NETWORK FILE SHARING
AN INTERNSHIP REPORT

Submitted by

GOKULAKRISHNAN K J

(310620104045)

BACHELOR OF ENGINEERING

in

COMPUTER SCIENCE AND ENGINEERING

EASWARI ENGINEERING COLLEGE, CHENNAI

(Autonomous Institution)

Affiliated to

ANNA UNIVERSITY::CHENNAI – 600025

MAY 2023

CERTIFICATE OF EVALUATION

College Name	: Easwari Engineering College
Branch & Semester	: Computer Science and Engineering & VI
Internship Period	: 30/07/2022 – 30/10/2023
Company Name	: Vectra Technosoft
Duration	: 3 month

S.No	**Name of the Student with Regno**	**Title**	**Name of the Supervisor with Designation in Industry**
1.	Gokulakrishnan K J (310620104045)	Network File Sharing	Babu M.N

The report of the internship work submitted by the above students in partial fulfillment for the award of Bachelor of Engineering Degree in Computer Science and Engineering of Anna University were evaluated and confirmed to be are part of the work done by the above student.

The internship evaluation was held on ____________________

EXAMINER -1 **EXAMINER-2**

TABLE OF CONTENTS

1.1 OBJECTIVE

The objective of network file transfer in Red Hat Linux is to securely and efficiently transfer files over a network from one system to another. This can be done using various protocols such as FTP (File Transfer Protocol), SCP (Secure Copy), SFTP (Secure File Transfer Protocol), and Rsync.

The primary goal of network file transfer is to ensure that data is transferred reliably, securely, and without corruption. This can be achieved by using encryption protocols, such as SSL (Secure Socket Layer) or TLS (Transport Layer Security), to protect the data in transit. Additionally, it is important to ensure that the transfer process is efficient and does not consume excessive network bandwidth.

In a Red Hat Linux environment, network file transfer can be accomplished using various tools and utilities, including the command-line utilities such as scp, sftp, and rsync. Additionally, there are graphical user interfaces available, such as the Nautilus file manager, that provide an easy-to-use interface for transferring files over a network. The objective is to choose the appropriate tool that best meets the needs of the user and the security requirements of the organization

1.2 SCOPE OF THE INTERNSHIP

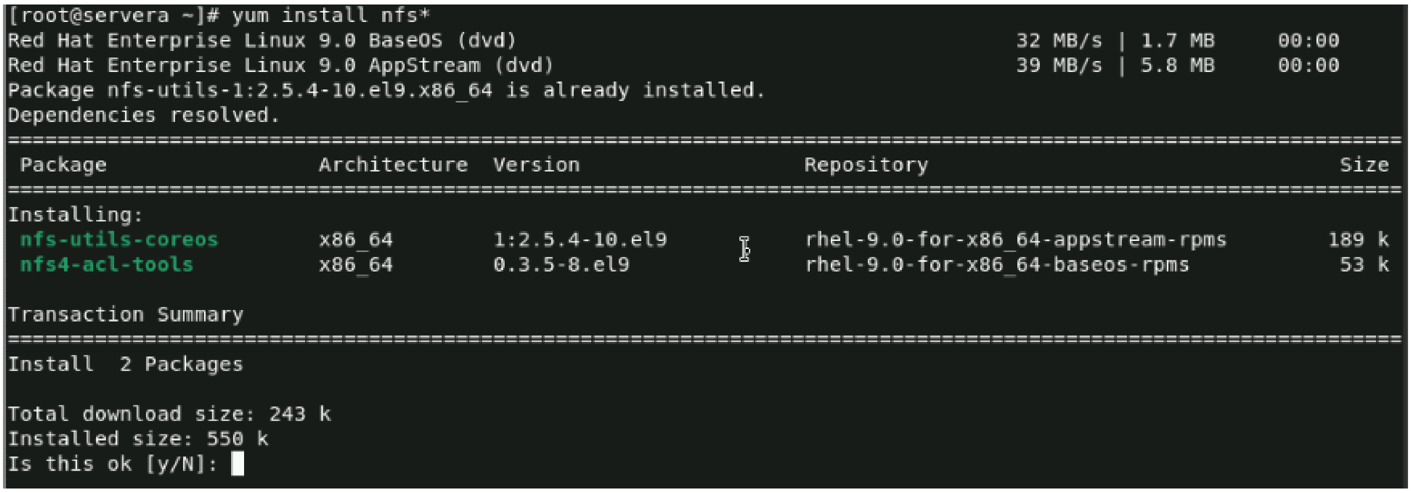
The internship will provide an opportunity for students to gain hands-on experience with Linux command line interface in Red Hat Linux technology. The internship will cover fundamental concepts such as navigating the file system, creating and managing files and directories, manipulating text files, controlling processes, and performing basic system administration tasks. The interns will learn how to use various Linux utilities and tools such as grep, sed, awk, and more. Additionally, the internship will cover best practices for security and file permissions, and introduce basic troubleshooting techniques.

