engineering from TU Berlin. My experience spans IT support, system administration, cybersecurity projects, customer service, and project coordination. I've worked in both technical and user-facing environments and enjoy solving problems that combine technology, communication, and real-world impact. I'm especially interested in roles that intersect IT operations, cybersecurity, smart manufacturing, and digital project management.

Core Competencies

• IT Support & System Administration

• Cybersecurity Auditing & Compliance Assessment

• Malware Analysis & Threat Detection (FLARE VM, REMnux)

• Vulnerability Scanning & Penetration Testing (Nmap, Metasploit, Hydra, Nikto)

• Project Coordination & Cross-Functional Team Collaboration

• Technical Documentation & Security Reporting

• Customer Communication & Analytical Problem Solving

• Microsoft 365 | Windows Server | VirtualBox | VMware | GitHub

• Smart Manufacturing & Digital Platforms

• Agile & Waterfall Methodologies

Professional Experience

Student Assistant – Technical Support & Research
Technical University Berlin | 2022 – 2025

- Supported IT platforms and infrastructure for the Global Conference on Sustainable Manufacturing (GCSM).
- Assisted in research involving digital production, Industry 4.0, and additive manufacturing.
- Provided technical support for academic teams and virtual event setups.

System Administrator / Dispatcher
Echo Express | 2021 – 2022

- Handled backend platform administration and dispatch operations.
- Delivered first-line IT support and helped troubleshoot technical issues.
- Maintained system reliability and supported coordination with technical teams.

Customer Service Representative
Specialty Life | 2020 – 2021

- Supported clients in the insurance industry via phone and email.
- Managed data entry, customer inquiries, and coordinated with internal teams.
- Used CRM systems to track issues and ensure timely resolutions.

System Admin / Customer Service
Fix Local | 2018 – 2019

- Provided tech support and monitored online service platforms.
- Helped users connect with local service providers and ensured issue tracking.
- Bridged communication between clients and the technical team.

Key Projects

Vulnerability Scanning & Mitigation Project (2024)

Environment: VirtualBox, Metasploitable 2, Kali Linux

Conducted a hands-on security assessment project focused on identifying and mitigating system vulnerabilities using Metasploitable 2 as the target environment. Leveraged industry-standard tools and techniques to simulate real-world attacks, analyze vulnerabilities, and propose effective mitigation strategies.

Key Responsibilities:

- Deployed a virtual lab with Metasploitable 2 (target server) and Kali Linux (attacking machine).
- Performed network and vulnerability scans using **Nmap**, **Nikto**, and **Dirb** to map open ports, services, and web application weaknesses.
- Used **Metasploit** for exploitation of known vulnerabilities and testing system resilience.
- Applied **Hydra** for brute-force attack simulations on login services.
- Conducted enumeration using **Enum4linux** to extract SMB and NetBIOS information.

- Documented findings and recommended mitigation techniques such as patching, service hardening, and configuration changes.

  Outcome: Successfully identified multiple critical vulnerabilities and outlined remediation steps to improve system security posture.
  https://github.com/Privitjay/Vulnerability-Scanning-and-Mitigation

Self-Hosted-Malware-Analysis-Lab

Environment: VMware, FLARE VM, REMnux

Designed and implemented a self-contained malware analysis lab to safely detonate, analyze, and reverse-engineer malicious software in a controlled environment.

Key Responsibilities:

- Configured VMware to host isolated virtual machines for secure malware experimentation.
- Deployed FLARE VM on a Windows guest system, equipping it with industry-standard tools for static and dynamic malware analysis.
- Integrated REMnux as a Linux-based analysis and command-and-control (C2) simulation platform to capture, monitor, and analyze malware network behavior.
- Performed static analysis (disassembly, string analysis) and dynamic analysis (runtime behavior, process monitoring) of malware samples.
- Simulated malicious network traffic and C2 interactions to observe communication patterns and extract Indicators of Compromise (IOCs).

Outcome: Developed a secure and functional lab environment for malware research, enhancing practical reverse engineering and network forensics skills.
https://github.com/Privitjay/Self-Hosted-Malware-Analysis-Lab

Security-Audit-Of Botium Toys

Scope: Organization-wide IT assets, network infrastructure, and systems

Conducted a comprehensive security audit of Botium Toys' IT environment to assess current asset management, security controls, and compliance with best practices.

Key Responsibilities:

- Reviewed and documented all IT-managed assets, including employee devices, internal network components, and core systems.
- Assessed existing security controls (e.g., access controls, encryption, patch management) against industry standards and organizational policies.
- Completed a detailed controls and compliance checklist to evaluate alignment with frameworks such as ISO 27001 and NIST.
- Identified gaps and risks within current practices and proposed strategic improvements to enhance the organization's overall security posture.
- Delivered a final report outlining key findings, prioritized recommendations, and compliance enhancement strategies.

Outcome: Provided actionable insights to strengthen Botium Toys' cybersecurity posture and improve adherence to compliance standards.
https://github.com/Privitjay/Vulnerability-Scanning-and-Mitigation

---

🎓 Education

MSc. Global Production Engineering *(Ongoing)*
Technical University Berlin
Focus: Project Management, Product Innovation, Smart Manufacturing

BSc. Mechanical Engineering
Technical University Ternopil | 2015 – 2019

📜 Certifications

- Six Sigma Certification – TU Berlin
- Ethical Hacking Bootcamp – Udemy
- Clifford Chance Cybersecurity Simulation – Forage
- SOC Level 1 - TryHackMe

💬 Languages

- English – Fluent
- Ukrainian – Intermediate
- German – Basic