A versatile security specialist with expertise in telecom/ISP, enterprise and linux solutions.

Neil Bortnak

Email: career@moro.us
Phone: +81 (0)90-5509-9833
Tokyo, Japan

Highlights

- 14 years experience in IT, 8 in Infosec
- Tested in top 1 percentile of technicians
- Discovered and published vulnerability
- Able to write own exploits and tools
- Expert in audits, pen tests and defense
- Lecturer at Conferences and Universities
- Face of Infosec for national Canadian news
- Extensive consulting experience
- Has run several businesses
- Expert in Linux (primary security platform)

Technical Skills (abridged)

Area	
Security	Penetration Testing Security Assessment VPNs Firewall Host Security
Programming Languages	Perl PHP Python C/C++ 68K & x86 Assembly
Networking	TCP/IP DNS SMTP (Postfix) HTTP (Apache) LDAP

Area	
Security (Cont.)	IDS Forensics Policy & Procedure B1 Systems PKI
Programming Techniques	Secure Programming Network Programming System Programming Kernel Programming Scripting
Linux Distributions	RedHat SuSE Mandrake Gentoo Debian

Personal Skills

Leadership	Team Player
Advanced communication skills	Reliable self-starter
Absorbs new technical skills quickly	Excellent under stress
Highly creative	Ability to make fast and correct judgments
Business understanding	Exper. at engineer, managerial and executive levels

Certifications and Memberships (Former and Current)

CNE	Computer Security Institute
MCSE	American Society for Industrial Security
Virtual Vault (B1 version of HP/UX)	Terminal City Business Club

Current Research and Projects

mlc	Research	Very high compression system for natural language text with translation capabilities
ecra	Research	New archive format with encryption, compression and data redundancy built in
mkchroot	Project	Utility for automatically building and maintaining chroot environments
secure_root	Project	4MB linux system for booting fully encrypted laptops with strong authentication
winmd5	Project	Integrates into right-click menu to provide md5 checksums under windows
tastybackup	Project	Multi-platform wrapper script for rsync

Recent Work History

2003-Present: Cisco Systems KK (Japan) via PasonaTech KK

World's leading maker of routers and switches for the enterprise environment. Cisco also focuses on advanced services such as Security, Video on Demand and Voice over IP.

Position: Consulting Engineer, Technical Lead for Asia Pacific

Soon after joining Cisco, became one of the top technicians in the AsiaPac theatre, working in a cross functional role on numerous projects. In the spring of 2004, was selected to help lead the global linux desktop initiative. Appointed to two global security teams in spring 2005; the DCSS Security and WINES Security teams.

Highlights:

Security Audits: Performed numerous security audits as part of the Shadow IT initiative, resulting in the identification of numerous security vulnerabilities. Worked with vendors and ASPs to correct the issues in their systems, educating them in the exploitation and defense of techniques such as SQL Injection. Outside of Shadow IT, discovered serious flaws in a sensitive ASP system, and trained InfoSec staff in the proper use of security analysis tools. Currently using IDS technology to track down and eliminate systems attempting inappropriate access to the data center.

Virus Analysis/Repair: The standard boot disk used to create new desktops began failing on a global basis and was asked to look into the problem. Identified the exact sequence of packets that caused the problem and the virus that originated them. Prepared a temporary solution by creating a Linux based floppy disk containing a bridging firewall which could be used on any system in the company without affecting the hard disk. The disk allowed support staff to make new desktops again. Also developed a long term solution which not only solved the problem permanently, but also identified and closed a potential security vulnerability.

Filer Migration Project: Instrumental in the migration of 4 file servers into one large 8TB Network Appliance Filer. Migration was complicated by requirements to change the directory structures to accommodate a new global standard. Wrote a perl script to migrate and synchronize data from the old systems to the new filer, changing the directory structures as they were copied. The script was also responsible for setting security, making groups and populating those groups in a Windows security environment.

Unix consolidation Project: Led a project to eliminate redundant and abandoned Unix systems in IT Japan. Over the course of six months reduced the number of Unix systems from 13 to 2, thereby saving the company significant expenditures in licensing, upgrades, maintenance contracts and labour.

1999-2003: Artaxata Data Security

High tech consulting company providing data security and linux services to organizations across Canada.

Position: President/Senior Consultant

Provided security and linux consulting services to a variety of organizations including those in the telecommunications industry. Spoke at conferences, taught at university and made numerous television, radio and print appearances. Ran all aspects of the business including accounting, legal and marketing.