1.3 IMPLEMENTATION

1. Open a terminal on your Red Hat Linux system.

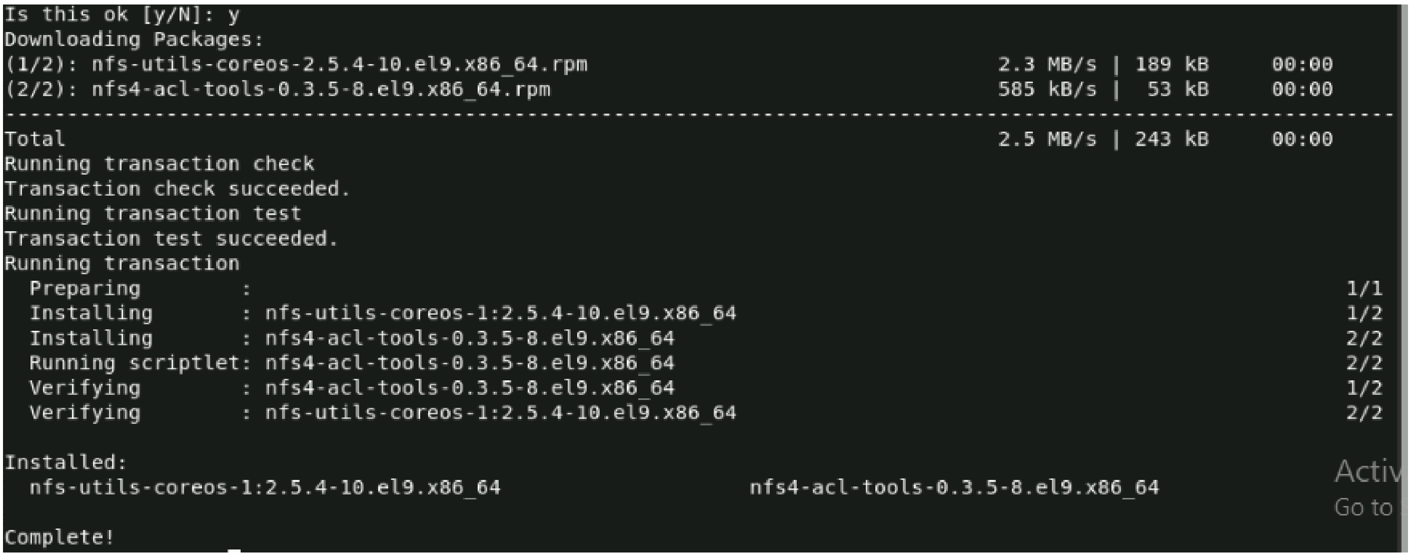
2. Ensure that you have administrative privileges by logging in as the root user or using the sudo command.

3. Once the package repository information is updated, run the following command to install all packages that begin with the string "nfs":



