# Paris Smith

Aspiring Cybersecurity Analyst
B.S. Cybersecurity | Sec+, CySA+ | Aspiring M.S. Cybersecurity; Net+, Linux+ & eJPT

Tampa, FL
**7273140234**
cvepfd@gmail.com
https://www.linkedin.com/in/smithparis-cvepfd/

## RELEVANT EXPERIENCE

### **Grand Canyon Education,** Phoenix, AZ— *ITS/Help Desk Technician*

October 2020 - January 2024

- Resolved 95% of technical issues independently through diagnostic techniques, including in-person and remote support via RDP, SCCM, Teams, Zoom, and phone
- Triaged and completed service requests in ServiceDesk; documented steps taken and suggested future troubleshooting actions
- Troubleshot/Researched solutions via online/internal resources for troubleshooting issues related to MS Office365, Cisco VPN and Unity, Azure, and both Windows/Mac environments to provide timely resolutions and ensure user satisfaction.
- Led onboarding and training sessions, fostering a knowledgeable support team equipped to deliver consistent and high-quality service
- Configured user accounts, devices, and printers in Active Directory to streamline access and provisioning
- Provided Audio-Visual support for classrooms, company events, and meetings.
- Collaborated with teams (Telecom, Networking, ITSec, CyberOps, CampusVue) to escalate and resolve complex technical issues

## PROJECTS/SKILLS

- Security Onion SOC/SIEM Lab (Proxmox + WUI@Ubuntu Desktop):Performed alert triage, case escalation, and event correlation. Practiced detection engineering through query tuning and rule modification.
- eJPT Lab Series – Network Enumeration & File Transfer: Enumerated 20+ live endpoints using active and passive scanning techniques on a controlled subnet. Transferred files securely via SSH/SCP and validated network connectivity. Documented findings, raw tool outputs, and analysis aligned with recognized penetration testing methodologies.
- Documented findings, tool output, and analysis reflections for each phase
- PiHole DNS Sinkhole + Upbound Recursive DNS: Configured recursive DNS infrastructure; monitored/blocklisted malicious domains and analyzed DNS logs for anomalies. Monitored DNS traffic, blocked ad domains, and validated traffic redirection and sinkholing.
- Wireshark Malware Traffic Analysis (ParrotOS): Analyzed PCAP files using Wireshark; extracted IOCs and correlated malicious activity timelines.
- Windows Server Domain Lab (VMware): Configured a Windows Server DC and domain-joined clients in VMware; applied and tested group policies and user account controls.
- Vulnerability Scanning with Nessus/OpenVAS: Conducted scans against lab systems to identify CVEs and misconfigurations. Compared scan output, validated findings, and documented remediation strategies.
- TryHackMe - PreSecurity Path (100%)
- Rangeforce - Incident Response Theme (75%)

## EDUCATION

### **Grand Canyon University,** Phoenix, AZ— *B.S Cybersecurity*

August 2019 - Present | Completed 124/120 credits, CAPSTONE in progress

- Cybersecurity Committee Member | NCAA D1 Track Scholarship Athlete | Faculty Academic Scholarship
    - 2021-2022 NCAA Regional Outdoor Qualifier | WAC Indoor & Outdoor Qualifier

### **Lakewood High School - Center for Advanced Technologies,** Saint Petersburg, Florida

August 2015 - May 2019

- FHSAA Track and Field 3x State Qualifier
- Guitar Ensemble | Future Business Leaders of America State Participant | Spanish Honors Society

## PROFESSIONAL SUMMARY

Security+ and CySA+ certified IT professional with 3+ years of hands-on experience in help desk, system administration, and user support. Skilled in threat detection, log analysis, and triaging alerts using tools like Security Onion, Wireshark, and Nessus in lab environments. Actively developing skills in threat hunting, detection engineering, and incident response. Known for taking initiative, documenting thoroughly, and supporting user satisfaction across technical teams. Seeking an entry-level cybersecurity or SOC analyst role to continue contributing to secure IT operations while growing in a fast-paced environment.

## CERTIFICATIONS

**Security+ (601) - Earned July ‘24**

**CySA+ (V3) - Earned June ‘25**

Net+ (V9) - Expected September ‘25

Linux+ - Expected October ‘25

eJPT - In Progress, Q4 ‘25

## TECHNICAL SKILLS

**SIEM & Analysis:** Security Onion, Nessus, OpenVAS, Nmap, Wireshark, Splunk Enterprise (via Rangeforce), Metasploit

**OS:** Windows/ Linux (Ubuntu, Kali, Parrot)/ Mac

**Scripting:** Bash, Powershell, Python, Regular Expressions (log filtering, grouping, matching)

**Systems Admin:** Active Directory, Microsoft 365 / Office 365, Azure, ServiceDesk, SCCM

**Networking & Comms:** nmap, Cisco Packet Tracer, Cisco Unity, Jabber, Cisco AnyConnect

## LANGUAGES

Spanish - Proficient

Bash / Python / Powershell / C - Intermediate

Assembly / PineScript / HTML/CSS / SQL - Familiar