


John Pennie

Chicago, IL 60641

(773)-706-3651 ✉ jrpennie@proton.me  [linkedin.com/in/john-pennie](https://www.linkedin.com/in/john-pennie)  github.com/jrpennie  jrpennie.us

Education

DePaul University

Bachelors of Science in Cybersecurity
Minor in Computer Science

Aug 2022 – Nov 2025

Certifications

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

Experience

IT Operations Analyst

Ulta

April 2023 – Present

Chicago, IL

- Provide Tier 2 support for Windows workstations, login issues, application errors, and network connectivity problems in both store and office environments.
- Create and manage user accounts in Active Directory and Microsoft 365, including MFA setup and permissions.
- Install and update software on workstations to keep systems secure and running properly.
- Monitor backups and storage on file servers and assist with recovery testing when needed.
- Support endpoint security by verifying BitLocker encryption, antivirus protection, and vulnerability patching.
- Support VPN access and remote connectivity for off-site users.
- Monitor security alerts using SIEM and EDR tools (Splunk, Defender) and escalate potential threats based on severity.
- Maintain clean documentation for systems, procedures, and recurring issues.

Tech Support

Prospect Air Services

Jan 2021 – Feb 2023

Chicago, IL

- Handled daily support tickets for laptops, tablets, and radios. Solving both hardware and software issues.
- Tracked IT assets and assisted with equipment refresh cycles and system replacements.
- Built a centralized backup system using TrueNAS for company data storage and recovery.
- Secured mobile devices with updates, passcodes, and basic security policy enforcement.
- Created network and server rack diagrams for 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 Mangement, NIST, Security Controls