James Luther
4102407411
jamisl@gmail.com
Walkersville, MD 21793

Professional Certifications

Certified Information System Security Specialist (CISSP)
GIAC Assessor / Auditor of Wireless Networks (GAWN)
Certified Ethical Hacker (CEH)
Microsoft Certified IT Professional - Server Administrator (MCITP) Offensive Security Certified Professional (OSCP)

Profile

Sixteen plus years of experience in the Information Technology field to include extensive knowledge of malware analysis, development, penetration testing, network administration, network security, information assurance, installation, configuration, troubleshooting and maintenance of workstations, servers, network connectivity and services.

Programming Languages

C#, Objective-C, C++, Visual Basic, ASP.Net, Python, Perl, Ruby, Django, Node.js, PHP, HTML, JAVA, Javascript, vbscript, powershell, bash, go

Employment History

The House of Flynn - Vice President/CTO
Frederick,Maryland 2015-Present
Vice President / Chief Technology Officer

- Implemented and maintained all aspects of all information systems, applications, and development.
- Built and maintained store web application that support millions of users daily
- Built and maintained internal network, applications for tracking inventory, employees, and security monitoring.
- Developed integrated systems for monitoring industrial systems to include laser engraving, computer numerical control systems (CnC), 3d printing, and clothing manufacturing.
- Worked with the open source community to make available or incorporate the non-proprietary software into open source projects such as Home Assistant and OpenHAB.

Van Dyke Technology Group - Penetration Tester
Columbia,Maryland 2011-2016
Senior Security Controls Assessor / Penetration Tester

- Developed over 240 custom scripts/applications to automate the Security Testing Center's effectiveness.
- Performed penetration testing on over 200 multi-computer, multi-location, multi-environment

operational computing systems in support of NIST RMF testing and enterprise vulnerability assessments.

- Performed web application penetration testing in accordance with OWASP Testing Guide by testing for directory traversal/file include vulnerabilities, authorization bypass, privilege escalation, insecure direct object references, bypassing session management schema, exposed session variables, cross site request forgery, reflected and stored cross site scripting, HTTP verb tampering, HTTP parameter pollution, SQL injection, NoSQL injection (MongoDB, Google NDB), LDAP injection, XML injection, command injection, and heap and buffer overflow vulnerabilities.
- Performed network based penetration testing that specifically targets applications and their technology (server side of client server applications), specifically weblogic, tomcat, etc.
- Developed wireless penetration testing methodologies for the team and provided training for team members
  on all facets of wireless testing (wifi, bluetooth, rf, mobile).

- Reverse engineered multiple web and Java applications in order to gain operational knowledge of applications and generate automated penetration testing tools.
- Audited controls for systems in accordance with DCID 6/3 Controls as well as NIST 800-53 Controls.
- Continued public security research on mobile technologies, embedded systems and printer firmware and man in the middle attacks.
- Worked with SANS and other security researchers to develop SANS Sec-575 course on mobile security.

U.S. Army - Army Red Team
Fort Meade, Maryland 2010-2011
Wireless Malware Development Team Lead

- Developed over 250 different scripts and applications to perform a multitude of functions over all wireless technologies to include GSM, CDMA, RF, Wifi, Bluetooth, Zigbee, and WiMax.
- Developed a fully functioning lab to train team members on all wireless technologies, interactions, and custom tools to achieve maximum effectiveness as a team.
- Developed software and firmware for linux embedded systems as well as arm microcontrollers to target specific wireless technologies.
- Performed countless hours of security research on mobile device technology to aid in better security practices and more effective understanding of mobile device infrastructure.

U.S. Army - Server / Network Operations Manager
Fort Meade, Maryland 2008-2010
Server and Network Operations Manager for the 704th MI BDE S6.