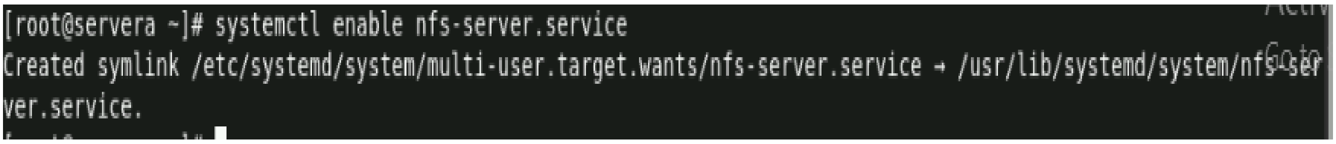
```
[root@servera ~]# yum install nfs*
Red Hat Enterprise Linux 9.0 BaseOS (dvd)                              32 MB/s | 1.7 MB     00:00
Red Hat Enterprise Linux 9.0 AppStream (dvd)                           39 MB/s | 5.8 MB     00:00
Package nfs-utils-1:2.5.4-10.el9.x86_64 is already installed.
Dependencies resolved.
=====================================================================================================
 Package                Architecture  Version                 Repository                        Size
=====================================================================================================
Installing:
 nfs-utils-coreos       x86_64        1:2.5.4-10.el9          rhel-9.0-for-x86_64-appstream-rpms   189 k
 nfs4-acl-tools         x86_64        0.3.5-8.el9             rhel-9.0-for-x86_64-baseos-rpms       53 k

Transaction Summary
=====================================================================================================
Install  2 Packages

Total download size: 243 k
Installed size: 550 k
Is this ok [y/N]:
```

4. Press y to Download the Packages



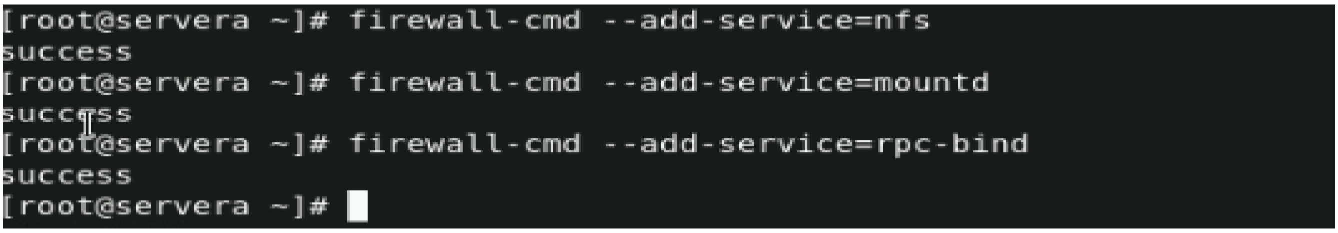
```
Is this ok [y/N]: y
Downloading Packages:
(1/2): nfs-utils-coreos-2.5.4-10.el9.x86_64.rpm                    2.3 MB/s | 189 kB     00:00
(2/2): nfs4-acl-tools-0.3.5-8.el9.x86_64.rpm                       585 kB/s |  53 kB     00:00
-----------------------------------------------------------------------------------------------------
Total                                                              2.5 MB/s | 243 kB     00:00
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing        :                                                                          1/1
  Installing       : nfs-utils-coreos-1:2.5.4-10.el9.x86_64                                   1/2
  Installing       : nfs4-acl-tools-0.3.5-8.el9.x86_64                                        2/2
  Running scriptlet: nfs4-acl-tools-0.3.5-8.el9.x86_64                                        2/2
  Verifying        : nfs4-acl-tools-0.3.5-8.el9.x86_64                                        1/2
  Verifying        : nfs-utils-coreos-1:2.5.4-10.el9.x86_64                                   2/2

Installed:
  nfs-utils-coreos-1:2.5.4-10.el9.x86_64                   nfs4-acl-tools-0.3.5-8.el9.x86_64

Complete!
```

5. The command "**systemctl enable nfs-server.service**" is to enable the NFS server service to start automatically at boot time on a Red Hat Linux system.



