**Phillip M. Harrell**

Colorado Springs, CO  Cell: (951) 772-3528  [phillip](mailto:phillip.harrellz@gmail.com)[.harrelly](mailto:.harrellz@gmail.com)@icloud.com



**C Y BER S E CURITY S PECIALI S T**

I am a highly skilled and dedicated Cyber Security professional with 15 years in information security. I pose a strong background in both military and civilian environments protecting and securing systems from cyber threats. My expertise lies in conducting vulnerability assessments, implementing robust SIEM tool security measures, and investigating and responding to security incidents. I am a reliable team player with excellent problem-solving skills and the ability to communicate complex security concepts to both technical and non-technical stakeholders.

**CERTIFICATIONS**

* **EC Council Certified Ethical Hacker (CEH)** 2014
* **CompTIA Security+ CE Professional (Sec +)** 2020
* **CompTIA Certified Advanced Security Professional (CASP)** 2016 (expired)
* **Cisco Certified Network Associate (CCNA)** 2012 (expired)
* **Microsoft Certified Technology Specialist (MCTS) – Windows Vista** 2009

**EXPERIENCED TECHNOLOGIES**

| Proofpoint RSA Archer Kali Linux Windows CMD  Ruby on Rails Splunk | Tenable Nessus Cisco/Brocade Networking  Network Security Design  Fortify WebInspect Web Application Assessment Remote Access Configuration | Active Directory  NIST & FedRAMP  BurpSuite Pro  PowerShell Scripting  Linux Terminal  Public Speaking |
| --- | --- | --- |

**WORK EXPERIENCE**

**Cyber Security Analyst Advisor Oct 2020 to Present**

General Dynamics Information Technology | Colorado Springs, CO

* Identifies network computer intrusion evidence and perpetrators.
* Performs forensic analysis of digital information and gathers and handles evidence.
* Monitors for fraud, waste and abuse, including content inappropriate to the workplace, Illegal Activity, Productivity Loss and Non-Compliant Activity, as well as Identity Leakage (PII).
* Utilizes tools such as Archer for case creation and management of incidents, Splunk and Proofpoint for granular verification of suspicious network activities
* Prepares case evidence and incident reports
* Works on special projects as assigned
* Created PowerShell script non-proprietary which provided 3400% speed of analysis gain with clear-and-present accuracy improvement in analyzing GBs of data vs an entire team of analysts using manual efforts alone
* Leverages AI for faster speed of delivery of application development with PowerShell and Splunk.
* Provides guidance and work leadership to less-experienced technical staff members

**Software Security Architect April 2020 to Oct 2020**

Access Data Consulting Corp | Denver, CO

* Evangelizes a security mindset with our development teams using OWASP and other

development/test integration best practices.

* Consults on NIST Cyber Security Framework and Risk Management Framework (RMF) activities to ensure robust security architecture is built into systems at or near infancy
* Deploys automated mechanisms to integrate audit logs, penetration testing, and vulnerability scans for investigation and response to suspicious activities.
* Identifies architectural and other security risks associated with the solutions, and compensating controls where necessary.
* Defines, documents and implements the technical architecture, operational processes and security

policies from engineering teams.

* Provide security architecture and advice in support of application development, and

infrastructure projects.

* Collaborates with teams to find solutions that minimize security exposure.
* Educates system administrators on security best practices and identifying common vulnerabilities.
* Acts as a resource and mentor for team members within the software organization, particularly

with regards to cybersecurity risk analysis, requirements, architectural design, and testing.

* Coordinates security activities with corporate Governance Risk and Compliance team.

