Patrick Vogel | Security Engineer

patrickvogel@cvpcorp.com

Experience Summary

More than 20 years of experience in system security, engineering, and administration for regional Internet service providers, Web hosting firms and the Federal government (NASA/ACF/DHHS). Strong background in Solaris, Linux, and BSD variants and hardware troubleshooting. Experience in training and support of multiple enterprise class network operating centers. A genuine appreciation for Operating Systems, Computer system security, and automation.

Relevant Accomplishments/Skills

* 20 years of Unix/Linux System Administration
* 5 Years as Security Engineer
* Automation of Sec Eng tasks with python integrating tools and data from Tenable.sc, AWS, RSA Archer and VMWare VCenter

Education, Certifications, and Training

* CISSP Certification, ISC^2 – July 2021
* Security+ Certification – CompTIA- December 2018

Technical Skills

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Languages | Databases | Applications/Tools | Methodologies/Frameworks | Systems/ Network Platforms |
| **Python** | **Mysql/Postgresql/Oracle/SQL server** | **Nessus** |  | **Unix/Linux/Windows** **Administration** |
| **Java** |  | **Metasploit** |  | **VMWare / VirtualBox** |
| **C/C++** |  | **Burpsuite, Owasp Zap** |  | **AWS** |
| **Aws cli/ S3 cli** |  | **McAfee, Crowdstrike** |  |  |
| **powershell** |  |  |  |  |

Professional Experience

Customer Value Partners (CVP) 12/17 – Present

Technologist / Security Engineer, Linux Technical Lead

***ACF OCIO* » Division of Security, Privacy and Risk Management; Security Engineer (12/17 – Present)**

* Building DISA STIG/CIS hardened and security minded RHEL and Amazon Linux systems
* Proof of concept implementing DISA STIG Ansible playbook into baseline AWS AMI using Packer and Terraform
* SME for CVP in Linux and UNIX Administration, Supporting other CVP and ACF Operations staff, IPT/Application groups and 3rd party vendors
* Security scanning with Tenable SC and Burpsuite, Owasp Zap, Web Inspect, interpretation and mitigation of vulnerabilities found with those tools and Synack pen-tests
* Learning Pentesting through Kali Linux and Metasploit training, now working towards OSCP certification
* Developed automation scripts for ACF systems:
* import AWS asset IP information into Tenable via API to keep scan information up to date automatically (aws cli, pyTenable)
* import VMWare IP address information into Tenable using PyVmomi
* import AWS asset IP information into RSA Archer via an AWS S3 bucket (aws cli, s3 cli, powershell)

Acistek Corporation 06/17 – 12/21

Senior Linux Administrator

*ACF OCIO* » Operations; Senior Unix and Linux Administrator (12/17 – Present)

* Administration of all Linux servers in both Server environments at ACF- Physical/On premises VMWare environment and AWS VPC virtual environment
* Server/Tool technologies such as RHEL, Amazon Linux, Apache Web Servers, Oracle/Web Logic Database and Application servers, Drupal and MySQL, Veritas Netbackup, Monitoring and Security scanning with Tenable (before Security contract took it over), Alertlogic IDS
* Deployments of web applications
* IPT / application / 3rd party vendor support
* Monthly patching of OS
* security scan vulnerability mitigation

Adnet Systems under contract to NASA HQ “HITSS” contract 02/12 – 03/17

Senior Unix Administrator

* Administration of the NASA HQ Solaris and RHEL Linux server environment on physical and VMWare virtual machines
* Web servers running Apache and Tomcat, Mysql and Oracle Databases
* Monitoring servers with Nagios, SolarWinds
* backup management with Veritas NetBackup
* OS patching and security scan vulnerability mitigation

Global Tunnels Limited Company 09/2006 – 02/12

Senior Unix Administrator – ACF Server Operations (before it was called OCIO)

* Solaris and Linux administration of entire ACF data center servers, services and hardware, on premises at the time. Apache, Oracle, Oracle Web Logic were the main technologies used.
* 50 – 100 servers on Sun and Dell Hardware, Data center on premises in the ACF Office

Security Clearance

* Public Trust

Awards, Honors, and Memberships

* N/A

Publications, Research, & Presentations

* N/A

Additional Information

Unix/Linux/Windows Administration, Mysql/Postgresql/Oracle/SQL Database servers, Apache, Oracle Weblogic/Tomcat Application Servers, Python/C++/Java programming, Metasploit, VMWare / VirtualBox, Burpsuite, Owasp Zap, AWS cloud/aws cli, McAfee, Crowdstrike, Splunk, Tenable.SC, powershell, bash shell scripting

Work Experience Start

|  |  |  |
| --- | --- | --- |
| Month | Year | Gap Years/Months  |
| **01** | **1999** | **N/A** |