

Jon Schipp

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

Primary Experience

- **National Center for Supercomputing Applications**

Security Engineer, CyberSecurity Directorate

Urbana, IL

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 and Cuckoo 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 Thrak, 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.**

Unix System Administrator and Security Specialist

Huntingburg, IN

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

- **Touch of Class, Parke-Bell LTD, Inc.**

Consultant

Huntingburg, IN

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.**

Contractor

Rochester, NY

December 2013 – April 2014

- Nagios and Munin deployment for a large number of network security monitoring sensors

- **Kitchen Jewels, LLC.**

Consultant

Jasper, IN

April 2014 – Present

- Network, server, and workstation installation
- VMware ESX, KVM, Nagios, Syslog, security controls, LastPass and backup solutions
- SecurityOnion and managed network security monitoring

- **Critical Stack, LLC.**

Contractor

Cincinnati, OH

September 2014 – Present

- **Nexus Engineering, LLC.**

Contractor

Evansville, IN

January 2015 – Present

- Log analysis and active response with OSSEC and Sagan
-

Education

- **ITT Technical Institute**
Computer Network Systems and Information Security, B.S. Applied Science

Newburgh, IN
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
 - 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)
-

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**
International Commercial
Film date - February 2014

Louisville, KY
ITT, La Fabrica Films, MGSCOMM
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 – 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, ARGUS, iftop, Ntop, passivedns, httptry, arpwatsh, 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, Make, HTML, and reStructured-Text. 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