**David A. Vaughan**, CRTO, OSWP, GPEN,C|EH,ITIL2011, Security+

LinkedIn Profile: <http://www.linkedin.com/pub/david-vaughan/31/b37/320>

**Objective:** Seeking a challenging penetration testing / red team role to enhance my skills and provide value where results are paramount

**Technical Tools Summary**

|  |  |
| --- | --- |
| Security Tools | ATAT, Powershell Empire (original and BC-SECURITY fork), Veil Framework, Metasploit Framework, SSLScan, lbd, Bloodhound, DBD, Android Meterpreter, Asleap, HostAPD-WPE, Airgeddon, Nethunter, Nmap, Zmap, massscan, Trend Micro IMSVA & OfficeScan, Microsoft TMG, Lancope, Exabeam, Tanium, Hashcat, John the Ripper, Medusa, THC Hydra, Reaver / Bully, WiFi Pineapple, BashBunny, USB Rubber Ducky, Ferret & Hamster, driftnet, dsniff, Responder, C# exploit tools such as the Ghost Pack Suite, Imperva, Incapsula, Whitehat, Armitage / Cobalt Strike, Arachni, Security Onion, Metasploit Framework, Nexpose, W3AF, OWASP ZAP, Burp Suite, TripWire, Palo Alto NGFW, Cisco / Sourcefire FireAMP, SNORT, Sguil, Snorby, SQueRT, OSSEC, Kibana, Kenna, Alert Logic, Cylance, Qualys, McAfee Host Intrusion Prevention (MHIPS), Proventia/BlackIce/Real Secure Desktop Protector (RSDP), Comodo, & many other firewall suites and Spyware/Ad-ware/Anti-virus packages including: AVG, Avast, MS Security Essentials, Eset NOD32, Trend Micro, Norton, McAfee, Spybot S&D, TDSS Killer, Malware Bytes, BitDefender, etc., etc. |
| Operating Systems | All Windows versions from Server 2000+, Many Linux Versions based on Debian, RHEL, and Gentoo including: RedHat Enterprise 9.0+, Ubuntu (All Versions), Fedora 12+, and Linux BackTrack 2+, Kali, ParrotOS, BackBox, Santoku, Mac OSX |
| Software | AWS, Docker, Awk, Sed, Grep, Windows Active Directory, Wireshark, Tcpdump, Splunk, Cisco, ServiceNow, VNC, RDP, Webex, Dame Ware, and NetMeeting, Logmein, Teamviewer, GoToMeeting, many remote software suites, Juniper Network Connect, SSL VPN, VSClient, iPassConnect, iPass Mobile Office Client V6, and Nortel Networks IPSec VPN clients, Mobi Control MDM, Sharepoint, etc., etc. |

**Skills Summary**

* Author of the Attack Team Automation Tool (ATAT) <https://github.com/ll3N1GmAll/ATAT>
	+ Showmecon 2018 – <https://youtu.be/9r8-WeryaN8>
* Designer of the ch0mps password auditing platform
	+ Showmecon 2019 – <https://youtu.be/R--w84fdytg> OR <https://youtu.be/Jw2141v6bk0>
* Passionate about security and finding new ways to break into systems as well as defend them
* Proficiency in application vulnerability assessment tools
* Proficiency in network and server assessment tools
* Coding/scripting experience in python, powershell, bash, php, java, perl, go, C#, and C
	+ Sample projects can be viewed at <https://github.com/ll3N1GmAll> OR <https://gitlab.com/ll3N1GmAll>
* Strong analytical and problem solving skills focusing on new and inventive ways in
* Proficiency in manual and automated techniques for penetration testing and executing vulnerability assessments
* Ability to analyze vulnerabilities, appropriately characterize threats, and provide remediation advice
* Understanding of core Internet protocols
* Understanding of encryption fundamentals (symmetric/asymmetric, CBC operations, AES, etc.)
* Strong oral and written communication skills, including a demonstrated ability to prepare documentation and presentations for technical and non-technical audiences

**Technical Skills**

* An accomplished professional with excellent communication skills: visual, oral and written and excellent at multitasking
* Wide ranging experience in both computer hardware and software
* Professional experience in computing security since 2007
* Threat modeling
* Advanced skills in:
	+ Network security auditing
	+ Penetration testing
	+ Security engineering/architecture
* A strong grasp of network & wireless communications including:
* OSI model
* encryption protocols
* VPN networks
* Enterprise authentication of many types
* Proficient with Blackberry exchange server including Blackberry encryption, setup, and troubleshooting
* Android OS
* Code review
* A novice programmer with experience in Visual Basic, VBScript, Javascript, Python, C, and HTML
* Automating tasks via scripting
* Penetration Testing
* Wired & wireless networking & security
* VPN connectivity
* PCI-DSS, SOX, HIPAA
* Vulnerability assessments
* TCP/IP protocols
* General hardware/software troubleshooting
* DNS
* DHCP
* Proxies

