Krutarth Upadhyay

Krutarth27598@gmail.com

8690085037

Career Objectives

Looking for a challenging role in a reputable organization to utilize my skills for the growth of the organization as well as to enhance my knowledge about Linux and ANSIBLE automation in market.

Education

GANPAT UNIVERSITY

M.Sc.IT (IMS) June 2020

8.27/10 CGPA

GANPAT UNIVERSITY

B.Sc.IT (IMS) June 2018

7.18/10 CGPA

Shree V.P. Mehta Jay Hind High School

COMMERCE March 2015

45% in 12th commerce

Experience

Internship 3 Months

I had Internship with project training on AWS at Compufy techno lab

Professional Skills

Server Linux Administrator and Management:	Advanced
ANSIBLE automation:	Advanced
Docker:	Intermediate
AWS:	Intermediate

Certificate

2018-06 RED HAT CERTIFIED SYSTEM ADMINISTRATOR

Certification id: - 180-147-845

Personal Details

Date of Birth: 27/05/1998

Nationality: Indian

Address: 632, sheshayi bhagavan ni pole, Naiwado, Raipur,
Ahmedabad 380001

Hobbies: Listening Music, Reading books.

Key Projects

Implementation of Docker cluster in centos 7

Experience:

1. I have learned that how to run Docker cluster.
2. It was easy to create, deploy and run application by using docker container.
3. Pulling the image of webserver in docker container to create a webserver.

Implementation of Hadoop cluster deployment with ANSIBLE automation.

Experience:

1. I had learnt that how ANSIBLE automation and Hadoop cluster works.
2. Installed ANSIBLE roles from ANSIBLE galaxy to deploy Hadoop cluster.
3. Using ANSIBLE roles is the easiest way to configure and implement any kind of application.
4. Using a jinja2 template to configure a core-site.xml, hdfs-site.xml, yarn-site.xml, mapred-site.xml.
5. To run a different task there are a different kind of modules in single playbook.
6. Including different playbooks in single playbook so two different playbooks can run at a single time.

Information Security Professional system using kali Linux.

Experience:

1. In this project I have got an experience to find vulnerability of system used it to breach into the system security using kali Linux’s tools and scripts.
2. Used network analysis tool for information gathering and network monitoring.

3. Used vulnerability analysis tools and scripts to find the breaches of systems and security.
4. Used ARP spoofing and man-in-the-middle (MITM) attack to get access of unauthorized and unencrypted data in the network.
5. Used SQL injection to poisoned database and gain access of data and web site.
6. Used password attack tools to decrypt the password using different hash formats.