**Penetration Testing and information Security Engineer Dec 2019 to March 2020**

Spartan Corp | Castle Rock, CO

* Leads penetration testing engagements against multiple commercial customers. Consults on assessment findings utilizing the NIST Cyber Security Framework and NIST Security Controls
* Leverages multiple penetration testing tools both with Kali Linux such as Burp Suite Professional, OWASP Zed Attack Proxy (ZAP), and command line based tools such as Curl and NMAP.
* Utilizes the OWASP Top Ten framework for assessing public facing web applications.
* Conducts enterprise level network penetration tests remotely IAW PTF and PTES frameworks.
* Performs automated and manual testing for identifying vulnerabilities not picked up in some scanners such as Brute Force detection and Vulnerable HTTP Methods
* Leverages Docker containers into multiple instances of Web Assessment tools due to efficient resource management and application availability
* Consults with customer’s regarding the implementation of FedRAMP System Security Plan Templates for building security and risk mitigation into the enterprise information system

**Information Systems Security Engineer / Manager March 2017 to Dec 2019**

ALKU Government Solutions | Herndon, VA / Aurora, CO

* Documents and describes multiple complex enterprise IT environments based on compliance frameworks including FedRAMP, NIST, CNSS, and FIPS security controls while balancing security requirements with customer mission priorities IAW ICD 503 guidance as Information System Security Manager
* Analyzes, reviews and approves Cloud security architecture documentation IAW NIST, DoD Directives, Instructions, Manuals and ICD 503 guidance
* Analyzes, configures, and executes PowerShell scripts which can loop through multiple recursive directories and thousands of files in order to identify objects containing specific criteria via regular expression (regex)
* Conducts Web Application and Database vulnerability scans using HP WebInspect in order to identify system attack surface/s while providing recommended guidance for patching and configuration to obtain C&A on multiple networks
* Presents correlation of returned Vulnerability IDs from Attack Status reports with Vulnerability Detail reports providing in-depth analysis of findings for system administrators and developers while providing Executive Summary information for Stakeholders
* Utilizes Nessus to create custom policies, active scans, and report generation for scope-specific requests
* Performs network common vulnerable ports and services check using NMAP for speed of use and reasonable accuracy; additional use is to determine presence of firewall between two hosts
* Applies Ariel Query Language syntax (AQL) to IBM Qradar in order to build dashboards reflecting system state-of-health and alerts for nefarious activity
* Utilizes Host Bases Security Solution (HBSS) to provide granular access and executable control of systems deployed within multiple network enclaves
* Provides Data transfers between multiple levels of network classification
* Adheres to NIST, DODI, and ICD 503 guidance for system hardening, cyber security best practices, and developing program TTPs for continuity of operations
* Applies Splunk query language in order to identify security related events
* Creates Splunk dashboards for security, administrative, and senior leadership which continuously report on network and system compliance ensuring end user cooperation with best practices

**Sr. Technical Analyst December 2016 to February 2017**

Parsons Inc. | ARL – Adelphi, MD

* Implements planning, coordinating, executing and providing deliverables associated with Command Cyber Readiness Inspection site-assisted visits IAW Department of Defense governance and performance measurement the Evaluator Scoring Metrics v9.2 (ESM), DoDI 8530.01, CJCSI/CJCSM 6510.01A/B, and NIST 800-53.
* Provides DoD Standards and Governance gap analysis from a technical configuration standpoint to federal mission organizations regarding cyber security posture
* Recommends and maintains effective and communication before and after assessments ensuring quality control and assurance procedures to ensure delivery of post-assessment reports.

**Cybersecurity Service Provider Auditor March 2016 to November 2016**

Booz | Allen | Hamilton / DoD - Chambersburg, PA

* Leads and conducts interviews with all Department of Defense Components (DoD) and all DoDIN/SE certified CNDSPs for the entire DODIN using as governance and performance measurement the Evaluator Scoring Metrics v9.2 (ESM), DoDI 8530.01, CJCSI/CJCSM 6510.01A/B, and NIST 800-53.
* Provides operational gap analysis in cyber security service providers’ functional capabilities to offer tailored enterprise services and mitigation strategies to their subscriber’s base of operations
* Serves as lead instructor for Client training course on the subject matter of the auditing and inspection methodology and philosophy; Provides students from DoDIN and Federal mission partner global operations community with guidance, philosophy, and applicability of the ESM and its higher supporting governance to their organization’s cyber security defenses
* Provides technical support and guidance to site personnel before, during, and after assessments on matters relating to determining quality of inter-collaboration between DoD Component Head and Federal mission partner organizations and their sub-component organizations capability to protect, detect/respond, and sustain operations and information stored, received, and transmitted on federal networks worldwide
* Presents audit findings in the method of observations and recommendations to audited site senior leadership regarding their operational and security posture following a Cyber Security Service Provider inspection

