

Ronald DuFresne

148 Lin Tilley Road, Durham, NC, 27712

(919) 477-4151

ron@sysinfo.com

dufresne@sysinfo.com

<http://sysinfo.com>

SUMMARY:

An experienced network and systems security administrator with a broad background in distributed systems. UNIX certified (all flavors) and has a good knowledge of TCP/IP, NT, Novell, LAN/WAN, Ethernet, Netbios, routers (Cisco/Wellfleet), switches, and gateways. Expertise with configurations, implementations, troubleshooting, hardware and software upgrades, administration, system support, firewalls, and user training. Supported clients across multiple industries including high-tech manufacturing, systems integrators, local and state government, distance learning, US military, small business, and others.

TECHNICAL SKILLS:

Hardware:

Cray	Data General	SSPS-X	LAN/WAN
RS6000	IBM PCs and compatibles	mini/mainframe	Xylogics term servers
HP9000	Macintosh	connections	Hubs
HP3000	Network cards, modems,	Cabling	Bridges
Sun	hard and floppy drives	Internet/Intranet	routers (Cisco,
Apollo		Ethernet	Wellfleet)

Software:

UNIX platforms: AIX,	FTP	HTML	Netcat
HP-UX, Solaris, IRIX,	SQL	ssh/scp <ver 1 & 2>	Nmap
SCO, Apollo, SGI,	telnet	TIS firewall tool kit <fwtk>	Ngrep
Data General, Linux,	rlogin	lpfwadm to iptables	Pong
Unicos/mk	Netbios	tcplogger	freeswan-1.00
NIS, NIS+	Linux/fwtk firewall	ipmon	mason-0.13.0
Novell Netware	SMTP	cheops	tripwire
MS Win 3.x/98/NT	QuickMail	hping	vpnd-1.0.6
NT Domain	OS/2	icmpinfo	cops
MS Office Suite	LegalEase	TCPwrappers	Netscape Enterprise Server
DOS 3.1-6.22	sh/bash	lpl	Apache
FoxPro	Perl, Awk, Sed scripts	TCPdump	SSL/TLS
lotus123	Paradox	Kerberos	Sslwrap
TCP/IP	Norton Desktop	FW-1	Sslproxy
IPX/SP	Remote Access	SecureID	ssleahy/OPENSSL

EXPERIENCE:

State of North Carolina ITS, Systems Programmer (December 2002 to Date)

- Systems admin on SUN, AIX and Linux systems; systems installs, patching, systems security, user maintenance, web and log analysis admin for iPlanet<SUN ONE>, apache, and Webtrends. Was key in laying out the design and architectural layout of the enhanced web hosting the state provides agencies under Linux/apache on the s390 IBM platform. Sunpass sa-299 sa-399 sa-200-S10 and sa-202-S10 course completion.
- **ITIL** foundation certified 2007
- Disaster recovery specialist in the unix group.
- Vulnerability mediation for unix and various clients.
- Though not representing the state, I also presented my papers on wireless security at ToorCon in the fall of 2003.

Independent Contractor

August 1985 to 2001

Recent Projects:

(May 2001 to December 2002)

- Researching of HIPAA regulations and how they apply to systems/network security.
- Pre-publishing review of a B2B manuscript for Horizon House publications Inc <artechhouse.com>.
- Wrote and published papers on how issues have remained the same since the Morris worm in the later 1980's to the recent code red and nimda virus that struck more recently. The second paper completed is an analysis of placement of IDS systems. Issues covered included looking at not only incoming traffic, but also out-going traffic to watch for signs of compromise and virus/trojan activity; and users not complying with corporate security policies and practices. Both papers are now available online at: <http://sysinfo.com/iworms.html> and <http://sysinfo.com/eds.html>. The first paper has

been cited in Frederick M Avolio's monthly security newsletter in the February edition at <http://www.avolio.com/columns/16-Nothing-has-Changed.html> and has been used by Alan Clegg for various other security symposiums including BSDcom2002. Mr. Avolio has cited the second paper in his Netsec monthly at: <http://www.avolio.com/columns/18-Network-VATs-for-Verification.html>. My paper on wireless security issues, <http://sysinfo.com/wire1.html>, will be delivered to the Computer Security & Intelligence Conference this August in Calgary, Alberta Ca. We have an additional paper recently published in the TISC Insight newsletter, <http://www.tisc2002.com/insight.html>, Volume 4 Issue 8, May10 2002, the state of systems security.

