John Pennie

Chicago, IL 60641

(773)-706-3651 **jrpennie@proton.me** linkedin.com/in/john-pennie github.com/jrpennie jrpennie.us

Education

DePaul University **Aug 2022 – Nov 2025**
Bachelors of Science in Cybersecurity
Minor in Computer Science

Certifications

Currently pursuing CompTIA Security+ and Network+, additionally studying for Certified Information Systems Security Professional (CISSP)

Experience

IT Operations Analyst **Aug 2019 – Present**
Starbucks *Chicago, IL*

- Provide Tier 2 support for approximately 40 users across Windows workstations, Microsoft 365, applications, and network connectivity issues.
- Resolve an average of 45 support tickets per week involving Windows systems, Microsoft 365, VPN access, endpoint security, software issues, and business application support.
- Manage user accounts in Active Directory and Microsoft 365, including MFA, permissions, groups, and access changes.
- Install, update, and troubleshoot software across Windows workstations to maintain secure, reliable, and properly functioning endpoints.
- Monitor file server backups and storage, supporting recovery testing and data availability.
- Support VPN and remote access issues for off-site users.
- Triage security alerts in Splunk and Microsoft Defender, escalating threats based on severity.
- Maintain technical documentation for systems, procedures, and recurring issues.

Tech Support **Nov 2018 – July 2019**
Prospect Air Services *Chicago, IL*

- Resolved an average of 30 support tickets per week for laptops, tablets, radios, and end-user applications.
- Supported approximately 30 users with device issues, access problems, mobile support, and equipment replacements.
- Tracked IT assest and assisted with refresh cycles, replacements, and lifetime documentation.
- Built a TrueNAS backup system for 4 company machines, improving recovery readiness.
- Secured mobile devices through updates, pass-code enforcement, and basic policy configuration.
- Created network and server rack diagrams to improve infrastructure documentation.
- Assisted with malware detection testing using SIEM tools and sandbox environments.

Projects

Homelab | *Docker, Proxmox, pfsense, Parrot Linux, Ubuntu Server, Windows Server, Wazuh* **|** *Project Link*

- Built and maintained a lab to test, increase skill, and maintain an enterprise-grade environment. The lab utilizes a Hypervisor, Pfsense, Wazuh, Ubuntu Server, Windows Server, Metasploitable machines, Parrot Attacker, and more.

Wildid | *CSS, Cursor, Docker, HTML, Javascript, HTML | Project Link*

- My team and I built a wildlife identification app using Cursor.ai and Together.ai for a project at DePaul University in our Software Projects course.

Passive Reconnaissance | *Google Dorking, SecurityTrails, Shodan* **|** *Project Link*

- During my Security Testing and Assessment Course at DePaul University, I conducted a passive reconnaissance assessment of a website of my choosing. Finding multiple vulnerabilities and points of failure.

Capture the Flag | *DIRB, HYDRA, Netcat, NMAP, Metasploit* **|** *Project Link*

- During my Security Testing and Assessment Course at DePaul University, I conducted a capture the flag assignment. Me and my partner utilized multiple exploits and past CVE's to gain and escalate access to ultimately own multiple systems.

Skills

Languages: Python, C, HTML/CSS, JavaScript, SQL, Bash, Powershell

Scanning: Nmap, Wireshark, Nessue Tenable, Splunk, Wazuh, Firewall Configuration

Exploitation: Metasploit, MITRE ATT&CK, Penetration Testing, Detection Engineering

Technologies: AWS, Linux, Docker, Git, Azure, Cloud Infrastructure, TCP/IP, DNS, Active Directory, Microsoft 365

Security: Incident Response, Forensic Analysis, Vulnerability Management, NIST, Security Controls