RAINMAKER
CONSULTING RESOURCES

65 Glen Rd Garner, NC 27529• (919) 805-3275 • thelukestephens@gmail.com

# Luke Stephens

## Objective

Senior security and technology talent ideally suited for offensive security work, leadership, or sales engineering role. I possess a hands-on, diverse background that enables me to be extremely capable at accomplishing any mission from hands-on delivery to customer facing roles. Whether that is doing so technically, socially, or physically it does not matter as I am highly skilled at all three. Thinking creatively like a "bad guy" is what I have been trained to do.

- Security project work including:
  - Extensive Application Security/Secure Development Life Cycle experience
  - Dozens of product security assessments covering web, mobile, traditional client-server, embedded and hybrid products.
  - Numerous traditional network vulnerability assessments
  - Worked several high-level commercial and government incident responses using Mandiant and other tools.
  - Some forensic work.
  - International physical, social and technological penetration assessments
  - F2F Social engineering assessments of organizations and organization processes
  - Secure SDLC project team consulting and augmentation
  - Secure coding audits of C, Java, Python, Javascript, ASP.Net and Lua
- Diversely skilled background that includes Special Ops, Law Enforcement, Information Technology, Social Engineering, and Privacy.
- Technology background is deep and broad including development, systems administration, and networking.
- Extensive international business and security work experience
- Business development, sales support and client management experience.
- Effective business communicator having written white papers, statements of work, contracts, and requirements documents.

## Experience

***Major Health Care Systems Provider*** **Jan 2016 - Present**

Security Architect

- Developed offensive security solutions practice that included automated scans and manual penetration assessments.
- Reviewed the Security Architecture of several EHR products
- Reviewed and interfaced with 3rd party applications which integrated with the products.
- Advised development teams on security concerns

- Conducted product and traditional penetration tests to identify security risks and vulnerabilities.
- Trained, and advised on secure software development to traditional and mobile development teams.
- Wrote white papers on emerging security concerns (DROWN, Ransomware,…)

***Tek Security Group*** **November 2010 – Jan 2016**

Security Evangelist/Chief Bad Guy

- Advised and assisted clients in all forms of offensive security needs.
- Conducted traditional network vulnerability assessments using Nessus, OpenVas, NexPose and other tools.
- Conducted product and traditional penetration tests to identify security risks and vulnerabilities.
- Provided mobile security consulting to clients.
- Trained, and advised on secure software development to traditional and mobile development teams.
- Developed privacy solutions for clientele
- Active advisor to several start-ups on security and privacy concerns
- Advised and delivered security consulting internationally (China, Jordan, Israel, Canada)

***N2Net Security/Tangible Security*** **September 2013 – September 2014**

Director of Application Security

- Conducted product security testing for clients on diverse application, mobile, hardware, embedded and network based systems
- Lead mobile, web and embedded assessor for team
- Led product assessment team
- Provided social engineering penetration assistance to infrastructure team
- Provided sales engineering support and customer liaison

## Other Work History

- **Director, Intelligence Solutions & Delivery** • Sep 2011 • Feb 2013 – *Saffron Technologies*
- **Architect/Director of Secure Mobile Development** • Jun 2011 • Sep 2011 – *SmartOnline*
- **Director, Federal Division** • Dec 2010 • Mar 2011 – *FedTech Services*
- **Cyber Security Program Manager** • Oct 2009 •Oct 2010 – *ARA*
- **Intelligence Architect** • Sep 2008 •Oct 2009 – *Knowledge Vector LLC*
- **Network Testing Tools Engineer** • Sep 2007 •Sep 2008 – *Spirent Comm Ltd.*
- **Application Security Engineer** • Jul 2006 •Sept 2007 - *IBM*
- **Senior Security Developer** • Sept 2005 •Jun 2006 – *Red Hat*
- **Senior eDiscovery Consultant** • Jan 2003 •Sept 2005 – *GSK*
- **Application Security Engineer** • Nov 2001•Jan 2003 – *CSX WT*
- **Security Practice Mgr** • Oct 1999 •Oct 2001 – *Montage*
- **Application/System Development** • May 1991 • Oct 1999 – Various
- **Raleigh Police Officer**
- **US Army Special Forces A-team NCO**

