

CONTENTS

CLOUD SERVICES	2
SaaS (Software as a Service).....	2
Advantages of SaaS Cloud Computing.....	2
Disadvantages of SaaS Cloud Computing	3
PaaS (Platform as a Service)	3
Advantages of PaaS Cloud Computing.....	3
Disadvantages of PaaS Cloud Computing	3
IaaS (Infrastructure as a Service)	3
AWS/Azure spinning machine.....	4
STEPS.....	4
Accessing the machines via ssh/rdp.....	5
SSH.....	5
RDP	5
Deploying the web application on cloud.....	5
Using Elastic Beanstalk.....	5
Deploying the web application using EC2.....	6
Configuring the access to the application	10
Configure Access management- IAM.....	10
Top 20 Linux commands including user management/network/configuration/setting/proxy/services	16
Creative services like SMTP/FTP login and send mail/file.....	17
SMTP.....	17
Create & use App Passwords:	18
Configure SASL with Your Gmail Credentials	18
Test Sending Email from Gmail	20
FTP	21

Creative file share service and configure NFS.....	23
NFS	23
Create SMB service and configure it	27
What is SMB	27

CLOUD SERVICES

Cloud Computing often referred to as “the cloud”, in simple terms means storing or accessing your data and programs over the internet rather than your own hard drive.

Three Types of Cloude Services

- ❖ SaaS (Software as a Service)
- ❖ PaaS (Platform as a Service)
- ❖ IaaS (Infrastructure as a Service)

SaaS (Software as a Service)

In this service, the Cloud Provider leases applications or software which are owned by them to its client. The client can access this software on any device which is connected to the Internet using tools such as a web browser, an app, etc.

Example: Google Sheets as an example here. The benefits provided to the consumer include the ability to create, edit and update spreadsheets from anywhere, with multiple users able to edit at one time. But the google sheets are owned by google only, we only use these services.

Advantages of SaaS Cloud Computing

- ❖ SaaS can make you several times more productive by letting you quickly access your data anywhere, anytime.
- ❖ With SaaS, you do not have to worry about the expense of installing software on each system. Instead, you can get your business up and running at a minimal cost.

- ❖ You do not have to worry about updating your SaaS apps as they are always secure and up-to-date.

Disadvantages of SaaS Cloud Computing

- ❖ Internet connectivity is necessary if you want to use a SaaS solution.
- ❖ You do not have much control over the data you share.

PaaS (Platform as a Service)

In this service, the Cloud Provider gives the ability to the customer to deploy customer created applications using programming languages, tools, etc that are provided by the Cloud Provider. The customer cannot control the underlying architecture including operating systems, storage, servers, etc.

Example:

This service would make sense to you only if you are a developer since this service provides you a platform for developing applications, like Google App Engine, Microsoft Azure, google cloud..etc

Advantages of PaaS Cloud Computing

- ❖ With PaaS, businesses can save themselves from the complex and costly process of having to purchase and manage software licenses.
- ❖ PaaS lets developers work on applications remotely from anywhere.

