Ian Macdonald

P.O. Box 1431

Herndon VA 20172

Email web@jobs.imacdonald.co.uk
Telephone 703 574 7080

Introduction

My name is Ian Macdonald. I have a Bsc(honours) in Computer Science from the University of Edinburgh in Scotland. I have been in the US since graduating and I am a Green Card holder. I have been working in IT field all my working life, specializing in computer security for the last 10. I have extensive experience in designing and implementing complex IT Systems. I have rebuilt multiple Intrusion Detection Systems covering multiple networks, spanning multiple countries. I have deployed corporate wide virus and spyware protection solutions for 10,000 plus hosts. I have implemented multiple web filtering solutions. I have designed and deployed reporting and monitoring solutions at large fortune 500 companies. I know how to program and write complex SQL queries and I enjoyed being a manager of a team Security Engineers.

My ideal position would be as a IT Security Lead, building complex systems in a small to mid sized company, and be within a reasonable commuting distance of Herndon Virginia.

Skills & Tools

- Security Engineering and deployment, Penetration testing, Virus discovery and remediation, Vulnerability Assessments, Strong trouble shooting skills, Data modelling and Data Integration, Incident Response.
- Snort, Bindview Control, Nmap, Nessus, Tcpdump, McAfee EPO, McAfee HIPS, Cisco Firewalls, Cisco Switches, Cisco Routers, Applied Watch, Intellitactics, Ironport Web Security Appliances, WebSense Enterprise, Breach ModSecurity, Splunk, Symantec Antivirus.
- Cyrus, Postfix, Bind, Apache, Nagios, Microsoft Exchange Server, VMWare Server, MS SQL Server tuning and administration, and Mysql tuning and administration.
- Microsoft NT, Microsoft XP, Microsoft Vista, Microsoft Server 2003, Red Hat, Ubuntu, SUSE, Solaris, Apple OS X.
- TCP/IP, SMTP, HTTP, DNS, and other protocols analysis.
- C, C++, Perl, Unix shell scripting, ML, Java.

Experience

- 10 years of computer and network security experience.
- 13 years experience administrating Linux and other flavours of Unix.
- 13 years experience administrating Windows Servers.
- Over 5 years of database/data modelling and data analysis experience.

Angel.com ***Sr. Systems Administrator and Security Lead*** ***Nov 2008 to Present***

- Responsible for Production IT Security, including maintaining PCI certification.
- Joint responsibility for 24x7 uptime of Angel.com
- Architected switch from Jboss on Windows to Jboss on Linux, including creating rpm packages for Angel.com application deployment.
- Implemented single sign on for Windows, Linux, and Apache web services.
- Deployed updated IDS and Antivirus in Production Environment.
- Deployed application firewall for protecting against cross site scripting and sql injection attacks.
- Deployed internal certificate authority.
- Researched and selected outsourced vendors to conduct network and application security penetration testing.

- Completed annual renewal of PCI certification.
- Architected and deployed new log management and monitoring system.
- Maintained and expanded Nagios monitoring solution.
- Architected and deployed Linux and Windows patch management solution.
- Standardized production platform on Centos/Redhat Enterprise linux.
- Tested and Deployed VMware for QE and Production environment.
- Created Linux system configuration and deployment system using Capistrano.
- Created and continue to teach Security Awareness and PCI compliance classes.

Ajilon/The World Bank Technical Security Analyst March 2008 to October 2008

- Responsible for developing and deploying an Internet security filtering solution to protect all computers at The World Bank.
- Reviewed and performed performance tuning of the Bank's McAfee EPO and VirusScan Enterprise implementation.
- Deployed a Nagios monitoring solution for Security Servers.
- Created a logging server based on Sawmill.

AOL LLC Technical Security Engineer April 2006 to March 2008

- Updated Perl based IDS reporting tool.
- Helped develop information security training courses.
- Performed a complete rebuild of the IDS monitoring solution covering multiple countries.
- Performed security design reviews and host assessments for multiple projects
- Member of the Computer Emergency Response Program, responsible for handling and coordinating computer incidents across all of Time Warner.
- Performed malware analysis and mitigation.
- Responsible for presenting a biweekly training course to new hires on computer security awareness.
- Integrated IDS reporting into Enterprise Security Management(ESM) system

Constellation Energy Group IT Security Engineering Team Lead November 2004 to April 2006