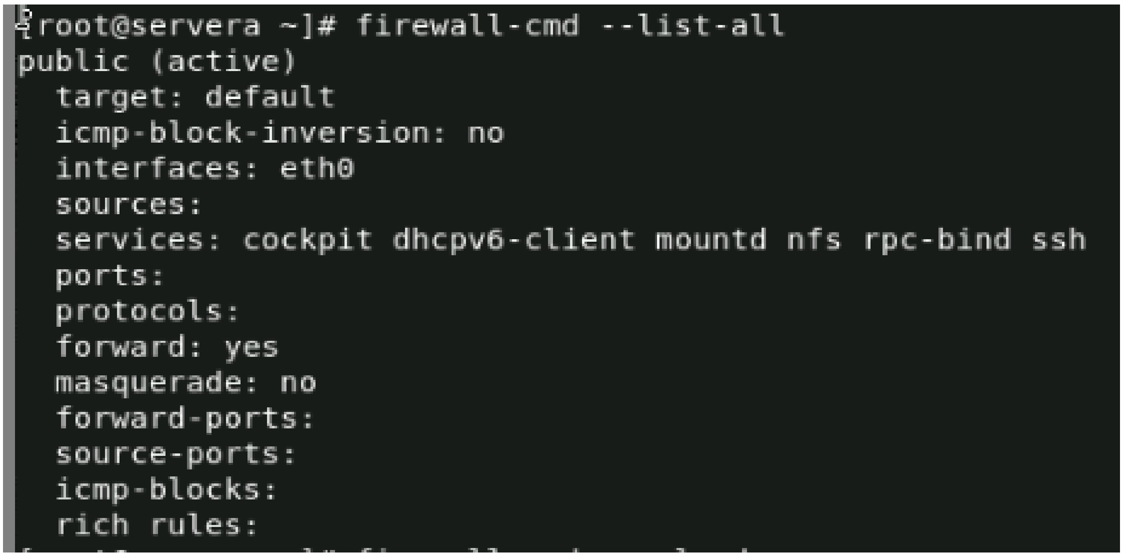
```
[root@servera ~]# systemctl enable nfs-server.service
Created symlink /etc/systemd/system/multi-user.target.wants/nfs-server.service → /usr/lib/systemd/system/nfs-ser
ver.service.
```

6**.** The command **"firewall-cmd --add-service={nfs,mountd,rpc-bind}"** is to add the NFS, mountd, and rpc-bind services to the system firewall .



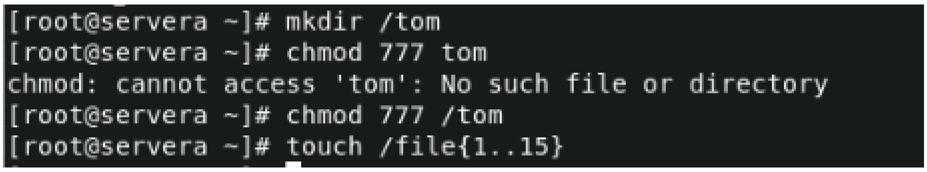
```
[root@servera ~]# firewall-cmd --add-service=nfs
success
[root@servera ~]# firewall-cmd --add-service=mountd
success
[root@servera ~]# firewall-cmd --add-service=rpc-bind
success
[root@servera ~]#
```

7. The command **"firewall-cmd --list-all"** is to display a comprehensive list of all firewall settings, including the currently enabled services and zones.



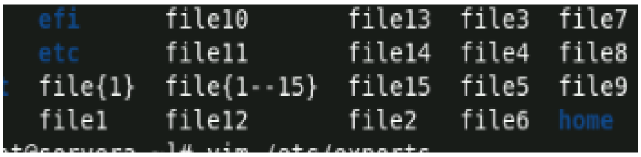
```
[root@servera ~]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: eth0
  sources:
  services: cockpit dhcpv6-client mountd nfs rpc-bind ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

8. The command "**mkdir /tom**" is to create a new directory called "tom" in the root directory of the file system**.”chmod 777 /tom “**is to give the read,write and execute access to the /tom file and
The command “**Touch /file{1..15}** is to create 15 files in the /tom directory.



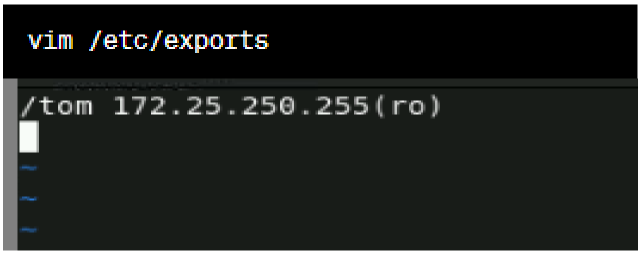
```
[root@servera ~]# mkdir /tom
[root@servera ~]# chmod 777 tom
chmod: cannot access 'tom': No such file or directory
[root@servera ~]# chmod 777 /tom
[root@servera ~]# touch /file{1..15}
```

9. The command "**ls /tom**" is to display a list of all files and directories located in the "/tom" directory.