Disadvantages of PaaS Cloud Computing

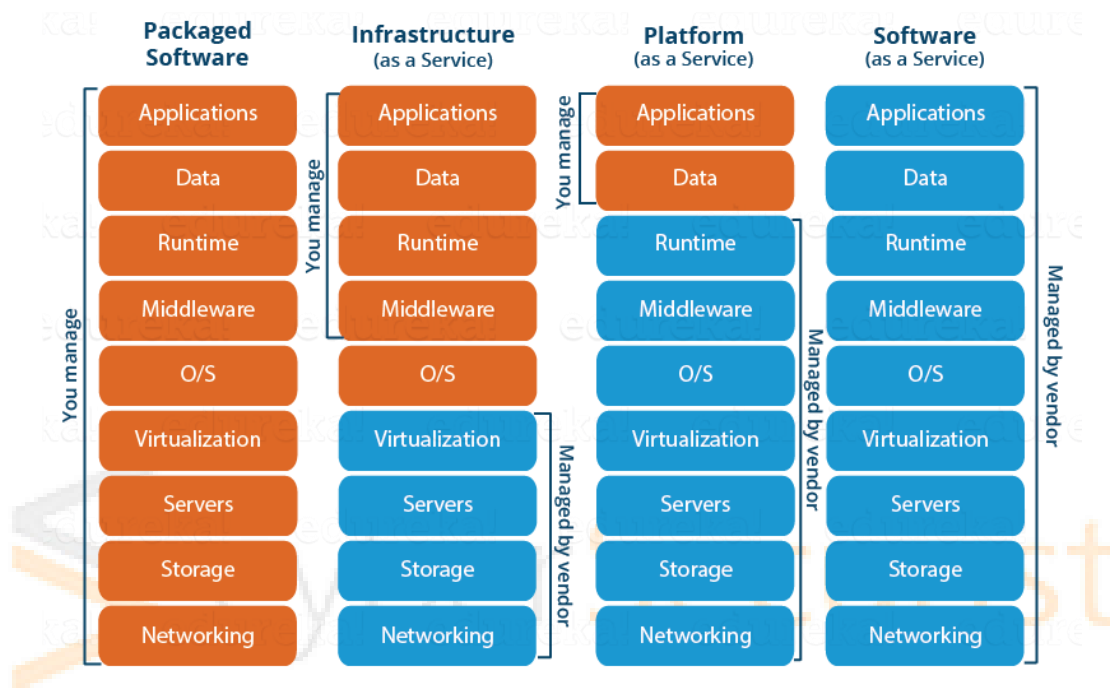
- ❖ With PaaS, you must rely heavily on the vendor for speed, support, and reliability.
- ❖ PaaS solutions are often vulnerable to data security issues.

IaaS (Infrastructure as a Service)

In this service the Cloud Provider provides the customer with virtual machines and other resources as a service, they abstract the user from

the physical machine, location, data partitioning, etc. If the user wants a Linux machine, he gets a Linux machine, he will not worry about the physical machine or the networking of the system on which the OS is installed, simple.

For Example, AWS (Amazon Web Services) is IaaS, like AWS EC2.



AWS/Azure spinning machine

STEPS

- Go to the Amazon AWS service website
- Click to the services > all services > view all services
- Choose EC2
- Launch instance
- Choose which OS you want to deploy
- Create a new key pair. Add your key pair name and click the create key pair button.
- Download it.
- Launch instance.
- You see the Successfully initiated launch of instance.
- Go to the view all instances.
- you see your current instances are running.

- Click the instance ID you will see all the details about your instance.
- Click the connect button to connect your instance.
- You can see your Instance ID, public IP Address, Username.
- Again click connect button.

Accessing the machines via ssh/rdp

SSH

Change the permission of your key, which you download

```
$ chmod 400 <key>
```

```
$ sudo ssh <username>@<IP> -I <key>
```

