

# LEANDRO CORREIA DE FREITAS

Email: [lcfreitas.it@gmail.com](mailto:lcfreitas.it@gmail.com)

LinkedIn: <https://www.linkedin.com/in/lecfreitas/>

Mobile Number: +1 (201) 932-8573

Address: Cliffside Park, NJ 07010

Github: <https://github.com/lfs3c>

## PROFILE SUMMARY

---

Cybersecurity student with Harvard CS50's Certification and hands-on experience in SIEM (Splunk), malware analysis, log analysis, and system hardening across Linux and Windows environments, Server and Network security hardening. Experienced Linux user (Ubuntu, Debian Server, Kali, Mint). Multilingual (Portuguese, English, Spanish and Mandarin).

## CORE COMPETENCIES

---

**Security:** Hardening (Linux/Windows) | SIEM (Splunk) | Network Security | Firewalls | Malware Analysis | Risk Management | GRC

**Tools:** Wireshark | Nmap | Metasploit | Splunk | Git

**Systems:** Linux | Windows Server | VMware | VirtualBox | Docker

**Networking:** TCP/IP | DNS | DHCP | VPN | Network Segmentation

**Languages:** Python | Bash | PowerShell | SQL

## EDUCATION

---

**Associate Degree in Cybersecurity | Bergen Community College, NJ | Dec 2026**

**Relevant coursework:** Network Security, Ethical Hacking, Digital Forensics, Unix/Linux Network Administration – Current GPA 3.786

**Graduate Certificate in Project Management | Faculdade Impacta Tecnologia, Brazil | Completed 2015**

**Bachelor of Business Management | Universidade Paulista (UNIP), Brazil | Completed 2012**

## PROJECTS

---

- **Home Lab – Debian Server Deployment and Hardening (Documented on Github)**  
Deployed and hardened a headless Debian server with secure remote access, system hardening, and full documentation. Designed as a foundation for virtualization, Dockerized services, honeypots, and malware analysis.
- **Home Virtual Machines for Malware Analysis (Windows 10 & Kali Linux) — Integrated with Splunk SIEM**  
Built isolated Windows and Kali VMs for controlled malware execution and adversary behavior analysis. Integrated Splunk SIEM for centralized logging, correlation, and incident-response practice.
- **Open WebUI — Local LLM Deployment and Integration (Ubuntu Environment)**  
Installed and optimized Open WebUI with Ollama to run multiple local LLMs for offline AI workflows. Benchmarked and managed models with focus on performance, privacy, and efficient resource usage.
- **n8n Automation Server — Workflow Orchestration and System Integration**  
Deployed n8n on a Debian server using Docker for persistent, self-hosted automation workflows. Implemented API-driven automations for system tasks and personal productivity use cases.
- **Cowrie SSH Honeypot — Isolated VM-Based Attack Observation Lab**  
Implemented a Cowrie SSH honeypot in an isolated VM to safely capture real-world intrusion attempts. Collected attacker commands and artifacts to study threat behavior and deception techniques.
- **Raspberry Pi NAS with PhotoPrism — Self-Hosted Intelligent Storage (Documented on GitHub)**  
Designed and deployed a PhotoPrism-based NAS on Raspberry Pi 4 with Docker, Samba, and external HDD storage. Enabled automated photo indexing and metadata analysis with a portable, SD-safe, privacy-first architecture.
- **Raspberry Pi Blue Team Sensor — Centralized Logging & Lightweight Monitoring**  
Built a dedicated Raspberry Pi 3B sensor to centralize logs from the NAS using rsyslog and strict trust boundaries. Applied SSH hardening, Fail2Ban, firewall rules, and structured logging for baseline and incident analysis.

## LANGUAGES

---

Portuguese (Native) | English (Fluent) | Spanish (Conversational) | Mandarin (Basic)

## CERTIFICATIONS

---

- **Harvard University:** CS50's Introduction to Cybersecurity | January 2026 | **Skills:** Web security fundamentals (phishing, URL manipulation); HTTP/HTTPS, DNS, and TLS concepts; input validation and code injection awareness (XSS); network privacy and tracking mechanisms (cookies, fingerprinting); cybersecurity risk awareness and mitigation.
- **TryHackMe:** *Pre Security* | March 2025 | **Skills:** Networking Basics (TCP/IP, ports, services); Linux (commands, file structures, permissions); Windows (basic interface, PowerShell); Web (HTTP, HTML basics); Cybersecurity (core concepts, threats)
- **Foundations of Cybersecurity (Google)** | April 2024 | **Skills:** Core Cybersecurity concepts; security attacks and business impact; security ethics; common tools used by Cybersecurity analysts
- **Technical Support Fundamentals (Google)** | July 2023 | **Skills:** Information technology; operating systems; technical communication; computer networking; software installation; customer and technical support; end-user training
- **Saint Peter's University:** Participant in the *Cybersecurity Competition "Capture the Flag for Novices 2025"* | October 2025 | **Skills Used:** CTF, Wireshark, Cryptography, OSINT

## MOST RECENT PROFESSIONAL EXPERIENCE

---

**CNC Machinist** | Service Metal Fabricating, Rockaway, NJ August 2025 – present | 40 hrs/week

- Operating CNC (Computer Numerical Control) machinery, keeping production at high level of excellence in measurements.
- **Optimizing and maintaining a Excell spreadsheet of all the tools used in the machine shop**
- Deburring pieces and cleaning sharp edges, finishing look.
- Interpreted complex technical blueprints and schematics, ensuring precise calibration of tools and materials for high-tolerance manufacturing.
- Calculating and checking the piece measurements, including true-position measurements.

**CNC Machinist & Programmer** | Barnett Machine Tool Corp., Elizabeth, NJ April 2021 – July 2025 | 40 hrs/week

- Programmed and optimized CNC machinery using G-code, improving production accuracy to within 0.003 inches while reducing cycle times by 15%.
- Interpreted complex technical blueprints and schematics, ensuring precise calibration of tools and materials for high-tolerance manufacturing.

**IT Support Technician** | Our Lady of Grace Catholic Church, Fairview, NJ Aug 2023 – Mar 2024 | 20 hrs/week

- Resolved 20+ hardware and software issues weekly through systematic troubleshooting, reducing system downtime by 40% and improving staff productivity.
- Implemented automated backup solutions and database management protocols, decreasing data loss incidents by 25% while ensuring compliance with security best practices.
- Configured and maintained network printers, workstations, and peripheral devices, streamlining office operations and enhancing user experience.
- Conducted Cybersecurity awareness training for 15+ staff members, reducing phishing susceptibility and improving overall IT hygiene.