Systems Administration

Year 2 // Semester 1

Project Document

Name: Katie Maher

Student Number: C00294512

Link to screencast: https://youtu.be/JgKIklXUP9E?si=FMWdkxrjYWgq6kko

INSTRUCTIONS FOR COMPLETION:

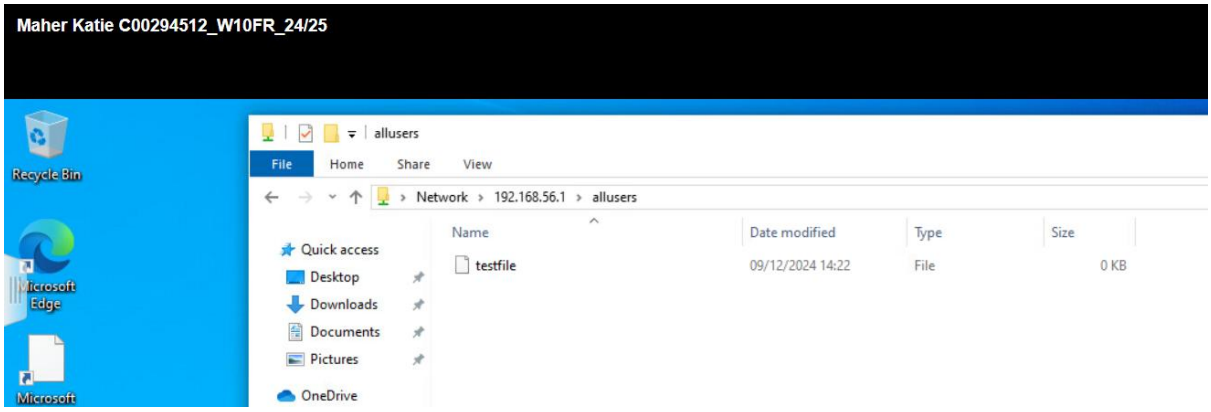
- **Rename** this document by replacing "FirstNameLastName" with your own name.
- **Enter** your name, student number, and the link to your screencast in the fields provided on pg1.
- Complete all tasks using the **labuser** account (NOT root).
- **Screenshots only**: You are not required to write detailed descriptions or step-by-step guides.
    - Paste **only relevant screenshots** for each task.
    - **Add captions** where necessary to clarify the VM, file paths, or configurations shown.
- Ensure **VM name** and **file paths** are clearly visible in screenshots. If not, include the file path or configuration location in a caption (e.g., `/etc/vsftpd/vsftpd.conf`).
- **Submit** this project document via the project submission link on Blackboard before the specified deadline.
- **Important:** Do not access or modify your virtual machines **after submitting** your document. Accessing VMs after submission may result in a grade of **zero**.

Samba Configuration and File Sharing:

In the box below, paste relevant screenshots showing:

- **Samba configuration files** after you edited them.
- Evidence that file sharing is working between the Linux Server and Windows Client, using the `allusers` shared directory.

Ensure the **VM name** is visible in the screenshots.



Maher Katie C00294512_LNXSER_24/25

```
# See smb.conf.example for a more detailed config file or
# read the smb.conf manpage.
# Run 'testparm' to verify the config is correct after
# you modified it.

[global]
        workgroup = WORKGROUP
        security = user
        netbios name = centos7
        printcap name = cups
        idmap config * : backend = tdb
        cups options = raw
        map to guest = bad user_

[homes]
        comment = Home Directories
        valid users = %S, %D%w%S
        browseable = No
        read only = No
        inherit acls = Yes

[printers]
        comment = All Printers
        path = /var/tmp
        printable = Yes
        create mask = 0600
        browseable = No

[print$]
        comment = Printer Drivers
        path = /var/lib/samba/drivers
        write list = @printadmin root
        force group = @printadmin
        create mask = 0664
        directory mask = 0775

[allusers]
        comment = needs username and password to access
        path = /samba/allusers
        valid users = @sambausergroup
        guest ok = no
        writeable = yes
```

SSH Configuration and Secure Remote Access:

In the box below, paste relevant screenshots showing:

- **SSH configuration files** after you edited them.
- Evidence that secure remote access is working between:
    - Windows Client -> Linux Server
    - Linux Client -> Linux Server

Ensure the **VM name** is visible in the screenshots.

