Joseph Giron

2150 E Evans Dr • Phoenix, AZ 85022 • (512) 902-3787• joe@gironsec.com

Summary of Qualifications

Dedicated Problem Solver, looking for exciting new challenges. Brings strong background in programming languages and application security, looking for an opportunity to work with a team to lead and teach new skills. Strong malware analysis and reverse engineering background with emphasis on x86/x64 Intel assembly. Excellent background in exploit development.

Certifications / Education

- **Security+ Certification, 2013, CEH Certification 2013, CEMA 2017**
- **Several Published CVE's:**

  http://insecure.org/search.html?q=joseph.giron13
- **Numerous security whitepapers**

  Available for download at http://gironsec.com/papers

Accomplishments

- Spoke at InfoSec Southwest 2012, Toorcon 2012-2016, CactusCon 2013- 2017, HOPE 2014, and have also given seminars / training courses.
- Discovered numerous 0day vulnerabilities in open and closed source software between 2006 and now.
- Performed tech review for https://www.packtpub.com/networking-and-servers/windows-malware-analysis-essentials
- Member of the Phoenix OWASP, The Phoenix 2600 chapter and the Phoenix ISSA.
- Awesome blog updated regularly http://gironsec.com/blog

Technical Skills

Software:

HyperV, MSSQL, MySQL, FireEye, Visual Studio, Hailstorm, BurpSuite, IDA Pro, Ollydbg, Immunity Debugger, Metasploit Framework, Apache, IIS, Active Directory, ColdFusion, Mcafee EPO, LastLine, Vmware / VirtualBox / Qemu, Volatility, Bindiff, HP Fortify, Checkmark, AWS, Cloud based computing, Azure

Operating Systems:

Windows Server 2k-2k12 / Linux (FreeBSD, Ubuntu, RHEL, Debian. CentOS, FreeDOS, etc)

Programming Languages:

C, C++, C#, PHP, Perl, Visual Basic, Python, Intel asm (x86/x64), Ruby

Special Skills:

Reverse Engineering (malware), Source code analysis, Incident Response, PCI compliance testing, vulnerability management, risk assessment, penetration testing, software development.

Professional Experience

LunarLine Inc, Washington, DC
Senior Penetration Tester Mar 2016 – Present

- Worked primarily performing penetration tests on various government clients.
- Made extensive use of SQLMap, BurpSuite, Metasploit, Nexpose, masscan, nmap, SoapUI, WebScarab, and SET, depending on the engagement.
- Performed social engineering engagements, phishing attacks, recon, physical assessments, and web based attacks.
- Trained lower level employees on the basics of security, reverse engineering, and penetration testing.
- Threat intelligence gathering
- Worked on Mobile app pen testing on android and IOS devices.
- Source code analysis of Perl and .Net technologies
- Worked with the federal government and US Court and PACERNET systems.

Wells Fargo, Phoenix, AZ Sept 2018 – May-2019
Red Teamer (Contractor / part time)

- Web application pen testing utilizing BurpSuite and W3AF.
- Performed external network discovery and OSINT for Wells Fargo's external assets
- Did programming and scripting for projects related to the red team for the purposes of discovery and acquisition of new targets / attack surfaces

Megaplan-IT, Phoenix, AZ Jun 2016 – Sept 2018
Senior Penetration Tester (Contractor / part time)

- Source code review in many languages including; java, python, php, C#, perl
- Web application and network penetration testing
- Mobile application penetration testing as well as mobile code review
- Performed Incident response and forensic investigations
- Heavy usage of BurpSuite and HP Fortify
- Worked on cloud-based environments such as MS Azure and Amazon Web Services.

LastLine , Santa Barbara ,CA
Malware Reverse Engineer Mar 2015 – Feb 2016

- Primarily work with IDA pro, qemu, and ollydbg to reverse engineer malware and exploits threats in both the user-land and kernel mode space.
- Develop signature matching algorithms in python, YARA, and FLIRT for binary matching and differential analysis of malware signatures.
- Dissect 0day threats and malware from APT's and threat actors across the world to deliver the latest and greatest threat research.
- Publish blog posts about malware analysis and threat research.

Synack Inc, San Diego,CA
Security Red Team Dec 2014 – Jan 2016

- Performed web app penetration tests and collect bug bounties for various clients.
- Work primarily with BurpSuite and NetWitness.
- Have collected bounties for various items such as SQLI, XSS, CSRF, and code injection.

American Express, Phoenix, AZ
Malware and Forensics Security Investigator Dec 2013 – Oct 2014

- Was the chief malware / reverse engineer for Amex.
- Regularly performed training for analysts and engineers alike.
- Did special projects and research and performed penetration tests within the internal network.
- Performed threat intelligence gathering from various APT's and
- Developed internal malware database as well as internal tools for the analysts to aid in the detection / prevention of malware.
- Worked with various departments to implement policy changes to strengthen defenses and limit compromise.
- Performed forensic investigations for special cases / management compromises.

American Express, Phoenix, AZ
Security Analyst Jun 2013 – Dec 2013

- Administered full disk encryption with Open PGP on all assets.
- Monitored network for DDOS traffic with trending tools like FrameFlow and Prolexic.
- Worked with FireEye and EPO to document and analyze malware for incident reporting and root cause analysis.
- Wrote snort rules and administered Mcafee IPS / HIPS policies.
- Reverse Engineered malware and trojans using both static analysis tools (like IDA and BugDB) as well as dynamic analysis with tools like Immunity Debugger, Exe Suite, and various unpacking frameworks.
- Tested IPS / HIPS / IDS rules with Metasploit framework for tuning and adjustment of rules & alerts.

Independent Penetration Tester, Phoenix, AZ
Code auditor, penetration tester, ethical hacker June 2011 – Dec 2014

- Web security pen testing including PCI compliance, greybox, whitebox and blackbox testing.
- Source code analysis in .NET, C/C++, Java, and ColdFusion.
- Malware analysis and low level software research in x86 assembly.
- Security research in evasion, malware, shellcode, and 0day prevention.

HostGator Inc, Austin, TX
System Administrator / Security Administrator Feb 2011 – Jun 2013

- Performed various administrative duties on numerous Linux and Windows servers.
- Wrote scripts in Bash and Perl to aid in the maintenance of servers.
- Performed incident response on compromised dedicated and virtual servers.
- Managed cloud based and dedicated solutions of both the Windows and Linux variety. with HyperV and SANS(ATA over Ethernet) for high performance as well as associated maintenance.
- Performed incident response and PCI compliance tuning on Windows and Linux environments.
- Wrote documentation for security protocols and change management.
- Administered McAffee EPO for malware mitigation and spam control.

Venicom Inc, Scottsdale, AZ
Software Developer Sept 2010 – Feb 2011

- Developed numerous internal applications in C#, ASP.NET, VB, and SQL Server.
- Maintained small sized network with 150 computers, 13 servers, and various switches and firewalls.
- Maintained Asterisks dialers and SIP clients.
- Aided in switch from old VBA system to .NET system for wireless sales and customer service.

FI Corp, Fountain Hills, AZ
Software Developer Sept 2008 – Sept 2010

- Developed medical application(C# .net & SQL Server) and logging facility as a product for Startup Company.
- Wrote documentation and technical writing for product.
- Assisted in support of applications