**25B – Information Systems Specialist Oct 2010 to Mar 2016** U.S. Army

* Highlights of duties, tasks, and rewards for the same follow

**IT Specialist/S2 Security Aug 2015 to Mar 2016**

302d Signal Bn – Ft. Detrick, MD U.S. Army

* Coordinated with Information Assurance on vetting incumbent Civilian and Service Members for both building and network access.
* Performed daily scrub of Army Training and Certification System to ensure that both Civilian and Service Members where up-to-date on mandatory training and PD certifications authorizing them for continued network access
* Successfully passed derivative training receiving access to JPAS in order to verify visiting persons clearance into facility
* Conducted weapons room inspections according to AR 190-11 standards and procedures
* Ensured badge and key control inventory on a daily basis and followed ‘end-of-days’ storage container security measures

**IT Specialist/Cyber Incident Analyst May 2013 to June 2015**

6th Regional Cyber Center - Korea U.S. Army

* Analyzed, executed and reported on approx. 3000 Cyber Attacks against information systems in support of United States Force Korea (USFK) mission and its subordinate military organizations.
* Interfaced directly with Brigade Commander giving a classified brief regarding cyber incidents on a semi-weekly basis. Received public praise from the same with Brigade Coin honors.
* Coordinate with Information Assurance (IA) on vulnerability assessments to collaborate, plan, and execute remediation of software vulnerabilities on over 130 RCC-K desktop operating systems IAW ARCYBER and other Higher Agencies (NIPR/SIPR).
* Key participation in 10 OPORD Capture-The-Flag exercises. Performed analysis, direction and execution against cyber-attacks using open source and proprietary sensors primarily from a defensive posture.
* Simulates live Cyber Attack environment: Analyzed firewall logs, IP Audit, SNORT, AD, and HBSS for filenames, hash of files, suspicious IP addresses, new account creations, escalated privileges, etc. Reported activity to ACOIC.
* Team Lead on Command Cyber Readiness Inspection (CCRI) 2015. Received impact award from 6th RCC-K for organizing, planning, and implementing remediation of discovered software vulnerabilities, user account deficiencies, network medium classification labeling, etc.
* Actively monitors, isolates and corrects issues with enterprise LAN/WAN networks, nodes, and transport services throughout the Korea Peninsula.
* General Officer level support, including working with CCST and VIP support teams, for Blackberry Enterprise Services, Enterprise Email, and Mobile Service Platforms.
* Creation of Friendly Forces Informational Reports (FFIR) for Cross Domain Violations and other network security lapses, including reporting instances to higher Army Cyber Commands.
* Conduct presentations and technical briefings at Company, Battalion, Brigade and Theater levels of congressionally appointed leaders of the US Army.
* Participated, assisted, and executed in live Penetration Tests.
* Scans and maps known IP address network blocks to identify live nodal connections, specific operating system, and unnecessary, STIG defiant, or other risk associated open ports.
* Engages potential vulnerable public facing webservers from White Hat perspective; identifies vulnerabilities such as clear-text over TCP/IP (HTTP,Telnet,FTP), default login credentials to network devices.
* Operates Flying Squirrel to identify, locate, and isolate rogue wireless events.
* Worked with covert 3-letter agency’s implementation of pilot program for application whitelisting.
* Analyzes, tests and executes custom Application Whitelisting signatures from log data provided by HBSS and SysInternals
* Ultimately left assignment with multiple awards and public recognition for leveraged efforts