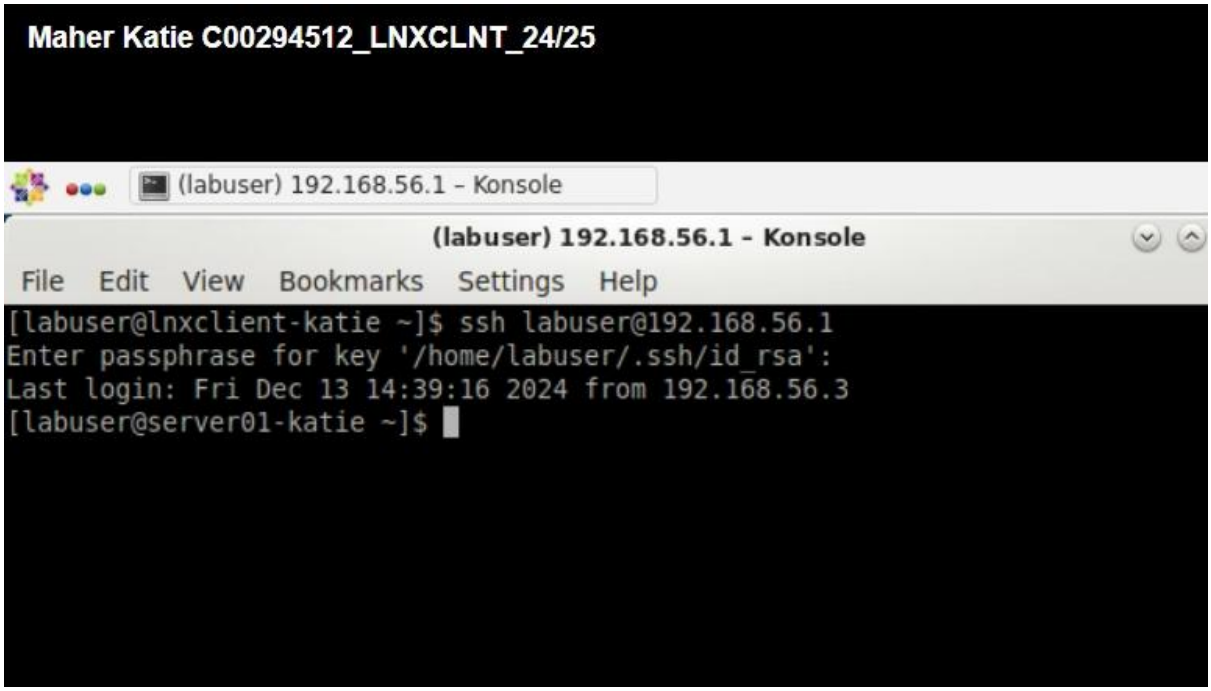
Maher Katie C00294512_LNXSER_24/25

```
#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

PubkeyAuthentication yes

# The default is to check both .ssh/authorized_keys and .ssh/authorized_keys2
# but this is overridden so installations will only check .ssh/authorized_keys
AuthorizedKeysFile      .ssh/authorized_keys

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
#PasswordAuthentication yes
#PermitEmptyPasswords no
PasswordAuthentication no

# Change to no to disable s/key passwords
#ChallengeResponseAuthentication yes
ChallengeResponseAuthentication no
```

Maher Katie C00294512_W10FR_24/25

labuser@server01-katie:~

```
Microsoft Windows [Version 10.0.19045.3930]
(c) Microsoft Corporation. All rights reserved.

C:\Users\labuser>ssh labuser@192.168.56.1
Enter passphrase for key 'C:\Users\labuser/.ssh/id_rsa':
Last login: Fri Dec 13 14:38:23 2024 from 192.168.56.3
[labuser@server01-katie ~]$
```

