

John Smith

Prattville, AL

career@hashbangsecurity.com

Career Objective

I am a certified and skilled senior security and UNIX systems administrator with over twenty years of experience. I am seeking a position that allows me to contribute to meeting the organization's goals and also exercise, expand and improve my technical experience.

Professional Certifications

- Certified Information Systems Security Professional (CISSP),
- EC-Council Certified Security Analyst (ECSA),
- Certified Ethical Hacker (CIEH),
- Computer Hacking Forensic Investigator (CHFI),
- Certified Systems Administrator HP-UX 11i v3 (CSA), and
- Sun Certified System Administrator for Solaris 10 OS (SCSA)

Detailed Experience

Defense Information Systems Agency (DISA)

Aug 2010 – Present

IT Specialist (App/SW)

July 2011 – Present

IT Specialist (SysAdmin)

May 2011 – July 2011

Information Assurance Officer

Aug 2010 – May 2011

Responsibilities:

- Maintain DISA's Enterprise Security Posture System (ESPS) Java-based UNIX Host Configuration Reporting Agent (HCRA).
- Maintain DISA's UNIX ESPS toolkit scripts.
 - o This toolkit is a vulnerability assessment tool used in multiple Defense Enterprise Computing Centers on thousands of UNIX/Linux servers.
 - o The scripts support AIX 5, 6 and 7; HP-UX 11i v1, v2 and v3; Red Hat Enterprise Linux (RHEL) 5 and 6; and Solaris 9, 10 and 11.
 - o The scripts check hundreds of security settings and generate reports on the results.
 - o If specified a subset of the scripts remediate security settings on the server.

- o Perform vulnerability assessments on hundreds of Department of Defense (DoD) and Air Force new and existing IBM AIX (versions 6 and 7), HP-UX (versions 11i v1, v2 and v3), Red Hat Enterprise Linux (versions 4, 5 and 6), and Oracle Solaris (versions 9, 10 and 11) servers using DISA's Security Technical Implementation Guide (STIG) and Security Requirements Guides (SRG).

Accomplishments:

- Redesigned and rewrote the ESPS Host Configuration Reporting Agent in Java. The redesigned agent supports all current versions of IBM AIX, HP-UX, Linux (Oracle Enterprise Linux, Red Hat Enterprise Linux, SuSE Linux Enterprise x86 and System z), and Oracle Solaris.
- Added over 360 new findings to the ESPS toolkit when DISA converted from the UNIX STIG to the new Secure Content Automation Protocol (SCAP)-based SRG.
- Added over 150 new findings to the ESPS toolkit to support Red Hat Enterprise Linux 6 and Solaris 11.
- Helped DISA achieve outstanding results on official UNIX server reviews conducted by DISA's Field Security Office (FSO).

Branch Banking and Trust (BB&T)/Colonial Bank Mar 2006 – Aug 2010

UNIX Supervisor

Jan 2007 – Aug 2010

UNIX Administrator

Mar 2006 – Jan 2007

Responsibilities:

- Senior Systems Administrator supporting IBM AIX, HP-UX (Serviceguard cluster), Red Hat Enterprise Linux and Sun Solaris systems.
- Support the Service Oriented Architecture (AIX/WebSphere), Online Banking (HP-UX/BEA Tuxedo), Check Imaging (Solaris/NCR) and Statement Imaging applications (AIX) and Internet-facing DNS servers (RHEL/BIND).
- Supervise three UNIX administrators.

Accomplishments:

- Performed a health check and systems security audit of BB&T's Specialized Lending Group's UNIX servers (Red Hat Enterprise Linux, Sun Solaris and IBM AIX).
 - o Provided security findings and remediations, and best practice UNIX systems administration recommendations.
 - o Created over two hundred and ninety (290) pages of server configuration documentation.

- Designed and implemented a UNIX Security Review project to improve Colonial Bank's servers' security and meet auditing requirements.
 - The project reduced audit findings by 80% in the first year and eliminated all audit findings in the second year.
- Developed and implemented a patch management cycle.
- Wrote a log summary script in Perl to help meet log review auditing requirements.
- Improved the reliability and uptime of the UNIX environments by developing Perl and shell scripts to audit system and application log files and alert on defined events and messages.
- Successfully handled UNIX Disaster Recovery tests.
 - Wrote scripts that reduced system administrative preparatory time by sixty-seven (67) percent.
- Hardened RHEL DNS servers responsible for serving the bank's DNS domains to the Internet.
- Wrote monitoring script to replace BMC Patrol Agent.
 - The script sent email alerts to Colonial's Command Center when issues were detected.
- Authored multiple processes and procedures standardizing UNIX team support and customer experience.

Science Applications International Corporation Jan 2005 – Mar 2006

Security/Network Engineer for NOAA's National Data Buoy Center (NDBC)

Responsibilities:

- Security and Network Engineer
 - Manage security platforms (SonicWALL firewall, Foundry ServerIronXL and Nessus Linux servers).
 - Manage existing client network (Cisco Catalyst 3750, 5500 and 6500).
 - Document and maintain the client's Business Continuity and Disaster Recovery plans.
 - Assist the client with their Certification and Accreditation (C&A) requirements.
- UNIX Systems Administration
 - Backup UNIX Systems Administrator.
 - Mentor Systems Support coworkers in UNIX/Linux, Security and Networking.

Accomplishments:

- Served as Senior UNIX Systems Administrator during contract transition.
 - Automated manual UNIX backups on AIX and Solaris systems.
 - Wrote Perl scripts to monitor the AIX real-time systems and send email alerts when problems were detected.
- Identified and corrected issues in the client's servers' backup scheme.

Konica Minolta Printing Solutions USA, Inc.

formerly Minolta-QMS, Inc. and QMS, Inc.

Mar 1991 – Jan 2004**Senior Systems Administrator
Programmer/Analyst****Dec 1991 – Jan 2004****Mar 1991 – Dec 1991****Responsibilities:**

- Senior Systems Administrator of more than 175 HP-UX, Linux and Solaris workstations and servers; Digital OpenVMS cluster; and Cisco network administration.
- Support the Engineering Hardware and Software development groups' application software running on HP-UX and Sun Solaris.
- Internet DNS Administrator managing approximately thirty domains.
- Support the Engineering Hardware and Software development groups' application software.
- Security Administrator of the corporation's Cisco PIX 520s and VPN 3030.

Accomplishments:

- UNIX
 - Designed and managed all server backups and restores.
 - Installations and upgrades of Engineering UNIX operating systems and applications.
 - Prepared all UNIX systems and applications for Year 2000.
- Security
 - Designed and built corporate DMZ, firewall, DNS, email, ftp and web servers on Sun Solaris systems using publicly available tools.
 - Created and maintained access-lists for corporate Internet access.
 - Built corporate Intrusion Detection Systems (IDS) using Snort on Linux servers.
 - Built Syslog server for the IDS systems and other network devices on Linux servers.

- Network
 - Debugged DHCP issue with development printers using Fluke Networks Protocol Expert and Ethereal.
 - Resolved auto-negotiation issue between Cisco switches and all UNIX servers and workstations.

Education

University of South Alabama

Sep 1979 – May 1983

- Bachelor of Science Degree in General Management.
- Emphasis in Operations Research Management, Statistics and Computer Programming.
- Major GPA: 3.64.
- Overall GPA: 3.26.
- Member of Sigma Iota Epsilon (honorary management).