Jon Schipp

(812) 309-1989 • jonschipp@gmail.com • Champaign, IL

Primary Experience

- **National Center for Supercomputing Applications** **Urbana, IL**
  Security Engineer, CyberSecurity Directorate *July 2013 – Present*
  - Team is responsible for defending one of the world's fastest supercomputers, Blue Waters
  - Implement and configure security controls and solutions in a security conscious R&D environment
  - Administration of two large Bro clusters, Collective Intelligence Framework integration.
  - Development operations using ESX, Puppet, Ansible, Vagrant, and Git
  - Instituted a multi-tier logging infrastructure (relays, analyzers, and collectors) for thousands of nodes.
  - Large Nagios deployment with Thruk, MySQL, IRC interaction, NRPE proxies, and custom plug-ins
  - Red Hat and CentOS Linux server administration
  - Intrusion detection, network flow analysis, and incident response
- **Touch of Class, Parke-Bell LTD, Inc.** **Huntingburg, IN**
  Unix System Administrator and Security Specialist *June 2011 – July 2013*
  - Manage and configure computer networks and computer network systems for four locations
  - Design, implement, and automate solutions to increase business productivity
  - Maintain telephony software and hardware for a call center utilizing VoIP technologies
  - Monitor networks for problems, intrusions, incidents, and other anomalous activities
  - Coordinate the storage of events and logs, and ensure the integrity of system records
  - Pursue compliance with PCI's Data Security Standard and follow common industry practices in an effort to protect company assets
  - Perform and review vulnerability assessments and internal penetration tests
  - Policy writing and technical documentation of modifications, configurations, and tasks

Secondary Experience

- **Draconyx, LLC.** **Evansville, IN**
  Director of Security *July 2015 – Present*
  - Full service IT company specializing in providing secure solutions
- **Touch of Class, Parke-Bell LTD, Inc.** **Huntingburg, IN**
  Consultant *August 2013 – May 2014*
  - Train staff in network security monitoring practices and tools
  - Git training and orchestration, Github.com workflow for project management
  - Administer a SecurityOnion machine monitoring 7 links, write Snort rules and Bro scripts
  - Nagios, Multi-Router Traffic Grapher, and NFSen deployment for network monitoring
  - Network administration, OSX and Linux server support
- **Syncurity Networks, LLC.** **Rochester, NY**
  Contractor *December 2013 – April 2014*
  - Nagios and Munin deployment for a large number of network security monitoring sensors
- **Kitchen Jewels, LLC.** **Jasper, IN**
  Consultant *April 2014 – Present*
  - VMware ESX, KVM, Nagios, Syslog, security controls, LastPass and backup solutions
  - SecurityOnion and managed network security monitoring
- **Critical Stack, LLC.** **Cincinnatti, OH**
  Contractor *September 2014 – Present*
- **Nexus Engineering, LLC.** **Evansville, IN**
  Contractor *January 2015 – Present*
  - Log analysis and active response with OSSEC and Sagan

Education

- **ITT Technical Institute** — **Newburgh, IN**
  Computer Network Systems and Information Security, B.S. Applied Science — *Sept 2007 – June 2011*

Selected Additional Training & Education

- Over 1000 hours of specialized information security and technology based workshops and conferences
- Attended the HFC Metasploit Framework workshop in Cincinnati and Louisville
- iOS Development Course, *Vincinnes University*
- CourseEra - Learn to Program: The Fundametals (Python), *University of Toronto*
- National Science Foundation's 2013 Bro Workshop
- International Supercomputing Conference's Ensuring Network Performance with perfSONAR tutorial
- Information Systems Security Association's Password Exploitation Workshop, *Louisville*
- SecurityTube.net's Wireless LAN Security and Penetration Testing Megaprimer

Certifications

- COMPTIA A+
- COMPTIA Network+
- COMPTIA Linux+
- COMPTIA Security+
- Wireshark Certified Network Analyst (WCNA)
- GIAC Certified Intrusion Analyst (GCIA)
- GIAC Reverse Engineering Malware (GREM)
- Linux Professional Institute Certification Level-1 (LPIC-1)
- Berkeley Software Distribution Associate (BSD-A)
- ARRL Technician Class License