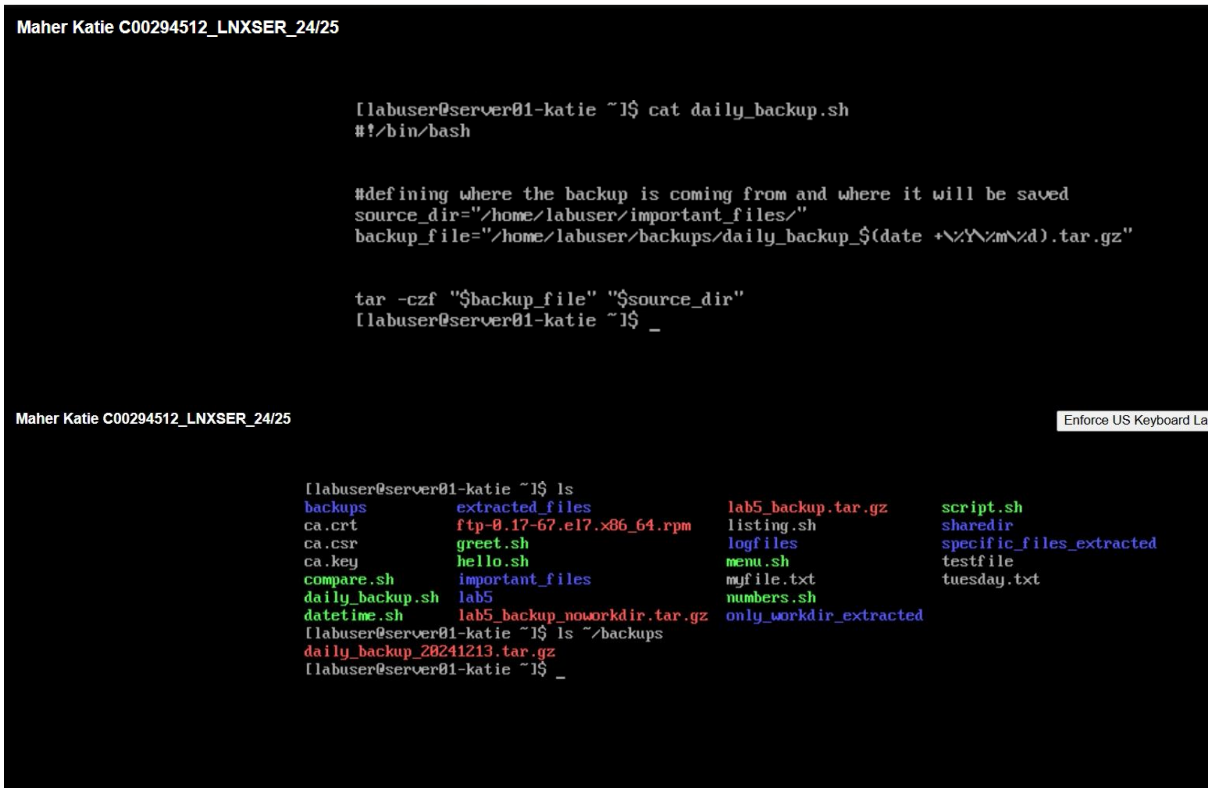


Shell Script for Task Automation:

In the box below, paste relevant screenshots showing:

- **Your BASH Shell Script** (full script).
- Evidence of the script's functionality in action (or your attempt at it).

Ensure the **VM name** is visible in the screenshots.



Miscellaneous VM Screenshots:

In the box below, paste screenshots showing the results of the following commands, per VM.

Ensure that both the command you entered and the VM name are clearly visible in each screenshot.

These screenshots should be taken after you've finished configuring your services and script.

On the Linux Server:

Command: `sudo firewall-cmd --list-all`

On the Linux Client:

Command: `sudo firewall-cmd --list-all`

Maher Katie C00294512_LNXCLNT_24/25

(labuser) 192.168.56.1 – Konsole

(labuser) 192.168.56.1 - Konsole

File Edit View Bookmarks Settings Help

```
[labuser@server01-katie ~]$ sudo firewall-cmd --list-all
[sudo] password for labuser:
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: ens192 ens224
  sources:
  services: dhcpv6-client ftp http https mountd nfs rpc-bind samba ssh
  ports: 21/tcp 80/tcp 443/tcp 2002/tcp
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:

[labuser@server01-katie ~]$
```