**Rahul Saple**

Bangalore, Karnataka 560076 6♦ 9833747372 ♦ saple.rahul.eightythree@gmail.com

**Professional Summary**

Looking to transition into the Cyber Security industry as a Junior Penetration Tester. Have over 3 years 8 months of varied and extensive experience in System Administration. Am well versed with cross-domain concepts from networking to administration/implementation, programming to security. Passionate about technology and learning new things. Currently practicing on HackTheBox. Will appear for OSCP in next 3-4 months.

**Skills**

|  |  |
| --- | --- |
| * Linux/Windows * TCP/IP Networking * Cloud Computing * DevSecOps | * Penetration Testing * Vulnerability Assessment * Programming/Scripting |

**Work History**

DevSecOps Engineer , 09/2018 to Current

Systech Services – Bangalore, Karnataka

* Setup a complete Public Key Infrastructure (PKI) system for one of our US clients for their internal purposes. This was based on Windows Server 2016 and involved a two layer setup with an offline root CA and an intermediate issuing CA. Hooked up all their systems to login via certificates automatically issued via Group Policy. \
* Implemented a Central Access Security Broker(Apache Guacamole) cluster that helped in centralizing all access to infrastructure and auditing for improved security. Setup MySQL replication for back-end fail-over.
* Implemented a Pritunl VPN cluster setup using Mongodb cluster as the database back-end for an employee strength of over 2000 users.
* Familiar with Hetzner Cloud as most of the client's physical and virtual infrastructure was on it. Is a much cheaper option to AWS/Azure but requires more hands-on effort and knowledge.
* Setup a Jenkins build system for a client to run test, development and production builds. Integrated it with their Bitbucket repository to automate the builds on git changes and notify it via mail on build status.
* Have extensive experience in writing Ansible scripts from setting up firewall rules, installing applications, monitoring and notifying processes to building and deploying our internal product iTaaS. Even successfully used and deployed AWX(community based version of Ansible tower) for better usability.
* Implemented a 3-node application logging ELK cluster for centralizing logs in one place. Used plugins like LogTrail for accessing raw application logs. Also implemented ElastAlert to monitor events and notify(via mail) on its occurrence.
* Implemented a Redis cluster of 2 nodes using an existing single node Redis instance which was heavily used to load balance traffic and get better performance.
* Client had around 10-12 single instances of HAProxy (Application Load Balancer) for test, development and production environments. Had to convert all of them into 2 node clusters. Implemented HTTPS redirection on the production unit for improved security.
* Implemented a 2-node ProxySQL load balancer from scratch to redirect incoming SQL traffic and benefit from improved efficiency.
* For many of the applications, implemented a multi node High Availability setup using pacemaker and corosync . Where possible also implemented Single Sign On (SSO) using OpenIDConnect or OAuth by integrating it with GSuite.
* Wrote a custom extension for NextCloud application that would parse audit logs and generate a monthly report(summarized and detailed) in PDF format by using the TCPDF plugin.

Linux Administrator, 10/2017 to 09/2018

Agni Information Systems – Bangalore, Karnataka

* Have extensively used private cloud with OpenNebula to host our Kavach iTaaS product as well as our company's virtual production and testing infrastructure. Implemented and tested a high-availability cloud scenario using Ceph cluster as the storage back-end. Ceph is an open-source, highly scalable, distributed storage platform that offers block, object and file storage solution. Tested various cloud related functionalities from snapshotting to live migration. Had to experiment initially with DRBD as the storage back-end before settling for Ceph.
* Have used Wazuh as our go to SIEM and log server. Wrote custom rules for parsing logs from uncommon applications not included as part of default setup. It uses popular ELK stack (Elasticsearch, Logstash and Kibana) for its back-end, pipe lining and visualizing means. Have some experience troubleshooting Elasticsearch too.
* Immensely experienced in installing, troubleshooting and implementing any open-source software, technology for experimental and developmental purposes. Tried out countless no of them to help see which fits our need by thoroughly reading publicly available documentation.
* Am moderately experienced on network related issues. From TCP/IP foundations, host-based and network-based firewalls and general network related troubleshooting.
* Have a firm grasp of bash scripting. Used it to administer many Cron level jobs such as backups, mails and various application related tasks.
* Setup a groupware solution (Kolab) with Amavis/SpamAssassin as the content/spam-filter, Cyrus-Imap as the mailbox service, Postfix as the mail server, Roundcube as the web client. Configured a multi domain scenario with separate name-spaces along with some restrictions at the domain and user level on who could send external mails and to which domain.
* Did a web polygraph test to benchmark the proxy server on one of our firewall products. Required a thorough reading and understanding of low level concepts with respect to networking and systems.

**Education**

B.E: Computer Engineering, 06/2008

K J Somaiya Institute of Engineering And Information Technology - Mumbai

**Certifications**

Working on Offensive Security Certified Professional (OSCP)

Oracle Certified Professional Java Programmer (OCPJP)

Oracle Certified Professional Web Component Developer (OCPWCD)