- Maintained and expanded server and network operations of the entire 704th MI BDE and all of its 2500+ users worldwide.
- Provided e-mail services with Microsoft Exchange to the organization.
- Provided strategic analysis of network, software and asset usage with Microsoft System Center Configuration Manager, What's Up Gold and the Solar Winds suite of tools.
- Assisted with the planning of network upgrades from Windows 2003 to 2008, backbone infrastructure from 100MB/s to 1000MB/s and to 10000MB/s.
- Planned and created rigorous training programs to ensure all users were 100% compliant on Information Assurance and Personally Identifiable Information.
- Upgraded the SIPRnet backbone from 100MB KG-175s to 1000MB KG-255s.
- Increased help desk productivity by 450% by automating Microsoft Active Directory scrubbing with automated vbscripts that also generate reports on all activities, automating user expiration warnings with vbscript, as well as countless other Active Directory tasks using vbscript and powershell.
- Performed network vulnerability scanning using eEye Retina for all assets on multiple networks.
- Remediated all vulnerabilities using Microsoft SCCM, GFI Languard and Microsoft WSUS.
- Maintained a multitude of Microsoft technologies such as Exchange 2003, SQL 2003-2010, Sharepoint 2003-2010, SCCM, SCOM, Windows Vista, Windows 7, Active Directory Rights Management, Active Directory Federated Services, WSUS, and clustering services.
- Maintained other services such as VMware ESX/ESXi 3.0-4.5, McAfee HBSS, Blackberry Enterprise Management, Good for Enterprise, Symantec Endpoint, Backup Exec, and Symantec Endpoint Security
- Requested and maintained site DIACAP.
- Assisted in planning of server room expansion and supervised a team of 5 to move all servers to newly built server room quickly and efficiently to limit down time.
- Developed multiple training programs from basic technologies for incoming personnel to advanced training

for more experienced personnel as well as company certification programs to ensure administrators had expert knowledge in area of responsibility.

U.S. Army - Information Assurance Network Manager
Fort Stewart, Georgia 2006-2008

Information Assurance Manager / Red Team Member at 3rd Infantry Division G6

.

- Built the deployable communication server stack from the ground up in order to support the entire MND-C in Iraq.
- Scanned all network assets for IAVA compliance with eEye Retina as well as Nessus and reported through AVTR and Microsoft SCCM.
- Monitored all server and network traffic to ensure all 5000+ users were in compliance with all documented policies and guidelines.
- Implemented all DISA STIGs, MNC-I, and BBP security templates and guidelines to ensure all 10000+ division assets were hardened from all attacks.
- Designed and implemented Active Directory scripts on all Microsoft servers and workstations to ensure password cracking tools were defeated by replacing all local admins with ones specified in the script.
- Performed Penetration Tests on all MND-C assets from remote and local locations to ensure all guidelines, operating procedures and best practices were followed.
- Wrote countless penetration testing tools for multiple platforms to include Microsoft Windows, Linux and Blackberry to perform Bluetooth scanning and enumeration, wifi scanning and enumeration, nessus plugins and metasploit plugins to connect to remote servers. Other tools written include tool for scanning connected USB devices on all systems on the network, server enumeration tools for ldap, dap and active directory and lun stack smashing tools.

U.S. Army - Defense Message System Administrator
Heidelberg Germany 2003-2006
Defense Message System Administrator at 43rd Signal Battalion

- Maintained user accounts and systems for all of the European and African Defense Messaging System and Advanced Message Handling System to total over 10,000 users and workstations.
- Deployed 5 different Directory Service Agents throughout the area of operations.
- Migrated 10 servers from Exchange 5.5 to Exchange 2003
- Migrated all servers from Windows NT 4.0 to Windows Server 2000 and then again to Windows Server 2003.
- Migrated all domain user and computer accounts from Windows NT 4.0 to Active Directory in Windows 2000 using csvde and Exmerge.
- Maintained the Deployable Communications Package (DCP) for EUCOM and served as the team supervisor for over 15 different missions throughout Europe.
- Used MRSAT, STE and ISDN in conjunction with CISCO devices to multiplex over BRI ports to provide connectivity for the DCP.
- Developed training programs for the shift workers from basic shift supervision to advanced troubleshooting of all DMS/AMHS services, CA services, Active Directory and Microsoft Exchange.

Security Clearance

Top Secret with Full Scope Polygraph

Education

Dublin Institute of Technology, B.S. Computer Science 2008