Garrett Galloway

1471 W. Rockcrest Dr.
Bloomington, IN 47403

garrettg84@gmail.com

850-345-0037

Professional Experience

REN-ISAC — July 2014 - Current

Principal Security Engineer

- Served as point of contact for abuse notifications to the higher education space.
- Wrote security outreach notifications and advised on security incidents and procedures.
- Developed perl scripts and utilities to ease sending non-standard mass notifications.
- Attended industry conferences related to messaging, malware, phishing, hacking, and other security topics.
- Administered mail and database servers used in importing security feeds and sending automated security notifications for higher education.
- Fostered communication in the REN-ISAC community through active mailing lists and IRC channels by answering questions and releasing pertinent security information to members.
- Developed contacts at outside organizations such as ISPs, web hosts, and email providers to ease handling coordinated phishing and spam takedowns.
- Contributed new and unique intelligence to our intelligence framework (CIF/SES) based on analysis of various reported attacks.

Navy Civilian (NSWC Crane) — April 2011 - July 2014

IT Specialist NT-2210-5

- Wrote certification and accreditation packages for multiple systems following DOD8570 and DIACAP instruction.
- Applied technical security controls on Windows, Linux, OS X, VMware, and other embedded operating systems.
- Validated security controls (both technical and physical) for multiple accreditations.
- Performed multiple penetration tests of various networks and systems locally and OGA.
- Designed a classified wireless network using cutting edge encryption techniques and hardware.
- Implemented large VMware cluster across a large infrastructure with various hardware.
- Managed shared storage systems (SAN/NAS) for all servers.
- Managed Linux (Redhat and Debian variants) and Windows (2000-2008) servers.
- Designed and configured specialized measurement hardware for use in Linux and Windows.
- Security analysis on RF data and other captured protocols.
- Techniques development for electronic attack.
- Wrote multiple proposals for new research into emerging RF technologies.
- Advised multiple local organizations on current and newer CNO techniques.
- Evaluated commercial and open source penetration and security tools.
- Participate and speak in multiple forums and conferences.
- Scripted many administrative tasks in PowerShell on Windows and BASH on Linux.
- Created computer based device control interfaces for automating scientific equipment in C#.
- Microcontroller development using PICBASIC and C.
- FPGA development using Altera Quartus for custom hardware used in signals processing.
- PCB troubleshooting and modification for additional capabilities.

SAIC/URS – Navy Contractor — July 2009 - April 2011

Virtual Network Engineer

- Performed high level security analysis on developmental systems for DoD C4I systems.
- Developed automated remediation tools for certification and accreditation process.
- Managed base wide vulnerability scanning using SCCVI (eEye Retina).
- Redeployed HBSS (McAfee EPO) base wide.
- Created secure OS builds for certification and accreditation process.
- Developed virtual testing environment.
- Brought a new package from concept to running accredited system in less than 6 months.
- Explored new areas of research for the business unit.

Vincennes University — August 2010 - August 2011

Adjunct Faculty of Digital Forensics

- Taught digital forensics for multiple course sections.
- Designed the course curriculum around required materials.
- Guest lecturer on various IT security topics for other courses.
- Course topics include: File systems, file types, log analysis, operating systems, boot processes, basics of Bash shell, steganography, encryption, evasion techniques, attack techniques, common hacker tools, common forensics tools, forensic process, forensic documentation, and related legislation.

AEIT - Office of Information Security — May 2008 - July 2009

Enterprise Information Security Analyst

- Draft and approve security policies, guidelines, and best practices for all State of Florida Agencies.
- Design and develop enterprise level security analysis tools.
- Provide training at enterprise level meetings on various security topics.
- Provide technical guidance and assistance statewide on computer security incidents.
- Cooperate with and provide assistance to Florida Department of Law Enforcement and FBI on investigations involving State of Florida.
- Provide technical analysis on numerous security related policies.
- Evaluate enterprise level security vendors in all aspects of security.
- Audit several state agencies on best security practices.
- Developed new infrastructure for AEIT from the ground up.

Florida Department of Health — April 2007 - May 2008

Security Administrator

- Planned and strategically implemented SNORT IDS sensors throughout an enterprise network.
- Backup system for linux and Windows servers.
- Created and managed virtual machines using VMware ESX and VMware server.
- Participated in the implementation of the ITIL process throughout the IT group.
- Designed and automated many different security related task through scripting in BASH, Perl, and VBScript.
- Developed multiple web applications for security services and other IT related services using Perl, PHP, java and AJAX concepts.
- Drafted and distributed many different simplified guides, instruction manuals, and installation walkthroughs.
- Managed ACLs on inbound and outbound email gateways.
- Managed anti-spam and virus scanning software for border proxies and email.
- Managed BlueCoat devices for proxy services and network site to site tunnel compression.
- Installed and administered many Fortinet hardware firewalls.
- Used Fortinet GUI and CLI to create and maintain policies for network usage.
- Created various forms of VPNs using Fortinet products.
- Log analysis from different sources including syslog, rancid, and others using SecureVue eiQ and various scripts.
- Vulnerability scanning using QualysGaurd enterprise utilities and appliances.
- Web application vulnerability testing using IBM Rational/Watchfire AppScan as well as manual assessment.
- Installed and managed many linux/MySQL database servers for various tasks throughout the DOH.
- Served in a 24/7 on call rotation one week out of every four weeks to respond to security and connectivity related issues.
- Managed authentication methods using LDAP, Radius, TACACS, and TACACS+ for several different platforms.

