Michael Jackson

Network Security Engineer | Cybersecurity Analyst
Security Clearance | Security+ | CySA + | eJPT (In Progress)
GitHub: github.com/takecntrl | **HTB**: takecntrl | **THM**: takecntrl | **LinkedIn**: linkedin.com/in/takecntrl

Objective:

Cybersecurity analyst with over 3 years of experience defending high-security networks, supporting red team operations, and responding to live threats in DoD and enterprise environments. Adept at correlating SIEM data, performing forensic triage, and identifying attack vectors before damage escalates. Certified in CySA+ and Security+, currently pursuing the eJPT to deepen offensive fluency and sharpen incident response readiness.

Core Skills:

- Proactive threat detection and incident response across complex, segmented DoD and enterprise networks
- Endpoint telemetry and log triage to identify attacker behaviors and trace root cause
- Detection strategy development aligned with MITRE ATT&CK and real-world TTPs
- Red team engagement support through privilege escalation analysis and exploit validation
- Documentation and communication tailored for investigative clarity and audit readiness
- Automation of scripted automation for recon, detection tuning, and event correlation using Python and Bash

Tools & Technologies:

- SIEM & Log Analysis: Splunk, Kibana, NetFlow
- Network Forensics: Wireshark, TCPDump
- EDR/XDR Platforms: Familiarity with CrowdStrike, SentinelOne, Microsoft Defender
- Pentest Tools: Kali Linux, Metasploit, Nmap
- Scripting & Automation: Python, Bash
- Firewalls & NGFWs: Cisco ASA, Firepower (including 2110 series)
- VPN & Access Control: ASA SSL VPN (WebVPN / AnyConnect)
- Vulnerability Tools: Familiar with interpreting output from tools like Nessus, Qualys, and OpenVAS
- Certificates & Crypto: PKI validation, CA trust chain debugging, TLS troubleshooting

Professional Experience:

Network Engineer Jan 2025 – Present
DISA/Leidos | Contract | On-site

- Supported secure DoD operations by monitoring network integrity and identifying anomalies through Kibana dashboards and NetFlow data
- Collaborated with cybersecurity teams to investigate suspicious patterns, escalate potential incidents, and contribute to containment recommendations
- Managed and audited ACLs across classified network environments to ensure segmentation, compliance, and security policy enforcement
- Documented configuration changes, trends, and detected anomalies to support audit readiness and incident investigations
- Participated in cross-functional troubleshooting and supported mission-critical communication paths in high-security operational zones
- Operated under DoD Secret Clearance, ensuring all actions met federal cybersecurity and handling protocols

Help Desk Specialist Feb 2024 – Jan 2025
BuddoBot | Contract | On-site

- Recovered and upgraded unstable RHEL 8 systems to RHEL 9 when legacy issues blocked progress, proactively stepping up to lead the effort when no one else could
- Created internal documentation and knowledge base articles to support smoother contract handoffs and reduce onboarding gaps
- Maintained IT service continuity and system uptime during high team turnover and unclear ownership periods, often serving as the fallback point of contact

Network Security Engineer / Network Engineer III — May 2022 – Jan 2024
Secure Data Technologies | FTE | Remote

- Diagnosed and remediated TLS trust failures between Cisco ISR4431 gateways and CUCM; analyzed PKI chains, validated trustpoints via CLI and resolved cryptographic registration errors
- Investigated certificate store discrepancies and root CA mismatches causing device trust issues; isolated faulted endpoint configurations by comparing operational vs. broken deployments
- Deployed and monitored Sysmon for advanced endpoint visibility; analyzed process creation and network connection logs to detect potential threats
- Resolved GPO-based application deployment failures by identifying policy misconfigurations affecting security agent rollout
- Performed simulated internal red team assessments using Gobuster, Nmap, Hydra, and Burp Suite; uncovered vulnerable endpoints, brute-forced weak credentials, and mapped exposed directories
- Used Impacket and Metasploit to exploit SQL services and elevate access across internal test environments
- Captured and analyzed network traffic with Wireshark to identify plaintext credentials, unencrypted sessions, and insecure authentication flows
- Audited ASA SSL VPN configurations (WebVPN/AnyConnect), troubleshooting domain-specific ACLs and validating access controls via CLI filters

Projects & Labs:

- Completed over 50 labs and machines on Hack the Box and TryHackMe, focusing on privilege escalation, enumeration, vulnerability chaining, and lateral movement
- Built a personal cybersecurity lab using VMware Workstation Pro with Kali Linux, RHEL jumpboxes, and isolated network segments; simulated attacks and defense scenarios across multiple OS environments
- Conducted Active Directory exploitation in lab settings using Mimikatz, Hydra, and Impacket to extract credentials and simulate red team lateral movement
- Exploited real-world CVEs (e.g., Cacti CVE-2022-46169), performed post-exploitation, and achieved persistence via SETUID binary enumeration
- Deployed Sysmon and used Wireshark and Netcat for live endpoint and network visibility across simulated attack environments
- Created an automated log parser and report generator in Python, that extracts system metadata and organizes client diagnostics from disorganized logs
- Performed Docker exploitation, custom reverse shell delivery, and privilege escalation via environment variable poisoning and sudo misconfigurations
- Participated in bug bounty-style simulations using OWASP Juice Shop and DVWA, exploiting SQL injections, XSS, and command injection
- Completed password hash cracking labs using Hashcat and John the Ripper on Cisco Nexus configuration files
- Reverse engineered and de-obfuscated JavaScript to expose logic, function flow, and authentication request payloads in a simulated bug bounty setting

Education:

Associate of Applied Science – Information Technology & Cybersecurity — Aug 2020 – May 2022
Ranken Technical College | St. Louis, MO

- Magna Cum Laude
- President’s List
- Tutored students in networking and cybersecurity fundamentals