**Network Management Technician Jan 2012 to May 2013** 169th Signal Battalion, U.S. Army Camp Walker, Korea

* Served as a network administrator on an automated systems team of approx. seven technicians.
* Developed and maintained Class B IP address database (Sharepoint) for coordinating, organizing, and assigning IP addresses for approx. 10,000 network devices.
* Configured, maintained, and secured approx. 750 layer 2/3 network devices (e.g., Cisco/Brocade ISR and BigIron/XMR, respectively) operating over IP and ADSL networks in support of U.S. and ROK Military installations throughout the Korean Peninsula on NIPR and SIPRnet.
* Configures, maintains, utilizes Brocade Iron View, Van Dyke Secure CRT, and Cisco Call Manager to remotely manage software configuration, security, and patch management updates.
* Created automated installation packages to deploy software or create custom Task Sequences for new Operating System Deployments.
* Configured, secured, updated, and maintained KG175-A/KG175-D network access/encryption devices
* Served as Acting Team Leader on specific projects as IOS upgrade in Camp Mujuk, DBIDS Fortress network access, ROKA network access for 2 Star General and his aide.
* Remotely blocked network access to suspicious users with coordination with Information Assurance Managers (IAMs). Our LAN/WAN team was the first to implement, configure and administer Port Security at the end-user level.
* Utilized Remedy Ticketing System to respond to customers issues and resolving system problems.
* Assisted the Team Leader to plan, organize and execute work projects such as network device configuration, IOS upgrade, and remote access hardening.
* Conduct presentations and technical briefings at Company, Battalion, Brigade and Theater levels of congressionally appointed leaders of the US Army.

**Information Technology Student Jan 2009 to May 2010** Mt. San Jacinto College Menifee, CA

* Completed collegiate level classes for a Windows System Administration, HTML Web Design, and Cisco Routing/Switching technologies
* Obtained MCTS in MS Vista Configuration
* Constructed a multi-page web site using HTML
* Configured routers for CSU/DSU internet connectivity via remote terminal putty graphical user interface and CLI
* Implemented OSPF routing protocols and spanning tree protocol within classroom hands-on labs
* Promoted MS Server 2008 to domain controller while adding print, DNS, web, and file server functionality

**Desktop Support Contractor March 2008 to Nov 2008** 169th Kaiser Permanente Information Technology Bakersfield, CA

* Served as local and remote desktop support and lifecycle hardware replacement administrator
* Upgraded desktops from Dell XP to HP Desktops while simultaneously using custom built environment to configure group specific images for deployment to approx. 5 separate hospital facilities
* Upgraded Point-of-Sale credit card machines IOS for all hospital locations in the Bakersfield area
* Provided customer helpdesk troubleshooting for end-user systems via remote assistance using PCAnywhere, Active Directory, and Merlin services.

**EDUCATION**

**Current Undergraduate**

The Pennsylvania State University, consolidated/earned 71 credits,

Expected graduation: 12/2023

**Diploma**, Hilltop Christian Academy, June 1998

**DoD Sponsored TRAINING**

**FEDVTE** Penetration Testing, HBSS, CEH V8, CCNA Sec

**SkillPort:** CEH, CASP, Windows Server 2008, Windows 7

**AIT: Information Technology Specialist**, Fort Gordon Signal School, June 2011

**Warrior Leader Course:** Noncommissioned Officer Academy, Cp Jackson Korea March 2015

**NSS PKI Trusted Agent Training,** CIO/G6, May 2014

**Derivative Classification,** Center for Development of Security Excellence, September 2015

**Additional Independent Research/Training**

**PCP:** InfoSecAddicts.com Pentest Candidate Program Jul-Sep 2017

**OSCP:** Offensive Security Certified Pentest Class, Oct-Nov 2017

**SANS GPEN:** Completed a week-long hand-on course for Penetration Testing

**RubyOnRails Web Application:** [*https://phillipsarticles.herokuapp.com/*](https://phillipsarticles.herokuapp.com/)

|  |  |
| --- | --- |