Daniel Davidson

Available upon request | linkedin.com/in/danieldav/ | pyrosec.github.io

SUMMARY

Information technology and security professional with experience in system/network administration, penetration testing, network security, endpoint security, vulnerability analysis, OSINT, network/security operations, and strategic automation.

Highly adaptable professional who embraces teamwork, but also enjoys working independently. Results-oriented, dependable person, who is good under pressure and can think on his feet. Carries a wealth of on-the-job experience and continual learning via Cisco Netacad, TryHackMe, Blue Team Labs, Vulnhub, LetsDefend, and daily practice in a home lab.

SKILLS & EXPERTISE

Core Skills
- *Value focused*
- *Team collaboration*
- *Strong communication*
- *Strong ethics & integrity*
- *Self-motivated & innovative*
- *Critical thinking & problem-solving*

Systems & Networks
- *Active Directory*
- *Networking Principles (TCP/IP - OSI)*
- *Windows Server (DNS/DHCP - SCCM)*
- *Linux/Unix operating systems*
- *Switch & Router Administration*
- *VMware Administration*

Security
- *General Security Principles*
- *Scripting (Python - Powershell)*
- *Security Breach Prevention*
- *Information Security & Compliance*
- *Endpoint Protection & Monitoring*
- *Firewall/Content Filter Management*

PROFESSIONAL EXPERIENCE

Dothan City Schools

Systems / Network Administrator — 2019 – Present | Dothan, AL

Objective: Spearheaded defense procedures to increase security posture.
- Served as the security systems lead and final escalation point for internal IT helpdesk, responding directly to users and other team members needing assistance. Continued all Jr. Sysadmin responsibilities.
- Configured, maintained, and repaired routers, switches, firewalls, wireless access points and controllers, servers, and remote access protocols. Network Technologies - LAN/WAN, TCP/IP, SNMP, VPN, SFTP, VLAN, VoIP, DNS, DHCP, RDP, SSH.
- Implemented secure and best practice design principles in system/network infrastructure across 21 MDFs and 150 IDFs comprising of about 200 switches.
- Monitored and triaged security alerts as well as performed containment and root cause analysis.
- Provisioned identification and authentication for over 10,000 end users, devices, and services.
- Installed, configured, and maintained 97 UPS battery backups to aid disaster recovery plans by providing consistent availability for core infrastructure across 21 remote sites.
- Collaborated with network engineers, field technicians, equipment vendors, and telecom carriers to effectively troubleshoot and resolve various types of network issues and outages.

Jr. Systems Administrator — 2017 – 2019 | Dothan, AL

Objective: Proactively ensure 90% uptime of network availability and consolidate critical infrastructure.
- Plan, design, install & troubleshoot network communication, IP cameras, fiber networks.
- Contributed to the development of security policy and procedure requirements.
- Consolidated over 50 physical servers into 40 virtual hosts managed in VMware ESXi & vCenter with high availability.
- Deployed routine patches for security vulnerabilities, drivers, and functionality updates on Windows/Linux servers as well as over 9,000 end-points company-wide using WSUS, SCCM, and Powershell.
- Released Windows workstation images with configurations monthly to be deployed company-wide.

Information Technology Specialist — 2016 – 2017 | Dothan, AL

Objective: Aimed to provide better visibility of resources and automate workflows.
- Increased ticket resolution by 50% by scripting in-house tools to automate software deployment and device provisioning.
- Improved information security awareness and education for password safety, phishing, and social engineering.
- Monitored and resolved network infrastructure alerts to provide consistent availability of resources.
- Ensured proper installation of structured cabling, operating systems, and software.
- Resolved computer hardware, software, printing, email, and operating system issues.

Quality Data Systems, Inc., *Field Service Technician* — 2015 – 2016 | Charlotte, NC

Service Relationship Initiative: Fostered feedback to better co-create value with service consumers and providers.
- Repaired malfunctioning system components.
- Managed teller automation systems and ATMs for over 15 locations in a 200-mile radius.
- Adhered to contractual, legal, industry standards, and regulatory requirements.

