**Jay S. McGuerty / GWAPT, CISSP**

www.linkedin.com/in/jay-mcguerty-48a6976 | 858.663.5209 | mcguerty@att.net | DoD TS/SCI FS Poly

**C# Developer/Cyber Security Engineer**

Skilled at devising and writing cyber warfare and defensive tools in Java, Python and PowerShell, software development, software security, static/dynamic code analysis, configuring routers, switches, firewalls, web and network perimeter penetration testing.

**Authored Software and Books**

* End point self contained SIEM focused on anomalous memory and privilege use
* “njecta” automated SQL/NoSQL/Cmd Injection, field interrogation (Python)
* “pwdFactory”, generates passwords using predictive linguistics, personal profile (Java)
* “reaper”, 250+ signatures for filtering raw NMAP output (BASH)
* “Network Field Survival Guide, 10,000 copies sold” (http://www.thewayofthepacket.com)

**IT/Cyber Security Work Summary Highlights**

• Network/Web Application Penetration Testing, Vulnerability Assessments,

• Selected and installed first VoIP system used by the President of the United States

• Interim Network Security Architect for San Diego Airport TW2 expansion

• Provided Pen Test and Cisco training to customers and co-workers

**Certifications/Skills**

(ISC)2 Certified Information Systems Security Professional (CISSP #98465 11/31/2023)

GIAC Certified Web Application Penetration Tester (GWAPT #3257 09/30/2023)

Expired Certs:

GIAC Exploit Research Advanced Penetration Tester (GXPN 414 expired), Certified Forensic Examiner (GCFE 3123 expired), GIAC Certified Penetration Tester (GPEN 6744 expired), GIAC Certified Incident Handler (GCIH #18408 expired), Cisco CCSP/CCNP (expired); Microsoft MCSE (expired)

Programming Languages: Java, C#, Python, PowerShell, BASH, Javascript

SDLC Eco Systems: Eclipse, Visual Studio, MS Team Foundation, JBoss, Git

Security Frameworks: Splunk, Metasploit, Nessus, KALI, HP Fortify, BURP

Forensic Tools: FTK, Encase, OllyDbg, Immunity Debug, IDA, GDB

Routing Platforms: Cisco, Juniper

Firewalls: Cisco, Palo Alto, Juniper

UNIX: Linux (RHEL, Mint) Open/FreeBSD

Cloud Services vSphere, vCenter, ESXI

**Education**

B.S. Aeronautics, Aircraft Maintenance Engineering, Parks College/St. Louis University

**Work History**

**Leidos C2 Cyber Security/Cyber Resiliency– Cyber Security Engineer Mar 2018 - Present**

* Designed and wrote cyber tools for DoD agency to test security and authentication bypass
* Designed and wrote an End Point Forensic SIEM for the Air Force Joint Missino Planning System (JMPS) using precedent/antecedent behaviors
* Scanned and pen tested VPN’s using MITM techniques, generating fake certs to test security
* Splunk dashboard studio, event genome survey, checkmk syslog integration, architecture, malicious behavior dashboards

**Leidos Security Risk Management Practice - Principal Security Engineer Jan 2010 – Mar 2018**

* Penetration testing for DoD agency performing black/white box penetration testing (remote and onsite) of IPv4/v6 network infrastructure and web applications (XML, SQL, SOAP, REST, Local/Remote File inclusion, command injection, session ID/ referrer and misc. parameter tampering, OWASP Top 10), vulnerability assessments, credentialed compliance scans
* Information assurance through entire life cycle of hardware, firmware and software including supply chain malware detection and mitigation beginning at chip foundry, transportation, software life cycle
* 37 commercial and DoD penetration engagements, remote, on site, writing, presenting and defending final report
* Cyber Warfare planning, USC Title 10 (Armed Forces/Military Law), USC Title 50 (War & National Defense – Chain of command), USC Title 18 (Crimes/Criminal – Cyber Security Law), International Treaties, defining Rules of Engagement Doctrine for computer network attack (CNA) and exploitation (CNE), preparation, OSINT, characterizing nation state chain of command
* Interim Network Security Architect for the San Diego Airport billion dollar TW2 expansion project.
* Air Force TSAT (Transformational Satellite Communications System) Mission Operations System IA team; developing architecture and configuration to provide Cyber Attack Resiliency, testing product and architecture mitigation solutions for deficiencies in Control, Mgt and Forwarding Plane protocols

**SAIC NGIN PMO – Solution Architect Aug 2000 - Jan 2010**

* Assigned by the White House Communications Agency J5 Director to serve as the lead engineer in the planning and implementation of the first VoIP system used by the President of the United States
* Proposition “M” network modernization San Diego Unified School District. Responsible for surveying and proposed recommendations for fiber/CAT5e plant validation, rack mounting, clearances, power, structural, cooling, configuring switches/ router’s/conduct final acceptance testing.
* Lead engineer point to multi point “last mile” data solution, analysis of FDD/TDD antenna duplexing solutions, selection of modems, radios & antennas for P2MP & P2P backbone