Jonathon A. Williams

1555a Byam Rd.
Cheshire, CT 06410
917-993-3784
jon@spectralilluminations.com

Proficiencies

Penetration Testing (Tools)

- Kali Linux, Nmap, Netcat, SSH, Putty, Metasploit, SQLmap, Wireshark, John the Ripper, Hashcat, Hydra, Nikto, Dirb, Beef, Proxychains

Penetration Testing (Skills)

- Network scanning, Traffic sniffing, Vulnerability research, Simple buffer overflow exploitation, Exploit customization, Cross-compiling, Web application attacks (fuzzing, XSS, CSRF, SQL injection, RFI/LFI, path traversal, session hijacking, authentication bypass), Windows & Linux privilege escalation, Post-exploitation, Proxying, Tunneling, Pivoting

Security Engineering

- OSSEC, Elasticsearch, Logstash, Kibana, OpenVAS, ModSecurity, Fail2ban, RKHunter, Iptables, ClamAV, OpenLDAP, Duo Security Authentication Proxy, PKI

Systems Administration

- Debian, Ubuntu, RedHat, CentOS, Apache, PHP, Java, Tomcat, Ruby on Rails, Passenger, MySQL, PostgreSQL, Exim, Postfix, Dovecot, OpenDKIM, OpenSSL, Subversion, Squid, Cron, Chef, Ansible

API Integration

- Authorize.net (payment gateway), Google Tag Manager, Twitter, LiveChat (real-time customer support), Weather Underground (weather data), New Relic (server monitoring)

Languages

- Bash, PHP, SQL, HTML, CSS, Javascript, XML, RegEx

Education

Offensive Security

- OSCP Certification (in progress, expected July 2016)

CompTIA

- Security+ Certification (valid until April 2017)

SIT Graduate Institute

- MA Sustainable Development (May 2009)

Pennsylvania State University

- BA Sociology (May 2004)

Work History

IGG Software, Inc. (July 2005 - present)

- Security engineer - 3 years
- Systems administrator - 6 years
- Web developer - 10 years
- Quality assurance - 5 years
- Documentation - 11 years
- Customer support - 8 years

Selected Experience

Administration & Engineering

- Remotely administered 13 virtual CentOS servers and all matters relating to network, host, and application security.
- Conducted two data center migrations, automated infrastructure, and overhauled security stance.
- Assisted with defining network segments and configured tiered application stacks for high-security web services.
- Followed OWASP, NIST, and CIS guidelines to establish secure baseline configurations for all apps.
- Installed OpenLDAP for role-based access control.
- Configured Duo Security for two-factor authentication.
- Installed OSSEC for log aggregation and analysis, file integrity monitoring, alerts, and active response.
- Set up ELK stack for visualization and further analysis.

PCI Compliance

- Worked with third party service provider to define scope and classification, then implemented all requirements.
- Reviewed quarterly vulnerability scan reports, identified false positives, and mitigated remaining issues.
- Following reclassification from SAQ-A to SAQ-D under DSS 3, conducted internal vulnerability scans, installed WAF, added audit logging to our web store, expanded documentation, and increased staff security training.
- Ultimately redesigned billing platform to remove us entirely from PCI scope.

Documentation & Training

- Documented infrastructure via network diagrams, service and protocol maps, firewall justification lists, data flow illustrations, and more.
- Authored security policies governing employee conduct, password use, customer support, employee release, incident response, and more.
- Conducted code reviews with development staff.
- Worked with QA staff to integrate security into test plans.
- Administer periodic security training to all levels of staff.

Current Primary Responsibilities

- Monitoring security alerts, investigating anomalous events, and following up on suspicious activity.
- Observing trends and recommending proactive changes.
- Keeping abreast of latest threats and sharing knowledge.
- Carrying out penetration tests against our web services.
- Decoding and analyzing malicious payloads to better understand intercepted attacks.