**Work Experience**

####  Ethical Hacker / Senior GRC Consultant

***<private>***

September 2019 – Present Saint Charles, MO

* Perform internal and external penetration tests against client web applications, network infrastructure, Windows, \*nix variants, and Android to discover and exploit vulnerabilities
* Create comprehensive and accurate penetration testing reports with recommendations for appropriate remediation
* Collaborate with platform owners in a consultative manner to work toward remediation of the issues identified in testing
* Develop scripts, tools, and methodologies to enhance the penetration testing processes & overall security posture
* Develop and maintain the penetration testing team’s processes and documentation
* Perform regular maintenance of documentation and provide process improvements to the penetration testing processes on a regular basis
* Perform well known and proof of concept exploitation techniques
* Create new chained methods for the exploitation and post exploitation process to better illustrate the value of identified vulnerabilities
* Provided findings to client leadership and aid in the appropriate prioritization of what is discovered
* Provide a better understanding of the risk and financial impact associated with each finding in terms that are meaningful to our client’s senior leadership

#### Information Security Architect – Red Team Lead

***<private>***

May 2019 – Present Saint Louis, MO

* SSDLC Security Architecture projects responsible for security requirements, architecture design, SAST and DAST scan reviews in support of GDPR
* Perform and lead web application, API endpoint, and cloud environment penetration testing, remediation testing and vulnerability scans
* Perform and lead internal Red Team operations
* Manage penetration testing and red team personnel
* Collaborate with platform owners to facilitate remediation efforts
* Supervises tier one, third-party SOC services and provides tier three incident response support to the Information Security team
* Create process automation for the SOC team’s duties where appropriate (i.e., for Qualys/Cylance/Crowdstrike Etc.)

#### Lead Ethical Hacker / Security Engineer – Attack & Penetration Team

***Spectrum / Charter Communications***

July 2017 – May 2019 Saint Louis, MO

* Perform internal and external penetration tests against corporate web applications, network infrastructure, Windows, \*nix variants, and Android to discover and exploit vulnerabilities
* Create comprehensive and accurate penetration testing reports with recommendations for appropriate remediation
* Collaborate with platform owners in a consultative manner to work toward remediation of the issues identified in testing
* Develop scripts, tools, and methodologies to enhance the penetration testing processes & overall security posture
* Create the penetration testing team’s processes and documentation
* Perform regular maintenance of documentation and provide process improvements to the penetration testing processes on a regular basis
* Perform well known and proof of concept exploitation techniques
* Create new chained methods for the exploitation and post exploitation process to better illustrate the value of identified vulnerabilities
* Provided findings to leadership and aid in the appropriate prioritization of what is discovered
* Provide a better understanding of the risk and financial impact associated with each finding in terms that are meaningful to senior leadership

#### Senior Security Analyst

***Enterprise Holdings Inc.***

June 2014 – July 2017 Saint Louis, MO

* Working as a senior analyst inside the Security Operations Center (SOC) with the responsibility of developing and enhancing processes for monitoring host and network based Intrusion Detection/Prevention Systems (IDS/IPS), Web Application Firewalls (WAF), spam email filters, SIEM, log correlation, and anti-malware tools among others
* Engineering new solutions and developing maturity for all of the SOC's current utilities and processes
* Develop scripts, tools, and methodologies to enhance EHI’s investigation processes & overall security posture
* Create comprehensive and accurate incident & investigation reports with recommendations for appropriate remediation
* Responsible for creating logic that correlates events and identifies potentially abnormal system and/or user behavior
* Develop alerting that creates incidents for preliminary security investigation by the Monitoring Team
* Conduct in depth analysis in large scale or critical investigations
* Assess incidents to establish threat potential; and manage the incident response process
* Manage and coordinate efforts for large incidents that require multiple people and/or teams to identify root cause and work to mitigate the issue
* Develop and manage the threat and vulnerability management process
* Communicate with DHS, FBI, Secret Service, etc. to integrate intelligence data into a comprehensive understanding of our threat landscape and the threat actors pertinent to our environment

#### System Administrator & Internal Penetration Tester

***Dentwizard International***

July 2011 – June 2014 US & Canada Corporate Headquarters Bridgeton, MO

* Perform internal and external penetration tests against corporate web applications, network infrastructure, Windows, \*nix variants, and Android to discover vulnerabilities
* Create comprehensive and accurate penetration testing reports with recommendations for appropriate remediation
* Develop scripts, tools, and methodologies to enhance DWIZ’s penetration testing processes & overall security posture
* Domain Admin responsible for creating and applying companywide GPOs
* Troubleshoot complex network and mobile device components and infrastructure
* Implement client and server side network and security solutions
* Facilitate and coordinate large scale mobile PC deployment and training with the IT team
* Manage & Admin SonicWall Wireless network infrastructure
* Assess and maintain all company wide security policies, i.e. infosec, remote access, mobile device, acceptable use, etc.
* Manage and maintain security standards on externally facing and internal resources
* Coordinate and assess third party penetration tests
* Conduct regular internal vulnerability and penetration tests
* Implement threat and vulnerability mitigation techniques
* Run regular vulnerability assessments and penetration tests on company resources to verify a high degree of network security
* Sole party responsible for the acquisition, setup, configuration, monitoring, and maintaining of SNORT based IDS & network security monitor
* Sole party responsible for the acquisition, setup, configuration, monitoring, and maintaining of FOG imaging server

