Michael Jackson

Security Engineer | Threat & Vulnerability | Offensive Security
Secret Security Clearance
Email: Mjackson3089@gmail.com | Ph: 618-491-4171

Professional Summary:

Offensive security engineer with hands-on experience executing full attack chains, developing custom exploits, and building red-team tooling used daily in freelance engagements. Secret cleared with DoD background. Creator of Forge — automated exploit harvesting and search system indexing 400+ CVEs. Currently enrolled in SANS Bachelor's (9 GIAC track). Strong in MITRE ATT&CK emulation, C2 frameworks (Mythic/Havoc/Sliver), and detection engineering.

Professional Experience:

Freelance Offensive Security & Tooling Development **Oct 2015 – Present**
The Cyber Protocol (Remote)

- Creator and daily operator of Forge (automated exploit arsenal indexing 400+ CVEs)
- Indexed and tagged 400+ exploit PoCs using custom automation (Forge)
- Executed full attack chains across web, network, and cloud environments
- Developed custom exploits and proof-of-concepts for complex vulnerabilities
- Built and operated C2 engagements using Mythic, Havoc, and Sliver
- Delivered 15+ professional pentest reports delivered to clients
- Reduced exploit research time from hours to <5 minutes per CVE

Network Engineer III (Threat Detection Engineer) **May 2022 – Jan 2024**
Secure Data Technologies | O'Fallon, IL

- Assisted with internal pentests for clients by conducting structured recon, vulnerability analysis, exploit testing, and privesc validation.
- Conducted exploit proof-of-concept testing and verified vulnerability impact during client-facing assessments.
- Built Python/PowerShell automation to help identify exploitable misconfigurations in AD, cloud assets, and network appliances.
- Carried out exploit verification during incident simulations to validate the impact and likelihood of discovered vulnerabilities.
- Worked closely with SOC analysts to validate root cause analysis by recreating attacker behavior.
- Tuned detections based on real red-team behavior rather than textbook indicators.
- Created custom detection rules (Sigma/ELK/Snort) based on observed techniques in internal engagements.
- Reduced false positives and improved SIEM fidelity through adversary-informed rule design.

Help Desk Specialist (Security Analyst) **Feb 2024 – Jan 2025**
BuddoBot | Scott Air Force Base, IL

- Administered secure RHEL-based environments supporting internal ML and automation workflows.
- Resolved access control violations and remediated GitOps/CI/CD pipeline security risks.
- Collaborated with Tier II/III teams on log reviews and internal risk assessments.
- Restored and hardened failed RHEL deployments under strict operational timelines.

Network Controller (Cybersecurity Support) **Jan 2025 – May 2025**
DISA/Leidos | Scott Air Force Base, IL

- Supported cybersecurity operations across NIPR/SIPR environments in alignment with STIG/RMF requirements.
- Performed patch audits, identified configuration deviations, and coordinated remediation with sysadmin teams.
- Investigated anomalous traffic and escalated verified threats within classified communication networks.
- Helped maintain readiness of mission-critical systems powering global DoD operations.

Education & Training:

Associate of Applied Science – Information Technology & Cybersecurity
Ranken Technical College | St. Louis, MO

- Magna Cum Laude
- President's List
- Enrolled at SANS Bachelor's in Cybersecurity

Certifications

Current

- Cisco CCNA
- Cisco CyberOps Associate
- CompTIA Security+
- CompTIA CySA+

In Progress/Planned

- SANS Bachelor's Track (9 GIAC certifications)
- PNPT
- OSCP
- Pentest+

Core Security Domains:

Threat & Vulnerability Analysis

- Attack surface mapping
- Exploit chain reconstruction
- ATT&CK mapping
- Payload/delivery analysis
- Vulnerability triage & prioritization

Detection Engineering

- SIEM tuning (Splunk, ELK, Graylog)
- Snort/Sigma/Elastic rule development
- Log pipeline optimization
- Beacon pattern detection
- IOC enrichment & timeline reporting

Adversary Simulation

- Red team lab design
- TTP emulation & scenario builds
- Lateral movement & pivot testing
- Active Directory auditing (BloodHound)
- Custom recon/automation scripts

Offensive

- Nmap, Burp Suite, Hydra, Gobuster, SQLmap
- Metasploit Framework, Sliver, Mythic, Havoc
- BloodHound, Evil-WinRM, Impacket

Threat Intelligence

- Shodan, Censys, FOFA
- VirusTotal, URLScan.io, Any.run
- OTX, AbuseIPDB

Defensive/Detection

- Splunk, ELK, Graylog
- CrowdStrike Falcon, SentinelOne
- Velociraptor, Sysmon