Projects

- **The More You Bro** — **ICSI, NCSA**
  Video series for the Bro Network Security Platform — *2014*
- **ISLET: Isolated, Scalable, & Lightweight Environment for Training** — **NCSA**
  A Linux-based software training platform built around Docker — *2014*
- **Virtual Machine Infrastructure** — **UIUC GLUG and OpenNSM**
  Build Linux and NSM virtual machines with Xen Project hosts and KVM based Ganeti cluster — *2014*
- **Open Network Security Monitoring Group (OpenNSM)** — **ACM**
  Organized and led a weekly network security monitoring discussion forum with international participation — *2014*

Television Appearances

- **ITT Technical Institute** — **Louisville, KY**
  International Commercial — *ITT, La Fabrica Films, MGSCOMM*
  Film date - *February 2014* — Air date - *March 2014*

Selected Presentations

- 2014 "ISLET: Improving Linux-based Software Training" *Information Trust Institute, University of Illinois*
- 2013 "Intrusion Detection and Network Analysis" *ITT-Tech, Newburgh, IN*
- 2013 "The Netsniff-NG Toolkit" *Derbycon*
- 2013 "A Look at the Netsniff-NG Toolkit" *Midwest Open Source Software Conference, University of Louisville*
- 2013 "Hacker Hotshots" Interviewed by *ConsciseCourses.com*
- 2012 "A PCAP Workshop" *Hack3rcon 3*
- 2012 "An Introduction to Traffic Analysis" *AIDE Conference, Marshall University*
- 2011 "FOSS for Unix Administrators" *Vincennes University*
- 2011 "Implementing a Network Monitoring System" *Hack3rcon 2*

Publications

- 2015 Schipp, J., Dopheide, J., and Slagell, A., "ISLET: An Isolated, Scalable & Lightweight Environment for Training", *in the proceedings of XSEDE*, St. Louis, MO, Jul., 15.
- 2015 "Linux Containers for Event Training" *2600: The Hacker Quarterly, Volume 32.1*
- 2014 "Intelligence Data and Bro" *Bro Blog, bro.org*

Honors & Awards

- 2015 NCSA - HIGH5 for ISLET Award
- 2015 NCSA - Technical Excellence Award
- 2011 Touch of Class - Employee of the Month
- 2010 Hack3rcon - Capture the Flag winner – Black Badge recipient
- 2009 ITT Tech - Academic Honors
- 2007 ITT Tech - Academic Honors

Community Contributions

- Founder – Open Network Security Monitoring Group – *NSM discussion group*
- Founder – Dubois County Linux User Group – *Operating system discussion group*
- Founder – Southern Indiana Computer Klub – *Security research group*
- Contributor – Bro *the Bro network security monitor*
- Contributor – Netsniff-NG Toolkit *Suite of high performance networking tools*
- Contributor – SecurityOnion *The NSM Linux Distribution*
- Implementor – Free downtown Wifi, *City of Huntingburg*
- Author – HC3 presentation material used at Princess Sumaya University for Technology (PSUT)
- Author – 50+ online articles covering network security monitoring and system administration
- Author – mal-dnssearch, a malware host detection and prevention script that handles multiple logs
- Author – Many other useful system admin scripts such as pps, gencfg, and malcachesnoop
- Member – USENIX, ACM, REN-ISAC, ISSA Kentuckiana, Infragard, and Appalachian Institute of Digital Evidence

Skills

- Working knowledge of FreeBSD, OpenBSD, OSX, AIX, GNU/Linux (Fedora & Debian families), Windows
- Understanding and experience with firewall and packet filtering software such as iptables, PF, IPFW, OSX ALF, Sonicwall, Windows Advanced Firewall, Windows 2000 IP Security Policies
- Detailed knowledge of the TCP/IPv4 packet structure and network traffic
- Experienced in network and host based intrusion detection systems including signature and behavioral based detection engines such as Snort, Suricata, Bro, OSSEC, and Sonicwall
- Proficient with packet capture and network traffic analysis tools like Tcpdump, Wireshark, Bro, Snort, ARGUS, iftop, Ntop, passivedns, httpry, arpwatch, TCPick, TCPFlow, Netsniff-ng etc.
- Experience in the automation of administrative tasks on unix-like systems with Bash and Korn shell programming. Some additional experience with Git, Awk, Python, C, LaTeX, Tcl/Expect, Make, HTML, and reStructuredText. Very comfortable with command-line interfaces.
- Working knowledge of Metasploit, Nessus, Nmap, hping3, John the Ripper, Hashcat, Aircrack-ng and other popular open source security testing software and utilities

See http://jonschipp.com for further information and for verification of all claims made above (includes sources and references)
See http://github.com/jonschipp for code and open source contributions