#### Tier 2 Remote Access Services Analyst & Trainer

***Boeing***

May 2007 – July 2011 St. Louis, MO

* Windows based support in an enterprise environment with 50000+ users
* Customer Service - fielding support issues
* Created technical instruction scripts for analysts also maintaining & updating technical knowledge base documents
* Promoted to top tier Remote Access team and top tier Blackberry team within 6 months of hire
* Designated SME (Subject Matter Expert) for all internal (on-site) Boeing wireless support and structuring issues for the entire Enterprise
* Increased 1st level resolutions by implementing necessary trainings and modifying troubleshooting scripts as defined by ticket trends and issue tracking
* Designated SME for all virtual (off-site) network infrastructure and VPN connectivity support issues Enterprise wide
* Installing, configuring, analyzing, troubleshooting and administering networking, windows, security, and department specific software suites; ranging from responding to client side error messages to system wide events
* Analyze issue trends and implement process improvements ranging from training and/or system modification to new system implementation
* Promoted to RAS trainer for all new hires on 06/2010 (1 of only 2 Enterprise wide)
* A member of the SkillDev Team responsible for creating and maintaining: training materials for new hires; including knowledge checks and PowerPoint presentations, knowledge assessments for promotions to 2nd level, 2nd level road-maps for perspective 1st level analysts to complete; proving competency in necessary fields, & 2nd level assessments for 1st level analysts to take before being allowed into 2nd level
* Working with IT infrastructure groups to determine necessary authentication models for internal and guest wireless networks
* Personally tracked down and transitioned hundreds of factory and office users to increased wireless security types and in many cases coordinated the acquisition of new equipment to meet the WPA2-Enterprise encryption standard
* Delivering clearly conveyed communications to upper level management describing required authentication types and business needs
* The only EHD technician invited to work with the IT Infrastructure group to assist in the sunset of antiquated wireless networks and coordinate the smooth transition to updated wireless networks with WPA2 Enterprise encryption for the entire enterprise network.
* Worked closely with the enterprise IT Infrastructure group to increase capacity, integrity, and exclusivity of our guest wireless network
* Received 5 performance related pay raises in my first 3 years on the job

**Education**

**CRTO** Certified Red Team Operator

* Passed the certification exam on first attempt - November 27th – December 1st 2022
* Credential ID 638929827ebb967589788186

**OSWP** Offensive Security Wireless Professional

* Passed the certification exam on first attempt - November 12th 2019
* Credential ID OS-BWA-24751

**GPEN** GIAC Penetration Tester

* Passed the certification test on first attempt - November 16th 2016
* Credential ID 156178

**C|EH** Certified Ethical Hacker v8

* Passed the certification test on first attempt - April 23rd 2015
* Credential ID ECC046437

**ITIL 2011** certified

* Passed the certification test on first attempt - 2014
* Credential ID 14443-777809

**CompTIA** **Security+** Certified

* Passed the certification test on first attempt - May 2011

Fall 2002-Spring 2005 (Graduated June 7th 2005) ITT Technical Institute Arnold, MO

* Associate in specialized Technology Degree
* Major: Information Technology – Web Development Program

**Honors & Awards**

#### SANS Security 560 Capture The Flag Challenge Coin

##### GIAC SANS

August 2014

Awarded the SANS Security 560 Penetration Testing and Ethical Hacking capture the flag challenge coin in a hands on practical application tournament applying penetration testing techniques.

November 2016 *(Also noted below in community involvement)*

I was invited to the GIAC SANS advisory board as a result of my performance on the SANS GPEN certification test. This advisory board is a panel to discuss formal issues directly related to GIAC and SANS business such as training and certification.

**Community Involvement**

**Executive Board Member & Co-Founder**

***BSidesSTL***

December 2015 – Present

* Currently active on the Board of Directors for BSides Saint Louis
* We are actively developing the 2016 conference and building the BSidesSTL brand
* Running lock pick village
* Personally designed & built the lock pick village

**Executive Board Member & President**

***Community Education Facilitators d/b/a 31337 80X***

July 2013 – Present Saint Charles, MO

31337 80X (Elite Box) is dedicated to reaching and serving our community. We strive to learn and grow in our understanding of computer science and information security. We then invest in our community by sharing what we learn in the form of public events, conferences, private classes, etc.

Elite Box is dedicated to developing a community with access to information, tools, skills, and personal development opportunities. We have a passion to create, to learn, to teach, to grow, and to help people!

**GIAC SANS Advisory Board Member**

November 2016—Present

I was invited to the GIAC SANS certification advisory board as a result of my performance on the SANS GPEN certification test. This advisory board is a forum to discuss formal issues directly related to GIAC and SANS business such as training and certification.

**References**

Richard Kirby (retired)

EHD 2nd level RAS Technical Team Lead



\*Additional references available upon request\*