

ISAAC D. KISHK

isaac@kishk.org

SUMMARY

Experienced network security engineer looking for new and challenging engineering and development opportunities which allow for career growth and take advantage of 14 years of experience working interactively with customers and all levels of management. Broad knowledge of hardware, software, and networking technologies to provide a powerful combination of analysis, implementation, and support. Experienced in system and network administration and engineering, hardware evaluation, project management, systems and network security, incident analysis, system recovery, product engineering, and product development.

OBJECTIVE

Provide network, systems, and security experience, knowledge, and solutions in a system and network-diverse environment. Protect confidentiality, integrity, and availability of information and information systems. Advise and engineer secure solutions for business opportunities. Develop new and exciting products for customers.

EXPERIENCE

July 2010

Cisco Systems, c/o Kforce

June 2011

IT Network Systems Integration Specialist

Overview:

As a member of the Cisco ROS Service Delivery team, I must work closely with other CROS stakeholders to install, configure, monitor, operate, troubleshoot, tune NFX based security monitoring platform. Must review Cisco ROS Service operations and make recommendations of best practices or other improvements. Cisco ROS supports and trains stakeholders on NFX platform. Architecture of enterprise clients which include the support of Cisco Security domain devices, firewalls and IPS. Systems based support including XML, SOAP based Web services, Unix Shell scripting, Perl, Regex, Oracle SQL, and DBA skills are common. Network management tools such as NetCool, traffic sniffers, and packet analyzers are used for debugging networks and systems. Non-Cisco security devices are also supported.

February 2010

First Data Corporation, c/o Cognizant

August 2010

Information Security Analyst; Network Security and Firewall Operations Group

Overview:

Work within a highly secure, three tiered environment, to satisfy PCI and IRS security standards. Implement and maintain network security firewalls based on CheckPoint, Cisco PIX/ASA, and Netscreen platforms. Ensure the confidentiality, availability, and integrity of all systems, applications, and data in accordance with corporate policy. Monitor, identify, and mitigate security weaknesses. Enforce information security policies and procedures. Develop

detailed technical recommendations to solve security issues. Perform risk assessments, provided recommendations, and present findings. Work with application developers to ensure that proper security controls are identified, implemented, and tested. Design, implement, and maintain firewall systems and firewall policies. Participate in an incident response team as necessary.

June 2009 to
January 2010

Texas Association of Local Health Officials
Consultant

Overview:

- Responsible for network audits, maintenance, configuration, and installation, including various Cisco products ranging from a 7206VXR to Cisco PIX 525, as well as Catalyst switches and concentrators.
- Responsible for Blade server audit and maintenance on Dell and IBM platforms.
- Responsible for SAN audit and maintenance of EMC and DELL platforms
- Responsible for VMWare maintenance and upgrades, which includes day to day maintenance of Linux and Windows VMs.
- Migrated and converted a large County Health Department's physical servers to VMWare and Dell SAN.
- Performed Windows Active Directory migration from 2003 to 2008.
- In process of Exchange 2007 CCR planning, installation, and migration from 2003.
- Responsible for internal DNS via AD, and external DNS via an appliance which uses Bind.
- Responsible for various Linux systems with a company preference for CentOS with RHEL.
- Responsible for the CDC PhinMS backend implementation.
- Planned, configured, and installed various systems within mobile communications trailers with satellite connectivity providing VoIP, Wifi, and XM radar deployments to disaster zones.

November 2000 to
November 2008

Savvis (acquired Cable & Wireless America/Exodus Communications)
Senior Network Security Engineer, Master Architect; Managed Security Services

Overview:

As a senior member of the Managed Security Services team, provided technical leadership for up to 6,000 enterprise customers consisting of up to 10,000 devices. Provided direct customer support for various devices which included Cisco PIX/FWSM/MSB/ASA/IOS firewalls, Checkpoint Firewall-1/VPN-1/Provider-1 products, Cyberguard, Raptor, Iptables, Ipf, snort, nessus, and Qualys. Installed and maintained security infrastructure, including log management, security assessment systems, customer access to information, policy parsers, monitoring system, as well as system administration and hardening of Linux, FreeBSD, Solaris, and Windows with redundancy and bare-metal recovery in mind. Maintained a Citrix cluster for seamless application use. Maintained a Microsoft PDC which contained Active Directory as well as RSA SecurID. Planned and installed many customer devices from

power and BTU assessments to crimping network cables. Maintained various Cisco and Foundry switching including 6509, 3750, 2924xl, and BigIron. Assessed threats, risks, and vulnerabilities from emerging security issues. Drafted enterprise security standards and guidelines for firewall configuration and policies. Managed process and acted in the lead role for various internal and customer facing management networks. Engineered customer products using emerging technologies with focus on customer ease and usability. Performed and created procedures for system security audits, penetration-tests, and vulnerability assessments. Developed Perl and shell scripts to maintain, automate, report, and backup key security and infrastructure procedures.

Networking:

- Performed highly skilled work with Cisco and Check Point security products, as well as hardware and software from other leading vendors such as Foundry, ISS, Nokia, CyberGuard, HP, Netapp and Citrix.
- Acted as migration and integration lead in several successful network deployments involving the seamless integration of legacy Managed Security Support Architectures into existing corporate networks.
- Managed a large, enterprise network of Cisco FWSM blades on Catalyst 65xx systems and Cisco MultiService Blades on the Cisco 12000 XR platform.
- Designed, implemented, and maintained an IPSEC-based VPN management network. Documented and supported client VPN product for end user use. Assisted with basic configuration and QoS implementations of MPLS networks.
- Handled top-tier ticket escalations and provided flexible solutions to a wide variety of problems ranging from ACL and NAT configuration issues to more complex situations requiring vendor involvement. Offered calm and efficient guidance to clients in high pressure response situations.
- Designed and documented numerous security technologies for deployment within our global corporate network. Worked closely with related business partners, vendors, and engineering teams to coordinate proposed solutions.

Programming:

- Authored a Perl-based, SNMP/ICMP notification and response system designed to efficiently monitor thousands of devices while providing real-time status information to the Managed Security Operations Center.
- Designed and administered the managed security portal for use by in-house support personnel. Developed LAMP stack applications and features in support of an ongoing program to improve the overall level of service, responsiveness, and accountability for the clients.

January 2000 to
October 2000

1stBuy.com, Inc.

Technical Director, Network/Security/Systems Administrator

Overview:

Responsible for day to day operations of the systems and network. Oversaw three to five employees ranging from a webmaster to a database administrator. Administered most system tasks, varying from maintenance of various Cisco (2621, cat2924), 3com SuperStacks, and over 30 custom built and home built systems. Servers consisted of RedHat and Slackware Linux, with a Netattach File server. Handled all security issues from securing the site, keeping it secure, to handling security breaks. Programmed various backend interfaces for customer support and accounting departments. Maintained MySQL database integrity and operations. Handled all sendmail issues, including Majordomo Owner and spam control. Designed and maintained several pieces of logging software for inter-office communication. Assisted customers with upper tier technical issues. Assembled and installed systems from scratch.

- Migrated entire network from fractional T1 connectivity to 100Mbps in two weeks with no downtime for customers or employees.
- Oversaw all DNS, IP routing and Firewall/IDS operations.
- Assisted customers with upper-tier technical issues.
- Administered several file servers across a heterogeneous Windows/Linux environment (Samba).
- Maintained several MySQL databases.
- Authored numerous Perl programs to extract information from various backend interfaces to support the needs of our customer service and accounting departments.

January 1997 to
January 2000

Illuminati Online

Operations Manager, Senior Network/Systems Administrator

Overview:

Responsible for supervising and overseeing day to day operations of systems administrators. Managed the webmaster, customer support manager, and other administrators. Responsible for most system tasks, varying from maintenance of various Cisco (7206, 4000, 3640, 3620, 3000, 2501, as5300, as5200, Catalyst 5000, etc), Ascend, 3com and other products. Handled all DNS, and routing issues as well as systems upkeep. Servers ranged from Solaris, FreeBSD, Linux, and NetApp NAS. Handled all security issues from securing the site, keeping it secure, to handling security breaks. Rewrote some of the in-house billing system. Maintained several MySQL databases as well as a few Oracle databases. Handled all sendmail issues, which included Majordomo Owner and spam control. Handled all news server administration, which handled a full feed.