- Set up a firewall/VPN e-mail gateway system with a client in Atlanta on openbsd and Linux,
- For a client in Norway <bremspor.net> provided network analysis and consulted on upgrade of Linux slackware 8.0 system running ipchains and tcpwrappers.
- Setup a new server for sysinfo.com on a Sparc10 running openbsd, updated a number of ssl apache web servers as new apache and mod-ssl sources have come out.

Nortel Networks, Systems Security Auditor/Admin (November 2000 to May 2001)

- Lead technical admin, Defining and implementing systems security on and for internal and exposed Unix systems (SUN/Solaris, HP, AIX).
- System audits (ISS, sealer, proprietary tools), access rights, networked services, implemented the introduction of ssh into the Nortel infrastructure to replace telnet, ftp and rsh. Developed and improved the systematic auditing of system configuration settings to promote a standardized secure environment.
- Mentored co-workers in security and networking fundamentals. Advised various departments in the secure transmission of data in and out of the Nortel network, etc.

AT&T Solutions, Systems Security Analyst (May 2000 to November 2000)

- Maintenance of client perimeter devices, screen and choke routers (Cisco, various sizes and IOS version), Nortel Contivity switches, FW-1 (on Solaris 2.5.1, remotely managed over NT workstations) rules and server stability.
- Mentored co-workers in the fundamentals of network protocols and their significant issues in security.
- Helped various organizations develop various VPN PPTP2, L2TP> tunnels to promote their work with their corporate partners, and other internal and external customers

Lockheed Martin/EPA, Systems Installation and Documentation Specialist (January 2000 – April 2000)

- Composed configuration documents for various flavors of UNIX and windows OS'. This included a standardized set of procedures of services to install and configure across the various platforms to aid in interoperability in the EPA's new security policies and procedures
- Troubleshoot C2 installation and security issues for on and offsite clients.
- Departments lead technical admin mentoring co-workers.

Lake Region Manufacturing, Systems Admin and Security Specialist (five months, 1999)

- SCO 5.0.5 administration on a Compaq proliant 8000 box, network administration, security auditing nmap, probe, nexxus), porting and maintenance of a proprietary application to this machine
- Tailored and defined the internal security polices, documentation, and staff training

Webwinks Inc., Instructor (three months, 1999)

- HTML and basic networking instruction.

TekMetrics Inc., Security Analyst (three months, 1999)

- Evaluated and assessed their Systems Security Administrator testing module.

Network Computing Services, Systems Programmer (nine months, 1999)

- Worked in a predominantly Cray/UnicosMK environment (Cray2, T3E 900, T3E 1200, Y-MPEL, Y-MP81, J90, etc.).
- The University of Minnesota and the US military used CRAY T3E's. This required a higher-level security clearance and work in conjunction with military security auditors to maintain proper security policies.
- Primary responsibilities included maintaining the IRIX Origin 2000 system running IRIX 6.4 on 12 processors with 8gigs of memory and a few terabytes of disk capacity local, and mounted. FW-1 on NT, swatch, nmap, nessus, tcpdump, etc.

Cargill, Systems Specialist (three months, 1998)

- Set up an HP9000 HP-UX EDI document exchange system for an external client, Direct Connect.

United Health Care, Systems Admin (five months, 1998)

- Upgraded a new AIX server from 4.1.4 to 4.1.5. Moved users and SQL databases to new server.
- Maintained and managed approximately 10 servers in testing and production.

Platinum Technology, Systems Technical Specialist (five months, 1997)

- Provided QA testing of pre beta corporate Web management software.

- Researched competitive products requiring extensive traveling and documentation.

K-9 Webs Inc/Pelham Saddlery, Instructor (three months, 1997)

- HTML, web administration training.

Goretek Data Systems, Systems Engineer (three months, 1996)

- Provided general systems administration in a DG/UX-Novell TCP/IP environment. Maintained HP, AIX, SCO, and Data General servers, Xylogics term servers, hubs, and bridges.
- Maintained a Linux/fwtk firewall to the Internet.
- Supported 32 servers for in-house software development.

