JAMES CHAPMAN

Ellenboro NC
(828) 289-3320
6sec6cyl@gmail.com
https://www.linkedin.com/in/james-chapman-a4376982/
https://james-r-chapman.github.io/

PROFESSIONAL SUMMARY

Aspiring IT Professional and cybersecurity analyst with hands-on experience in network security, system administration, and technical support. Combines practical IT operations expertise with advanced security training. Ranked top 1% on TryHackMe with 400+ days of continuous security skill development. Proven ability to automate workflows and solve complex technical challenges.

SKILLS

Network Security
Ethical Hacking & Red Team Operations
Network Security
Digital Forensics & Malware Analysis
Vulnerability Assessment & Penetration Testing
Incident Response & Threat Hunting
Linux/Unix (Ubuntu, Kali, CentOS)
Wireshark
Metasploit
Cryptography
Cloud Computing: AWS, Microsoft Azure
Security Information and Event Management (SIEM) Splunk, Elastic Stack (ELK), Wazuh
Digital Forensics
Malware Analysis
Python (automation, data processing, scripting)
Forensics: Volatility, Autopsy, FTK Imager
IDS/IPS: Snort, Zeek, Suricata
Network Analysis: Wireshark, tcpdump, NetworkMiner, Nmap, Nessus
Bash/Shell scripting
PowerShell
Windows Server & Workstation

EXPERIENCE

PARTS MANAGER AND IT HELPDESK January 2023 - Present
Courage Kia, Gastonia NC

- Controlled physical security infrastructure including IP cameras and NVR systems, maintaining 99% up time throughout 2024 and contributing digital forensic evidence to law enforcement authorities.
- Performed hardware diagnostics and software troubleshooting on Windows workstations and tablets, ensuring network connectivity and system availability for 20+ workstations.
- Documented processes and procedures for knowledge base, team reference, and 6 specific job roles.
- Delivered technical support to 15+ employees, resolving hardware and software issues to minimize downtime.

FM TECHNICAL SUPPORT MANAGER September 2020 - April 2025
Total Dealer Solutions, Fort Lauderdale FL

- Developed Python automation scripts to streamline variance report generation, reducing manual processing time and improving data accuracy.
- Supervised 10+ field managers with 15-40 inventories every weekend, asset control, and inventory management across multiple locations.
- Supplied remote desktop support to streamline inventory tracking and asset management processes resulting in 99% less errors.
- Managed compliance with company policies and procedures through regular audits and assure process oversight for over 300+ dealerships.

EDUCATION

Bachelor of Science in Cybersecurity (B.S.) October 2025

Full Sail University, Winter Park, FL

Associate of Science in Information Technologies October 2024
Full Sail University, Winter Park, FL

CERTIFICATIONS & ACHIEVEMENTS

- Google Cybersecurity Certification.
- Microsoft Cybersecurity Analyst Certification.
- CompTIA Security+ (In Progress).
- TryHackMe - 375+ rooms and challenges with a 400+ day streak, ranking in top 1% of users on platform. TryHackMe SAL1 (In Progress).

PROJECT LIST

Class Labs/TryHackMe August 2023 - Present

- Performed vulnerability assessments using Nmap and Nessus on networks with 80+ devices, scanning 200+ services and identifying 25+ security gaps ranging from critical to low severity.
- Discovered and documented 30+ critical vulnerabilities using Nmap and Nessus, proposing 2-4 remediation strategies per finding with comparative analysis of implementation complexity, cost, and risk reduction.

TryHackMe September 2024 - Present

- Completed comprehensive SOC Level 1 learning path on TryHackMe.
- Developed proficiency in SIEM platforms including Splunk, Elastic Stack (ELK), and Wazuh for log aggregation, analysis, and threat detection.
- Analyzed network traffic using Wireshark, tcpdump, and NetworkMiner across 50+ scenarios, processing 50GB+ of packet captures to identify malicious activity, C2 communications, and data exfiltration attempts.
- Investigated and resolved 50+ simulated cyber incidents including ransomware attacks, credential compromise, and lateral movement, analyzing over 50GB of log data, and identifying 100+ indicators of compromise (IOCs).

Home Lab Environment July 2022 - Present

- Built and maintain virtualized cybersecurity lab using VirtualBox/VMware/Proxmox with 10+ VMs for hands-on security testing.
- Configured multiple vulnerable machines (including 2 machines containing DVWA and Metasploitable) for ethical hacking practice and exploit development.
- Configured pfSense firewall with 3 VLANs (trusted, IoT, security testing) and 20+ rules enforcing network isolation and zero-trust policies between zones.
- Deployed Pi-hole DNS filtering blocking 100,000+ ad/malware domains and implemented Grafana + Prometheus on Ubuntu server for monitoring network traffic, system metrics, and firewall logs across home lab infrastructure.

LEADERSHIP

- Lead cross-functional collaboration efforts to solve technical incidents, coordinate resources, and sustained timely incident response.
- Communicate complex technical issues to non-technical stakeholders, leading customer expectations and citing solutions.
- Train and mentor team members on IT security best practices, troubleshooting methodologies, and compliance requirements.