David Shaw

dshaw.jobs@gmail.com

Experience

Redspin, Inc. Carpinteria, CA
Lead Security Engineer *Aug. 2009 – Present*

- Performed external and web application penetration tests for use in PCI, HIPAA and NERC compliance. Created reports detailing issue, impact and recommendation for each finding. Assisted clients with finding mitigation, working with a variety of complex systems.
- Worked on various research and development projects including a zero-day vulnerability scanner, a data stealing USB "drop" key, various internal shell and Ruby scripts
- Performed social engineering assessments including e-mail and telephone scripts to snatch domain credentials.

Secure Science Corporation San Diego, CA
Security Researcher *May – Sep. 2007*

- Worked as part of the External Threat Assessment Team, interacting with clients and ISP's as part of anti-phishing efforts. I created a perl script to join phishing group IRC channels (gleaned from malicious C99 installs) to monitor for URLs, effectively pre-empting duplicate attacks.
- Assisted in malware analysis

Softwink, Inc. Global Network Security (Remote Work) Boone, NC
Network Security Analyst *May – Sep. 2006*

- Analyzed live Snort log outputs from perimeter IDS boxes on large banks and law firms across the Eastern seaboard. Interacted with clients when alerts warranted immediate attention, as well as through monthly status reports.
- Worked with a minimal existing codebase to better categorize incoming alerts through our Snort PHP front end.

University of California, San Diego La Jolla, CA
Database Engineer *May – Sep. 2005*

- Interned with the Computer Vision department, managing a MySQL database of contacts throughout the department.

San Diego Supercomputer Center at UCSD La Jolla, CA
Programming Intern *June – Sep. 2004*

- Interned with a programming team working on integrating SDSC GIS servers into the OpenCroquet 3D operating system using Squeak/Smalltalk. Implemented netcode for relaying data from GIS servers to the 3D environment.

Skills

Security: Extensive experience performing penetration tests of large corporate networks using nmap, Nessus, Burp Suite, firewalk, sip-vicious, nikto, as well as experience manually testing for Cross-Site Scripting, SQL injection and otherwise unsanitized input.

OS: Extensive experience using and administrating *nix environments including FreeBSD, Gentoo, Arch Linux, Debian and Red Hat.

Languages: Ruby, Lua, NSE (Nmap Scripting Engine), bash

Projects: Source code for my various open source projects (including the TeX source for this document) is available at http://github.com/davidshaw