

Jonathan D. Schipp

2503 W. Springfield Ave. Apt. A-11 • Champaign, IL 61821
(812) 309-1989 • jonschipp@gmail.com

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.
 - Provisioning systems using Puppet, Ansible, Vagrant, and Git
 - Virtual Machine building and administration with VMware ESX and VCenter
 - 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
 - **Mitchell International** **Evansville, IN**
Technical Support Specialist *March 2011 – June 2011*
 - Aid customers in resolving software issues by phone and with remote assistance
 - Troubleshoot and configure different software in various network environments
 - Document dialogues, procedures, and solutions with and for the customer
-

Secondary Experience

- **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 – Present*
 - Nagios and Munin deployment for a large number of network security monitoring sensors
 - **Kitchen Jewels, LLC.** **Jasper, IN**
Consultant *April 2014 – Present*
 - Network, server, and workstation installation
 - VMware ESX, Nagios, Syslog, security controls, LastPass and backup solutions
 - **Critical Stack, LLC.** **Cincinnati, OH**
Consultant *September 2014 – Present*
-

Projects

- | | |
|--|------------|
| • The More You Bro | ICSI, NCSA |
| <i>Video series for the Bro Network Security Monitor</i> | 2014 |
| • Bro Live: Sandbox Environment | ICSI, NCSA |
| <i>Design system that issues isolated environments (LXC) to improve conference training events</i> | 2014 |
| • ISLET: Isolated, Scalable, & Lightweight Environment for Training | NCSA |
| <i>A Linux-based software training platform built around Docker</i> | 2014 |
-

Education

- | | |
|--|--------------|
| • ITT Technical Institute | Newburgh, IN |
| <i>Computer Network Systems and Information Security, B.S. Applied Science</i> | 2007 – 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, Vincennes University
 - CourseEra - Learn to Program: The Fundamentals (Python), University of Toronto
 - National Science Foundation's 2013 Bro Workshop
 - International Supercomputing Conference's Ensuring Network Performance with perfSONAR tutorial
 - 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)
-

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, ARGUS, iftop, Ntop, passivedns, httprry, arpwatrch, 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, Bro, C, L^AT_EX, Tcl/Expect, 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

Television Appearances

- **ITT Technical Institute**
Nationwide Commercial
Film date - February 2014

Louisville, KY
ITT, La Fabrica Films, MGSCOMM
Air date - March 2014

Selected Presentations

- 2014 "Vagrant Environments" *Association for Computing Machinery Linux User Group, 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

- 2014 "Intelligence Data and Bro" *Bro Blog, bro.org*
-

Honors & Awards

- 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 – 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 – ISLET (Isolated, Scalable, and Lightweight Environment for Training)
- 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