Highlights:

Telecom/ISP Audits: Performed security/infrastructure audits for GT Group Telecom and NorthwesTel. GT is a national telco/ISP with a large and complex network spanning 5 major cities and 72 smaller ones. NorthwesTel is a similar company serving northern Canada. Single handedly built a system to automate discovery of networks/nodes, scan them with Nessus, eliminate false positives, generate reports with replacement wordings and provide a web based tracking tool. Built project with perl, C, Nessus, Postgres, Apache, and TeX.

Enterprise level mail cluster: Designed highly scalable, LDAP based mail cluster built on Postfix, Cyrus IMAP, Apache, Horde/IMP, BIND, Postgres, Amavis, SpamAssassin, ISPMan, LinuxHA and Linux Virtual Server. Mail could be accessed via POP3, IMAP or Web Interface and incoming mail was subject to spam controls, virus scanning and SMTP authentication. All connections, both incoming and outgoing were encrypted via TLS/SSL. As part of a cost cutting measure, the final implementation was cluster-ready, where all of the components were on one system but could easily be broken out into a full cluster when needed.

Guest expert for media, conferences and university: A regular guest for computer security on regional and national television, print, radio and web for a period of 2 years. Interviewed for news broadcasts, talk shows, documentaries, newspaper/web articles. Wrote articles and papers in support of broadcast work. Spoke at numerous conferences including the Computer Security Institute and Comdex Canada West. Lecturer for University of British Columbia regarding encryption technologies.

Published vulnerability: Researched and discovered vulnerability in McAfee Virus Scan and some versions of Norton Anti-Virus. Well known viruses and trojans could be run undetected in the recycle bin. Published to Bugtraq and NTBugtraq with proof of concept exploit code.

1996-1999: DTM Systems Corporation

Value added reseller and consulting firm specializing in security, clustering, storage and other enterprise technologies.

Position: Chief Security Consultant (1998-1999)

Develop and drive creation of internal security practice. Provide advisory and implementation expertise to clients such as Ballard Power Systems (fuel cell research), BC Hydro (6000+ user utility), and Canaccord Capital (securities brokerage). Work with marketing to promote security awareness and services to internal sales and customers. Represent DTM by speaking at conferences and by educating at client sites and public events.

Position: Systems Engineer (1996-1998)

Consulting, on-site troubleshooting, and preparing servers and workstations for clients. Worked mainly with Hewlett Packard hardware, Netware 2.12 - 4.11, Windows NT 3.51 - 4.0, HP/UX and Linux. Other duties included pre-sales support, security consulting and in-house maintenance. A CNE and MCSE was maintained while at DTM.

Highlights:

Secure Internet Solutions Group (SISG): Led the development of the SISG within the Professional Services division. Defined strategic directions, product development and marketing focus. Trained company staff in basic Internet security and represented the SISG to customers in conjunction with the sales force.

Network Design: Designed an extremely fault-tolerant network to connect a large server to the rest of the client's corporate systems. Design incorporated a pair of dual attached FDDI rings connecting the two halves of this mirrored server and two redundant switches. To increase fault-tolerance on their existing network several redundant links and additional data paths using spanning-tree and sub-networks were added. The final design provided a very high level of fault tolerance and lowered server to server traffic on the main network.

1994-1996: ProTechnical Insurance

Insurance brokerage/company hybrid specializing in commercial insurance.

Position: Network Administrator/Automation Programmer

Responsible for the day-to-day operations of company network and major upgrades. Improve and maintain code for the office automation system. Train staff to use office systems. No other technical employees were employed.

Highlights:

Office Automation System: Single handedly built an automation system tying together all major company systems. Time required to issue policies fell from 20 minutes to 45 seconds. Production code base stabilized at 3.5MB and was used for virtually all office operations, producing dramatic increases in efficiency across the board.

Network Upgrade: Performed extensive upgrade of all corporate systems. 386 clone workstations were replaced with Dell pentiums, 486 clone server replaced with HP Netserver and 10BaseT network upgraded to 100BaseVG. Wrote a number of C utilities to automate common user tasks and protect boot process against tampering. Client OS (Windows 3.11) and applications centralized on server, enabling most clients to boot from a floppy disk. Also wrote an automated workstation upgrade system, obviating the need for additional technical staff.

Security Enhancement: Vendor application required that all users of their application have supervisor (root) access to the entire server. Managed to quarantine application into one section of the Netware server so that users could utilize normal accounts and have access controls applied to them.

Connectivity: Remote access to the network was provided for authorized users along with LAN-Internet connectivity using a dial-up router. A UUCP gateway and e-mail were provided for use with the new workstations to facilitate infra-office and Internet communication

References available upon request