## Education

RAINMAKER
CONSULTING RESOURCES

**NC State University** **1987 - 1991**

Bachelor of Science
Computer Engineering

## Certifications

**CompTia** **August 2015**

*Security+*

**EC-Council** **October 2003**

*Certified Ethical Hacker (CEH)*

**ISC²** **February 2003**

*Certified System Security Professional (CISSP)*
*(Administratively Lapsed)*

**Cisco Systems** **January 2003**

*Cisco Certified Network Associate (CCNA)*

## Technical Competencies

***Security Engineering:***

- Physical Assessments – Penetration and exploitation, security architecture
- Technical Assessments – Network, web, application & OS vulnerability, penetration and exploitation
- Secure Application Architecture/Development – Code/architecture security review and assistance.

*Tools/Skills Include:*

Kali, Kali-NH, Metasploit, Burp, ZapProxy, Wireshark, Cmd line tools (netcat, nmap, etc), SNORT, Fortify, Hopper, aircrack-ng, kismet, Peach, WSFuzzer, w3af, BackBox, Reaver, Google hacking, Nessus, OpenVas, Scapy, Cain&Able, Rubber Ducky…

***Social Engineering:***

- Human/Organization Penetration Assessments – Independent or part of an overall assessment
- Social Engineering Hardening – Social media, corporate environments, organizational
- Social Engineering Training – Sales force multiplier, custom hardening training, covert interrogation

*Tools/Skills Include:*

Body language, Con-estry, Hypnosis, NLP, Cold Reading, SET, BeEF…

***Privacy Engineering:***

- Custom Privacy Consulting – Specialized individual, organizational, or situational privacy consulting…encryption solutions, physical privacy, social media remediation, financial solutions…
- Mobile Privacy Hardening – partial to full private mobile solutions

*Tools/Skills Include:*

GPG, Tails, Tor, Firefox, Perfect Forward Secrecy, Cryptocat, RMAs, BitCoin, Proxy services, VPNs, SilentCircle…

RAINMAKER
CONSULTING RESOURCES

***Web, Mobile or N-tier Development:***

- Web Application Development
- N-tier Application Development
- Mobile (Android/IOS) Application Development

*Tools/Skills Include:*

Java, C#, Python, C/C++, Web (HTML5, Javascript, CSS, XML, XSL), Kivy, Groovy, Regex, SQL,Eclipse, Intellij, Netbeans, Visual Studio, Grails, JBoss, Websphere, J2EE, Spring, Spring Security, Subversion, Perforce, CVS, MySQL, Oracle, SQLServer, Postgres**,** Android ADK, IOS , Java, Objective C,LinkedIn API, Facebook API, Google Search API…

***Additional IT Skills:***

Unix/Linux (debian and rhel), Windows (XP, 7, & 8), Mac OSX, Cisco IOS (Basic Routing, Switching, Firewalls), Data wiring & punch down, Telecom wiring & punch down, VMWare, VirtualBox

***Miscellaneous Skills:***

Agile Teaming, Project Management, lock picking, martial arts/self-defense, combat/tactical shooting (rifle, shotgun, pistol)

## Published Works and Presentations

**CarolinaCon** **2014/2017**

*Social Engineering for the Introvert/Geek*
*Beyond Phishing and Whaling*

**Secret DoD Proposal** **2014**

*Obfuscation Intrusion Prevention*

**Secret DoD Proposal** **2010**

*Convert Communications Infrastructure*

**Secret DoD Proposal** **2009**

*Asymmetrical Threats in a Non-Metropolitan Locale*

## GIT

*Tek Security Group:*
https://github.com/Tek-Security-Group

*Personal:*
https://github.com/tektengu

*Blog*
http://badguyfu.net

## Organization

*Board Member Local OWASP Chapter (2014-2017)*

## Miscellaneous

TS/SCI