- Acted as the designated security officer, responsible for the in-depth analysis and handling of all online security-related incidents.
- Resolved all DNS and routing issues, providing direct assistance to customers as needed.

- Authored several computer programs for flexible log file analysis, inter-office communications and in-house billing and receipting.
- Maintained comprehensive online customer service guidelines and an internal staff web server for use by all support personnel.

August 1996 to
December 1996

Signet Partners

Unix Administrator/Technical Support

- Performed routine administration of local Unix servers including periodic system upgrades, user base and file system maintenance, backup snapshots, performance tuning and security audits.
- Provided courteous and timely email and telephone assistance to internal clients with prompt resolution on all trouble tickets.
- Successfully planned and implemented a significant wiring upgrade for one of the offices (UTP ethernet and digital telephony).

SKILLS

Matrix:

Skill Name	Skill Level	Experience
Linux System Administration	Expert	16 years
Solaris System Administration	Expert	8 years
FreeBSD System Administration	Intermediate	10 years
IP Packet Analysis - Ethereal, tcpdump, ntop	Expert	6 years
Intrusion Detection – Snort, Realsecure	Intermediate	5 years
Penetration Testing - Nessus/Nmap	Expert	12 years
DNS Administration (bind)	Expert	12 years
Perl	Expert	14 years
PHP	Intermediate	14 years
Apache, DHCP, MySQL, SAMBA, Sendmail, SSH, Qmail Administration	Expert	10 years
Cisco IOS interfaces, routing, firewall	Intermediate	10 years
Cisco XR interfaces, routing, firewall	Intermediate	2 years
Cisco IOS- BGP	Intermediate	6 years
OSPF	Intermediate	6 years
Cisco PIX/ASA Firewalls	Expert	9 years
Cisco FWSM Firewalls	Expert	6 years
Cisco MSB Firewall	Intermediate	2 years
Checkpoint Provider-1/Firewall-1	Expert	9 years
Cyberguard Firewall	Expert	8 years
Juniper Netscreen	Intermediate	2 years
Juniper NSM	Intermediate	1 year
Cisco 65xx, 35xx, 29xx switches	Expert	7 years
Vlan, Vlan tagging, Spanning tree	Expert	6 years
Foundry BigIron	Intermediate	5 years
Nokia IP appliances	Expert	7 years
Nokia CryptoCluster	Expert	7 years
RSA SecurID server administration	Intermediate	5 years
Citrix Metaframe Administration	Intermediate	5 years
F5 BigIP Administration	Intermediate	3 years

Siebel ticket system end user	Intermediate	8 years
Vantive ticket system end user	Intermediate	3 years
Remedy ticket system end user	Intermediate	2 years
SVN/RCS Administration	Intermediate	4 years
IP allocation and management	Expert	12 years
Microsoft Visio	Intermediate	9 years
RSA SecurID server administration	Intermediate	5 years
Radius administration	Intermediate	6 years
Qualys	Intermediate	2 years
EMC SAN	Intermediate	2 years
VMWare	Intermediate	7 years
Netapp NAS	Intermediate	7 years

Operating Systems:

- Experienced in the installation, maintenance, and administration of Solaris, Linux, BSD, IPSO, Cisco IOS, XR, CatOS, ASA, PIX, ACE, FWSM, MultiServiceBlade, and various Windows Server platforms.

Networking:

- Hands-on experience with hardware from Cisco, Foundry, Check Point, Nokia (IP Appliance and CryptoCluster), Ascend and many others.
- TCP/IP networking generalist. Able to quickly and efficiently isolate and repair complex hardware and software problems throughout the network.
- Proficiency designing enterprise class network architecture including specification, cost-benefit analysis, implementation and integration.

Programming:

- Experienced Perl, PHP and shell programmer, with considerable expertise developing LAMP stack applications (Linux, Apache, MySQL, PHP). Excellent team player, with the ability to work cooperatively and lead others in the successful delivery of important projects.

REFERENCES

Available upon request.