```
  efi      file10        file13  file3  file7
  etc      file11        file14  file4  file8
: file{1}  file{1--15}   file15  file5  file9
  file1    file12        file2   file6  home
t@servera ~]# vim /etc/exports
```

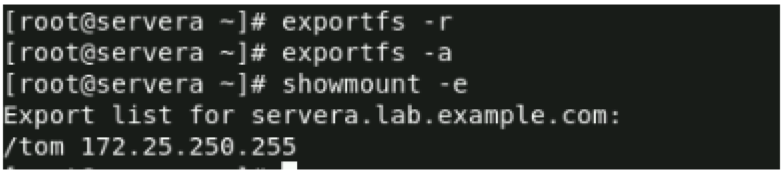
10. The command "vim /etc/exports" is to open the "/etc/exports" file for editing using the Vim text editor.



```
vim /etc/exports

/tom 172.25.250.255(ro)

~
~
~
```

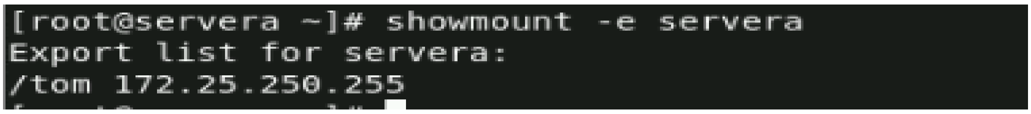
11. The command "**exportfs -r**" is to refresh the NFS exports to apply any changes made to the "/etc/exports" file and the command "**exportfs -a**" is to export all directories listed in the "/etc/exports" file to all clients with the appropriate permissions.

12. The command "**showmount -e**" is to display a list of all directories currently exported by the NFS server.



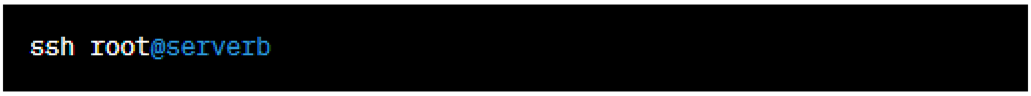
```
[root@servera ~]# exportfs -r
[root@servera ~]# exportfs -a
[root@servera ~]# showmount -e
Export list for servera.lab.example.com:
/tom 172.25.250.255
```

13. The command "**showmount –e servera**" is to display a list of all directories currently exported by the NFS server from the servera.



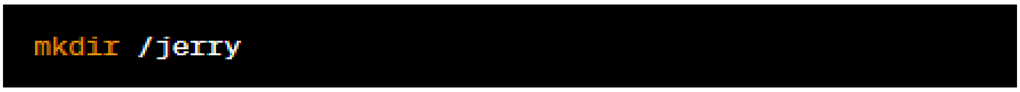
```
[root@servera ~]# showmount -e servera
Export list for servera:
/tom 172.25.250.255
```

14. the command "**ssh root@serverb**" is to establish a secure shell (SSH) connection to the remote server "serverb" as the root user, allowing for remote access and management of the server from a Red Hat Linux system.



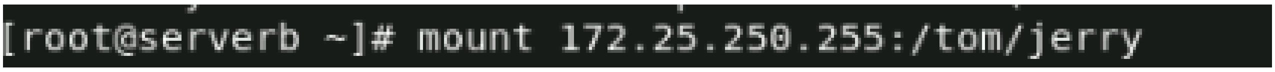
```
ssh root@serverb
```

15. The command “**mkdir /jerry**” is to create a directory in a server



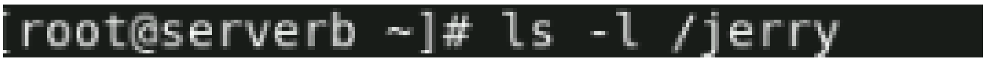
```
mkdir /jerry
```

16. The command "**mount 172.25.250.255:/tom/jerry**" is to mount the "/tom/jerry" directory from the NFS server with IP address "172.25.250.255" onto the current system's file system on a Red Hat Linux system. This will allow access to the files and directories within the "/tom/jerry" directory on the remote NFS server from the local system. Once the directory is mounted, it can be accessed like any other directory on the local file system.

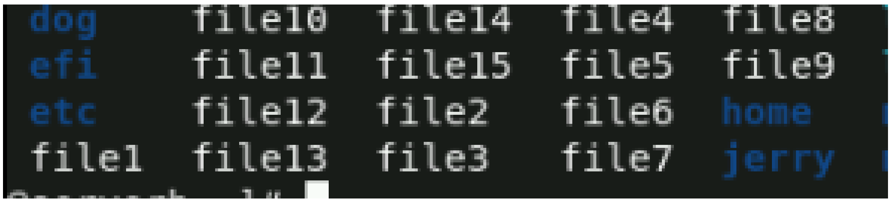


