JaJuan L. Grant

p: (512).997.5613
w: jajuang.co & jajuang.info
e: jg@jajuang.info

SUMMARY

Accomplished Cybersecurity Leader with a track record of spearheading innovative security solutions and guiding teams to success. Known for expertly navigating complex security landscapes, implementing cutting-edge strategies, and fostering a culture of excellence. Adept at translating technical complexities into business-oriented solutions, ensuring the utmost protection of critical assets. Committed to staying ahead of evolving cyber threats and leveraging a comprehensive skill set to deliver robust defense strategies and drive organizational resilience

EDUCATION

Western Governors University, Millcreek, UT — Graduated - May 2020
MS Cyber Security and Information Assurance

University of Maryland Global College, Adelphi, MD — Graduated - December 2019
BS Cyber Security and Networking

CERTIFICATES

CISSP, CISM, CEH, CNDA, CASP+, SEC+, NET+

COMPUTER SKILLS

Languages & Software: Red-teaming, Penetration Testing, Bash Scripting, C, Go, Nim, PowerShell, Python, Docker, AWS, NMAP, Nessus, Metasploit, C2 Frameworks (Sliver), BurpSuite, eMASS, DIACAP, Malware Development Academy (MalDev).
Operating Systems: Windows Active Directory, Unix* (Mac OSX), Linux* (Red Hat, Debian, Ubuntu, Gentoo, Arch), BSD* (OpenBSD, FreeBSD).

BLOGS

- ”Port Security and Why It's Important (I/II).” — July 05, 2022
  https://cowbell.insure/blog/port-security-1/
- ”Best practices for securing used and unused ports (II/II).” — July 05, 2022
  https://cowbell.insure/blog/port-security-2/
- ”Secure your cookie jar from this MFA loophole.” — November 30, 2022
  https://cowbell.insure/blog/secure-your-cookie-jar/

EXPERIENCE

Senior Offensive Security Consultant — October 2023 -
Netrix Global, Chicago, IL — 40 hrs/week

- Simulated APTs through malware development to evade AV/EDR solutions in red team exercises, updating organizations on sophisticated cyber attacks.
- Implemented targeted social engineering campaigns, gauging employee susceptibility to phishing attacks and delivering actionable reports.
- Executed thorough external penetration tests, pinpointing and exploiting vulnerabilities to strengthen client networks and systems.
- Performed Ransomware Assessments to to evaluate organization's susceptibility to ransomware attacks.
- Leveraged C2 frameworks to execute commands and maintain persistence in clients' networks.

Team Lead Penetration Tester — October 2022 - October 2023
Cowbell Cyber, Pleasonton, CA — 40+ hrs/week

- Pioneered the Micro Penetration service and introduced it to the Cyber Insurance Market.
- Led a team of 4 penetration testers in performing external penetration testing operations on organizations at $250M -$1B in revenue.

- Assessed the external security of applications, servers, and edge network devices to identify vulnerabilities and other potential attack vectors.
- Performed network scans, using vulnerability assessment tools to identify vulnerabilities.
- Conducted network and security system tests/audits, against the clients predefined scope of network assets; using the OWASP/MITRE penetration testing frameworks as guiding methodologies.
- Wrote comprehensive penetration reports to communicate technical and procedural findings and recommend solutions to Executives and IT stakeholders.
- Leveraged Open Source Intelligence (OSINT) and Darkweb Intelligence to consult clients on potential harmful publicly available company data and leaked users credentials.

Cyber Risk Engineer Manager May 2022 - October 2023
Cowbell Cyber, Pleasonton, CA 40+ hrs/week

- Led, managed and trained a team of 4 Senior and Junior Risk Engineers on how to consult with organizations at the $250M -$1B revenue range; explaining how to implement security controls and risk management best practices in accordance with National governance, risk & compliance (GRC) policies and European General Data Protection and Regulations (GDPR).
- Consulted Information Systems Owners on how to incorporate & test against Incident Response Plans and Business Continuity and Disaster Recovery Plans within their organizations.
- Performed, reviewed, and consulted security GAP assessments with organizations; providing information security recommendations to Executives & IT stakeholders.
- Developed and interpreted organizational goals by participating in multidisciplinary projects in areas such as threat intelligence, data science, and cyber claims.
- Developed & updated project plans for Cyber Risk Engineering projects including information such as project objectives, technologies, systems, information specifications, schedules, funding, and staffing.

Information Systems Security Manager April 2021 - May 2022
AMYX, Reston, VA 40+ hrs/week

- Served as cyber security Subject Matter Expert (SME) for Operational Technology (OT) Authorization of information systems and all associated cyber security policies, procedures, and processes for the Department of Defense (DOD).
- Monitored potential threats and vulnerabilities, and drove remediation efforts of identified risks and control deficiencies for the DOD.
- Supported the DOD's overall implementation and authorization, of improving cyber security capabilities for its enclaves; driving operational readiness.
- Oversaw performance of risk assessment and execution of system tests to ensure compliance in accordance with various NIST (RMF/DIACAP) frameworks.
- Leveraged eMASS for continuous risk assessment and ATO certification renewal of Government systems.

Information Systems Security Manager May 2017 - April 2021
US Navy — Defense Media Activity, Fort Meade, MD 40+ hrs/week

- Led a team of 8 high-performing military/civilians in the protection and continuous monitoring of over 796 DOD systems in accordance with NIST 800-53 utilizing eMASS to recieve ATO accredidations.
- Reviewed Host Based Security System (HBSS) reports as well as Assured Compliance Assessment Solution (ACAS) scans/reports for vulnerability assessments, patch management, and audit collection.

- Created, the first video point to point encrypted tunnel between two government agencies, Defense Information Security Agency (DISA) and Defense Media Activity (DMA), for secure communication and video broadcast.

Information Systems Security Officer August 2012 - May 2017
US Navy 40+ hrs/week

- Effectively led 20 Sailors in the managing, troubleshooting, and fixing of standard voice and data network infrastructure systems,secured terminal equipment and the trouble shooting of onboard Operational Technology (OT) and SCADA systems.
- Supported multiple Information Warfare Units and enhanced secure and non-secure voice communication via PICT terminals and POTS lines.
- Configured and stood up Satellite Communications (SATCOM) terminals for encrypted communication between Government and Military installations.

ACHIEVEMENTS

- Created a new service (Micro Penetration) and brought it to the Cyber Insurance Market - October, 2022
- Defense Media Activity Tech Service Performer of 2nd Quarter 2018
- 2x Navy Achievement Medal Recipient and 1x Joint Service Achievement Medial Recipient
- Earned Enlisted Information Dominance Warfare Pin (EIDW)
- USS Bonhomme Richard Sailor of the Year Award – 2014