- Managed the IT Security Engineering Group. Responsible for weekly team meetings, weekly status reports to upper management, Project Scheduling, task prioritization and workload management within the group.
- Consulted on IT Security related issues in IT projects.
- Technical lead and coordinator of incident response for virus and other security incidents.
- Presented “BindView Control’s place in a Security Organization” at the 2005 BindView Insight User Conference in Houston Texas to over a 100 people.
- Responsible for maintenance and upgrading the IDS infrastructure that monitors 15,000+ workstations and servers.
- Created IDS signatures for tracking Viruses and other Security events.
- Created team SharePoint site for tracking group tasks and engineering procedures.
- Created a web front end for displaying information generated by BindView Control.
- Coordinated testing and deployment of virus software upgrade to 12,000 machines.
- Responsible for coordinating and supporting internal IT Security systems, projects and associated budget.
- Conducted a bake off between 4 enterprise vulnerability assessment tools. Looked at quality of scan, the quality of reporting, costs and how it would fit into existing procedures and processes.

Constellation Energy Group IT Security Analyst March 2002 to November 2004

- Designed, built, and monitored a multi sensor Intrusion Detection System that covering multiple security zones and multiple subsidiaries.
- Deployed an IDS web front end that was written by myself and extended it to include virus data from our centralized virus protection solution.
- Performed network security audits.
- Performed forensic analysis of machines that were suspected of being compromised.
- Re-architected the BindView Control infrastructure to support enterprise monitoring and auditing.

- Created an automated system for emailing out security alerts and reports.
- Developed an 802.11 secure wireless solution.
- Implemented a web content monitoring and blocking solution.
- Maintained and performed analysis of syslog data supplied by firewalls and other devices.
- Deployed a centralized virus protection solution to 12,000 desktops and servers.

Strategy.com Lead Security Engineer June 2000 to November 2001

- Developed and deployed Windows NT 4.0 and Windows 2000 security hardening scripts to a production system of over 400 machines. These scripts prevented the production site from being infected by the Code Red and Nimbda viruses. The machines are a combination standalone and clustered machines.
- Developed a lab of machines based on Ghost imaging for testing the latest security patches and exploits. The lab could be used to quickly test either Windows 2000 or Windows NT based configurations and to test the latest builds of the strategy.com platform software.
- Designed a multi sensor IDS system originally based on ISS Realsecure then later revised to use Snort due to cost constraints.
- Helped obtain and keep ICSA/True Secure certification for the Strategy.com production system of over 400 machines.
- Investigated and researched suspicious network traffic both on the internal LAN and at the production site using tools like snort, sniffer basic, tcpdump, ethereal, dsniff.
- Worked as part of a team to conduct routine system security audits covering Windows NT, Windows 2000 and Unix based machines using ISS Internet Scanner, Cybercop, Retina, Nessus and SolarWinds Tools.
- Enforced company wide security policies.
- Monitored and contributed to Security Mailing lists.
- Created a monitoring and reporting system for the outgoing email machines using MRTG as the front end and a combination of SNMP and custom written Perl scripts on the backend.
- Researched and investigated 802.11 network security.

Education

Cisco
Cisco Certified Network Associate, CCNA (lapsed).

Managing IT Projects
Week long course developed by George Washington University and ESI International.

Shmoocon, Washington DC 2007, 2008, 2009, 2010
Attended three day conference on Computer Security

Institute for Applied Network Security, DC Forum 2007
Attended two-day forum and presented on the topic of Windows Mobile security vs Rim Blackberry Security.

Bindview BVcontrol training, Washington DC 2002
Attended a week long training class.

CSI Annual Security Conference, Washington DC 2001
Attended the security conference.

Black Hat Briefing, Las Vegas 2000 and 2003
Attended the security conference plus the Defcon convention that followed.

Microstrategy Technical Training
Technical boot camp,
Microstrategy Broadcaster,
Quality Engineering and testing.

Teradata
NCR Unix System Administration.

Edinburgh University, Scotland,
4 Year BSc (Hons) Computer Science, 1993-97

Other Activities and Interests

Personal Projects
My home network consists of machines running Linux, Windows XP, Solaris and OSX. I have about 2 terabytes of storage on the home file server running in Raid 5 mode with extra disks for backup and redundancy. I run a number of websites that are either hosted on my home network or on virtual private servers. I manage my own email and dns servers so I can fine tune spam filtering. I have also been experimenting with Asterisk and use it for the house phones.

SnortUI
I wrote a front end to Snort that is released under GPL and available on sourceforge.net. It displays alerts generated by a snort IDS sensor. A security operator can quickly view the alerts then drill down into the information to find all alerts for that machine.