```
[root@serverb ~]# mount 172.25.250.255:/tom/jerry
```

17. The command "**ls -l /jerry**" is to list all files and directories in the "/jerry" directory in a long format, including detailed information such as file permissions, ownership, size, and modification date. This command can be used to examine the contents of the "/jerry" directory



```
[root@serverb ~]# ls -l /jerry
```



```
 dog     file10  file14  file4  file8
 efi     file11  file15  file5  file9
 etc     file12  file2   file6  home
 file1   file13  file3   file7  jerry
```

That's it! You have successfully transfered the files from the server A to serverB

1.4 MILESTONES

PHASE	DESCRIPTION	STATUS
Controlling processes	Understand the concept of processes in Linux Learn how to start, stop, and monitor processes using basic Linux commands Gain familiarity with tools such as top and ps	Completed
Troubleshooting and best practices	Learn how to troubleshoot common Linux issues Understand the importance of security and file permissions in Linux Learn best practices for managing and maintaining Linux systems	Completed

1.5 RISKS

There are several risks associated with network file transfer in RedHat Linux. Some of the common risks are:

Unauthorized Access: Network file transfer may result in unauthorized access to sensitive information if the transfer is not secure. Attackers may intercept network traffic and steal data, or gain unauthorized access to the system and modify or delete files.