EDUCATION

B.S. Cybersecurity and Information Assurance, *Western Governors University* — 2021 – Present | Remote

A.A.S. Computer Information Science, *Wallace Community College* — 2012 – 2015 | Dothan, AL

CERTIFICATIONS & LICENSES

Blue Team Junior Analyst
Security Blue Team

ITIL 4 Foundation
Axelos

CCNA
Cisco

Splunk 7.x Fundamentals
Splunk

PROJECTS

Home lab
- Currently running Proxmox VE with appliances including Splunk, and an isolated 10-VM training range designed to practice red and blue team efforts as well as to strengthen system and network engineering skills.

Personal Blog, *pyrosec.github.io*
- A place where I actively post my security findings and various CTF write-ups.
- Built using Jekyll, a static site generator.
- Developed on GitHub and hosted for free ($0) using GitHub Pages.

Network Technologies and Network Security
- Used command-line tools (ping, fping, nmap, ipconfig, ifconfig, netstat, tracert, arp) to troubleshoot and analyze system connectivity issues and to identify the security posture of a network.
- Learned about, implemented, and configured protocols (SRTP, FTP, SFTP, FTPS, SSH, TLS, VPN, SMTP, POP3, IMAP4, HTTP(S), Kerberos, LDAP, NTP, DHCP, RDP) to support different use cases.
- Studied, Installed, and configured switches, routers, and firewalls to create a secure and efficient network.
- Studied and implemented wireless cryptographic protocols (WPA, WPA2 in PSK and Enterprise modes, TKIP, CCMP) to discover vulnerabilities, which led to understanding how to design secure wireless networks to thwart wireless attacks.

Blue Team Junior Analyst Training
- The Blue Team Junior Analyst training path enables cybersecurity professionals and students to gain live-environment experience with the foundational concepts and practices of a wide variety of cyber defensive roles.
- Leveraged the OSINT Framework to either increase the attack surface from a red team perspective or reduce the attack surface from a blue team perspective.
- Performed network traffic analysis to uncover suspicious or malicious activities.
- Utilized Digital Forensic methodologies to aid incident response with details revealing how a compromise occurred.
- Identified security flaws and vulnerabilities through Vulnerability Management and created a report so they can be fixed thus reducing the impact or risk of cyber-attacks.
- Gathered a large amount of threat intelligence from the Darkweb ranging from malware all the way to uncovering planning of cyber-attacks on private forums.
- Learned about Threat Hunting and how to search of any signs of advanced threats using indicators of compromise (IOCs).

Python VirusTotal API Project
- Utilized Python to upload files to VirusTotal for analysis.

Python Keylogger
- Created a Python script to record any keystrokes to a file.

Python ARP Scanner
- Leveraged ARP networking protocol to provide an alternative method of identifying live hosts.
- Unlike traditional network scanners that depend upon ICMP (Internet Control Message Protocol) to identify live hosts on a network this Python script instead utilizes ARP. Since ICMP packets can be monitored or systems can be configured to not respond at all to ICMP requests ARP can sometimes bypass these measures.

Steganography and Data Hiding
- Concealed and extracted payloads from images with LSB steganography and steghide.
- Employed cyber forensic software to view anomalies between virgin and modified images.
- Applied forensic hashing concepts to create a list of known file filters (KFFs) to identify and isolate suspicious files.

ADDITIONAL EXPERIENCE

Achievements:
Top 2% Worldwide on TryHackMe CTFs
Top 10 in Cardiff University Investigator OSINT CTF

Social Impact:
Helped build and co-manage a IT & cybersecurity discord community of 200+ members centered around helping beginners break into the industry as well as providing a safe space for feedback and questions. We host regular events for members to engage in CTFs or exchange ideas for projects.

Personal Development:
Cisco Netacad, Packet Tracer, TryHackMe, Hack the Box, LetsDefend, Blue Team Labs Online, Rangeforce, INE, TCM Academy, Coursera, freeCodeCamp, Udemy, and Youtube.

Current Goals:
CompTIA A+ | CompTIA Network+ | CompTIA Security+
CompTIA Project+ | CompTIA PenTest+ | CompTIA Cybersecurity Analyst (CySA+)
Certified Cloud Security Professional (CCSP) | Systems Security Certified Practitioner (SSCP)