Florida State University – Facilities — April 2006 - April 2007

Network Administrator

- Team lead for a group of desktop support technicians.
- Implemented and Managed a network for over 350 users.
- Designed the Active Directory infrastructure for use throughout our locations.
- Designed and managed all core networking services for the department including dns, dhcp, wins, and ACL's.
- Migrated an existing Windows NT4 domain over to a Windows Server 2003 Active Directory Domain.
- Restructured and designed a new SAN/NAS for user and server data
- Engineered a firewall, anti-virus, and anti-malware solution for desktops and servers.
- Implemented Nagios to monitor all servers and networking equipment.
- Architected a backup system for all user data and server data.
- Used various tools for security scanning and service mapping including Nessus and NMAP
- Assisted in the management of a Sun Solaris 9 and Oracle 8-10 database server.

- Built custom servers optimized for special needs including file I/O, memory usage, and CPU usage.
- Created hardened and locked down desktop images for all users.
- Implemented RIS and Norton Ghost servers for increased desktop support efficiency.
- Instructed small classes for the newly created workflow architecture for struggling and new users.
- Managed ArcGIS Enterprise server and licensing servers.
- Managed a small cluster of Citrix servers for remote users.
- Performed usability testing for field deployable tablets, slates, and convertible notebooks.

East Coast PC Repair June 2004 - August 2005

Owner

- Acquired all licensure and certifications for a home based business.
- Developed an advertising plan and established a large customer base of both small and medium businesses and individuals.
- Organized and scheduled a team of 4 technicians on house calls and small business calls.
- Worked in teams of 2 or 3 technicians for large projects that included entire business IT solutions.
- Designed and installed IT solutions for several small businesses using Microsoft products and small office networking hardware.
- Virus analysis and manual removal on mission critical small business servers.
- Off-site backup services and solutions.
- Data recovery for failed computers and servers.
- Built custom computers to customer specifications.
- Built custom servers to customer and customer's vendor specifications.
- Developed custom software applications using C++, VB and Python.
- Developed web sites and web applications using PHP, Java, HTML and ASP.
- Performed penetration testing and vulnerability assessment for small business clients.

Education

A.A. General Studies - Tallahassee Community College
Graduated April 2006
B.S. Information Technology Security - Western Governors University
Graduated April 2009
M.S. Information Security and Assurance (MSISA) - Western Governors University
Graduated December 2013

Technical Skills

Networking and Cabling, TCP/IP, Firewalls/Routing/Switching (Cisco, Fortinet, and Vyatta), VPN (Cisco, Fortinet, and Microsoft), SAN/NAS Storage Systems, Operating Systems (Windows 2000+, Redhat variants, Debian variants, and Apple), Active Directory, Group Policy, Databases (MySQL, postgreSQL, and MS SQL) Virtual Machines (VMware, Oracle, and Microsoft), Security Incident Write-ups, Incident Handling, IT Project Planning, IT Project Management, Intrusion analysis, Penetration Testing, Intrusion Detection Systems and Intrusion Prevention Systems, Coding: C/C++/C#, PHP, Java, Java Script, Perl, Visual Basic, VB Script, PowerShell, M68k and x86 Linux/Windows Assembly, Bash/Shell Script, Python, HTML, AVR C/C++, and PIC C

Certifications

GIAC Certified Incident Handler - February 2015
Cisco Certified Entry Networking Technician (CCENT) - August 2013
GIAC Certified ISO27000 Specialist (G2700) - June 2013
EC Council Certified Hacking Forensic Investigator (CHFI) - February 2013
EC Council Certified Ethical Hacker (CEH) - December 2012
CompTIA Linux+ - April 2011
LPI LPIC 1 - April 2011

Microsoft MCSA: Security - April 2009
Microsoft MCP 70-291 - April 2009
Microsoft MCP 70-298 Designing Security - February 2009
Sun (Oracle) Certified Java Associate - February 2009
CompTIA Security+ - January 2009
CIW Database Design Specialist - January 2009
CIW Professional - January 2009
CIW Site Designer - January 2009
CompTIA Project+ - January 2009
CIW v5 Associate - December 2008
ITIL Foundations Certified - July 2007
Microsoft MCDST - March 2006
Microsoft MCP 70-271 - March 2006
Microsoft MCP 70-272 - March 2006
Microsoft MCP 70-270 - March 2006
Microsoft MCP 70-290 - March 2006
CompTIA A+ - February 2006
CompTIA Network+ - February 2006

Recent Training

SANS Online
SEC504 GIAC Certified Incident Handler - Nov 2014 - Feb 2015

Focus Learning Systems
CompTIA A+ - February 2006
CompTIA Net+ - February 2006
Managing and Implementing a Server 2003 Environment - March 2006
Implementing, Managing, and Maintaining a Server 2003 Network Infrastructure - March 2006
Planning, Implementing, and Maintaining a Server 2003 Active Directory Infrastructure - August 2006
ITIL Foundations - July 2007

Sans 2008 - Orlando
SANS 2008 - SEC401 Security Essentials

ACT Online Cyber Security Training
Information Security for Everyone - February 2009
Cyber Ethics - April 2009
Cyber Law and White Collar Crime - April 2009
Information Security Basics - March 2009
Digital Forensics Basics - April 2009
Business Information Continuity - April 2009
Information Risk Management - April 2009

State of Florida - Information Security Manager Training
Fluke Networks OptiView Training - October 2008
Qualys QualysGuard Appliance Training - January 2009

Sentinal Training

Cybersecurity: Incident Handling and Response - January 2009

Microsoft WorkshopPLUS
Active Directory Troubleshooting - June 2007

Software Engineering Institute - Carnegie Mellon
Advanced Information Security for Technical Staff - June 2009

Offensive Security
Penetration Testing With Back Track - July 2010