Malware Infections: Malware can spread through network file transfer, infecting systems and stealing sensitive data or causing damage to the system.

Data Loss: Network file transfer may result in data loss if the transfer is interrupted or fails due to network issues. This may cause the transfer of incomplete or corrupted files, resulting in data loss.

Data Theft: Network file transfer may result in data theft if the transferred files contain sensitive information. Attackers may intercept network traffic and steal data, or gain unauthorized access to the system and copy or delete files.

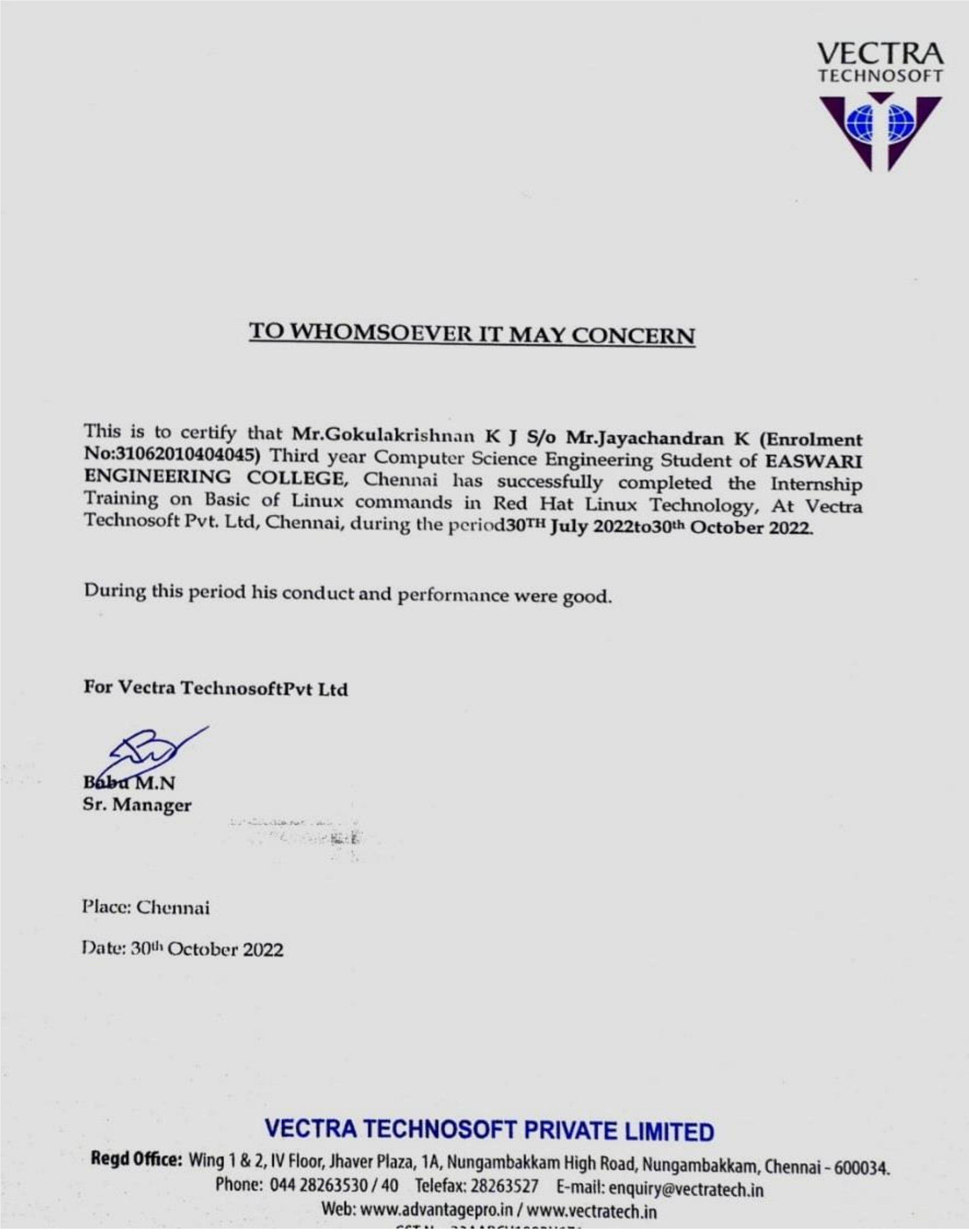
Network Vulnerabilities: Network file transfer may expose network vulnerabilities, making it easier for attackers to exploit the system. For example, attackers may use network file transfer to identify open ports or other vulnerabilities that can be used to compromise the system.

To mitigate these risks, it is recommended to use secure network protocols such as SSH or SFTP for file transfer, implement access controls, regularly update software and security patches, and perform regular backups of critical data.

1.6 CONCLUSION

In conclusion,Network file transfer in RedHat Linux can pose several risks such as unauthorized access, malware infections, data loss, data theft, and network vulnerabilities. To mitigate these risks, it is important to use secure network protocols, implement access controls, regularly update software and security patches, and perform regular backups of critical data. By taking these precautions, organizations can ensure that their network file transfers are secure and reliable.