Alliant Tech Systems, Systems Support Specialist (six months, 1995)

- Provided remote information/communications support for PC, MAC, assorted UNIX platforms (Apollo, Sun, HP, SGI), Novell, WFW3.11, Ethernet, and Tele/data-communications. Used Remedy trouble ticket system
- Made recommendations for new technology, laying wires, and supporting Internet services, training, and access services.

3M, Systems Support Specialist (ten months, 1997)

- Setup and maintained workstations and other devices in a TCP/IP environment tunneling Netbios for WINS trusted domains. The environment consisted mostly of NT 3.51, 95, and some 3.x. The printers were HP and Tektronics.
- Remedy was the service request tracking system that was used, focused on problem users, remote support, and NT and NT bug reports.

Metropolitan Council, Systems Support Specialist (three months, 1996)

- Upgraded systems from 286/386 to 486/pentium class machines. Migrated users from DOS to Win 3.xx.
- Provided end user support and training, and trained other consultants.

Anything PC, Inc., Systems Support Specialist (3/96 to 2000, multiple roles)

- PC hardware and software troubleshooting and repairs

Sysinfo.com, Systems Security Specialist (1995 to Date)

- Established an Internet presence, including SMTP, WEB (http/https/html) ssh, and various other TCP/IP services.
- Established and maintain packet-filters (ipfilter, ipfwadm, ipchains, tcpd), IDS security (tripwire, icmpinfo, tcplogger, logcheck, imon, tcpdump, ethreal, etc) and proxy services (squid) Solaris, SGI, Linux, FreeBSD (satan, nessus, nmap, cheops, hping2, etc), Windows

Honeywell Inc., Systems Support Specialist (1991 - 1994 2.5 years)

- Completed SCO, Apollo, SUN UNIX/Netware, dual protocol, PC and Macintosh node and software installations and upgrades in a SCO-Unix/Novell Netware (thin-net) multi-site LAN/WAN setting.
- Performed hardware and software testing and evaluation, installation, and support.
- Performed UNIX file restores, special projects, and e-mail. Installed cables, testing, moves, retrieved Paradox data and generated reports.
- General system administration, configured Cisco and Wellfleet routers. Overall responsibility included five sites, 1500 local users, three-five international sites including Mexico. Used Awk and Sed scripts to modify log in files for users. System Administration chores. Tested, evaluated, and installed hardware and software. Completed a UNIX TCP/IP configuration in a 1500+ LAN.
- Completed a survey and assessment of dataswitch (RS232/PBX) connections to mainframe hosts. This included removing PBX connections and disconnections where feasible and maintaining the databases of users.
- Configured, serviced, and shipped systems to Mexico.

Minnesota Information Systems, Systems Security Specialist (1991 to 2000, multiple roles)

- Established an Internet presence, including SMTP, WEB (http/html), and FTP services via PPP.
- Conducted an intensive study of the innerworkings of TCP/IP, routing, gateways, packet-filters (ipfwadm), security (tcpd, probe, identscan, cops, swatch), and proxy services (squid).

Starnet Communications, Systems Support Specialist (1994 - 2000)

- Network monitoring, systems audits (bass, nmap, nessus, identscan, probe, tcpdump, etc), administrative assistance, SUNOS, IRIX, etc.

Additional Contract Positions

(1985 – 1995)

Provided network and database support for clients including Unisys, Target Stores, Industrial Beltric, Dalhberg Inc, multiple law offices and medical practices. Technical environments included UNIX, Novell, DOS, Windows, OS/2 and VMS. Supported MS and proprietary applications for PC's, Paradox and FoxPro databases. (Specific details available upon request)

EDUCATION:

University of Minnesota 1976-78/1983-85

Minneapolis, MN Completed 250+ credits

TekMetrics Certified: UNIX Sys Admin, Linux Admin, Web Developer, Internet Security Specialist, 1999**ITIL** foundation certified 2007Resume online at: <http://sysinfo.com/resume.html>Certifications: <http://www.tekmetrics.com/transcript.shtml?pid=13775>Member: Eastern Carolina Infragard
Raleigh/Durham ISSA Chapter