A1 INTERNSHIP COMPLETION CERTIFICATE



VECTRA
TECHNOSOFT

TO WHOMSOEVER IT MAY CONCERN

This is to certify that **Mr.Gokulakrishnan K J S/o Mr.Jayachandran K (Enrolment No:31062010404045)** Third year Computer Science Engineering Student of **EASWARI ENGINEERING COLLEGE**, Chennai has successfully completed the Internship Training on Basic of Linux commands in Red Hat Linux Technology, At Vectra Technosoft Pvt. Ltd, Chennai, during the period**30TH July 2022to30th October 2022.**

During this period his conduct and performance were good.

For Vectra TechnosoftPvt Ltd

Babu M.N
Sr. Manager

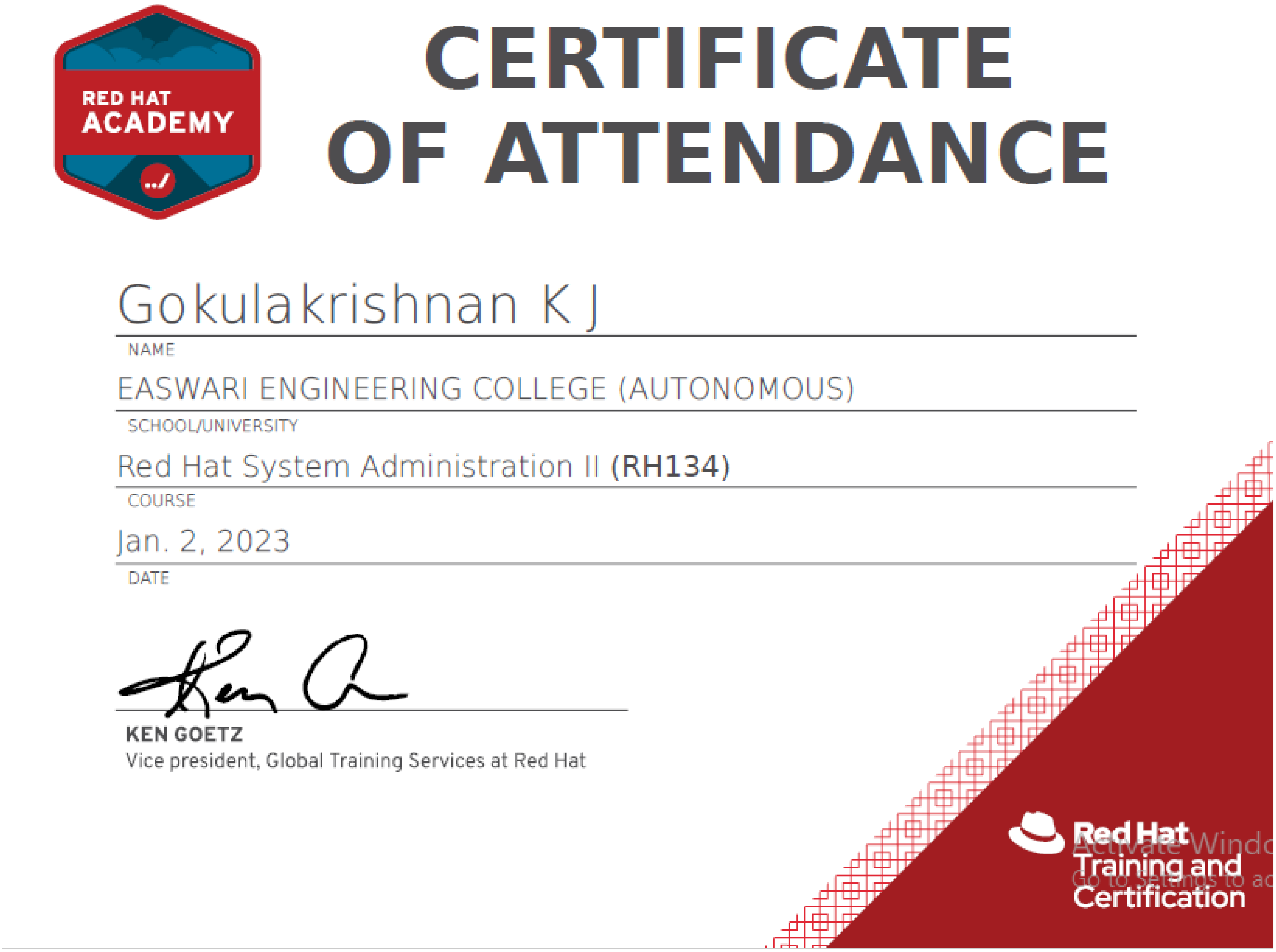
Place: Chennai

Date: 30th October 2022

VECTRA TECHNOSOFT PRIVATE LIMITED

Regd Office: Wing 1 & 2, IV Floor, Jhaver Plaza, 1A, Nungambakkam High Road, Nungambakkam, Chennai - 600034.
Phone: 044 28263530 / 40 Telefax: 28263527 E-mail: enquiry@vectratech.in
Web: www.advantagepro.in / www.vectratech.in

A2 Rhel-9 COURSE COMPLETION CERTIFICATE



RED HAT ACADEMY

CERTIFICATE OF ATTENDANCE

Gokulakrishnan K J

NAME

EASWARI ENGINEERING COLLEGE (AUTONOMOUS)

SCHOOL/UNIVERSITY

Red Hat System Administration II **(RH134)**

COURSE

Jan. 2, 2023

DATE

KEN GOETZ

Vice president, Global Training Services at Red Hat

Red Hat
Training and
Certification