RDP

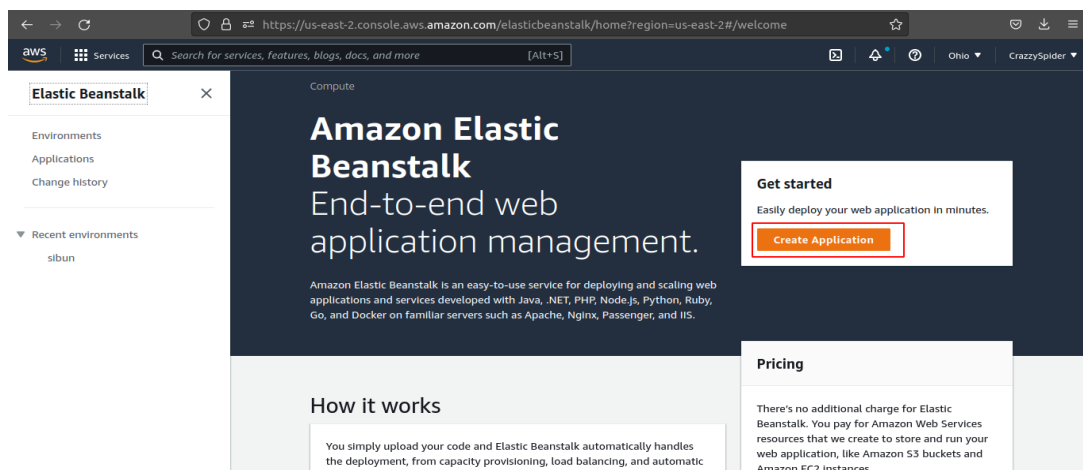
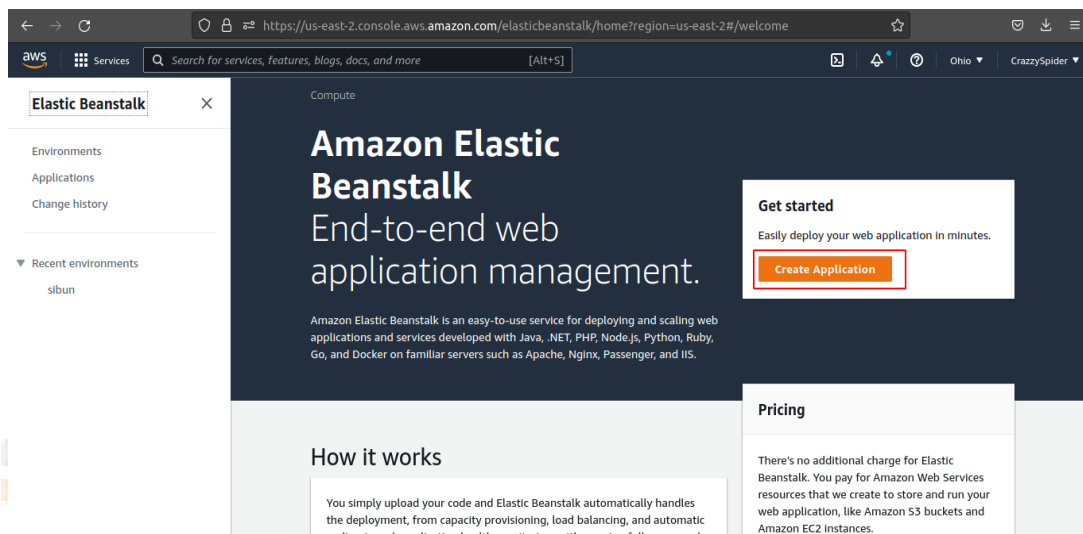
- Open Remmina
- Enter your RDP link
- Then Enter your user id and password and hit enter

Deploying the web application on cloud

Using Elastic Beanstalk

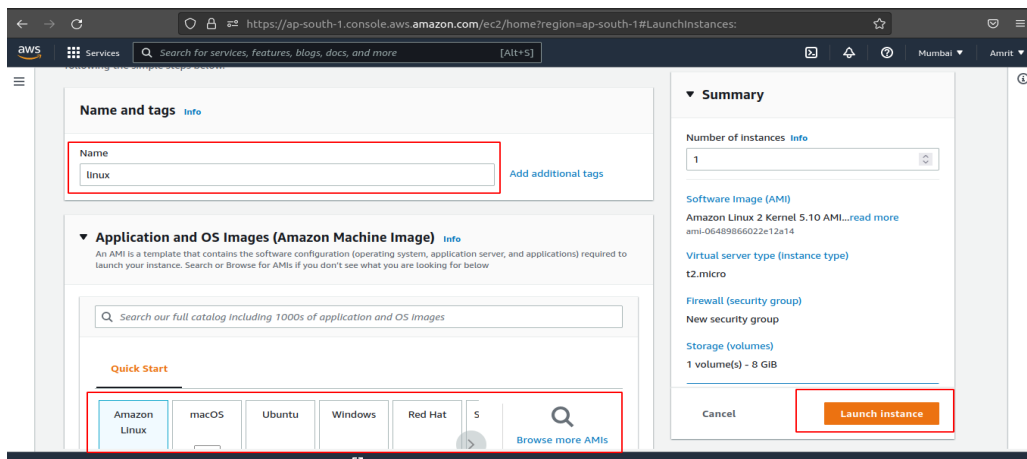
- Open AWS and search [Elastic Beanstalk](#) or click this link.
- Create application
- Add application name
- Choose Platform (like: python, docker, PHP, .NET)

- Then gives two options
- 1. Sample application
- 2. Upload your code
- Click Create application
- On the right-hand side, you see your application name, expand it.
- Click “Go to environment.”
- You see your application is ready.

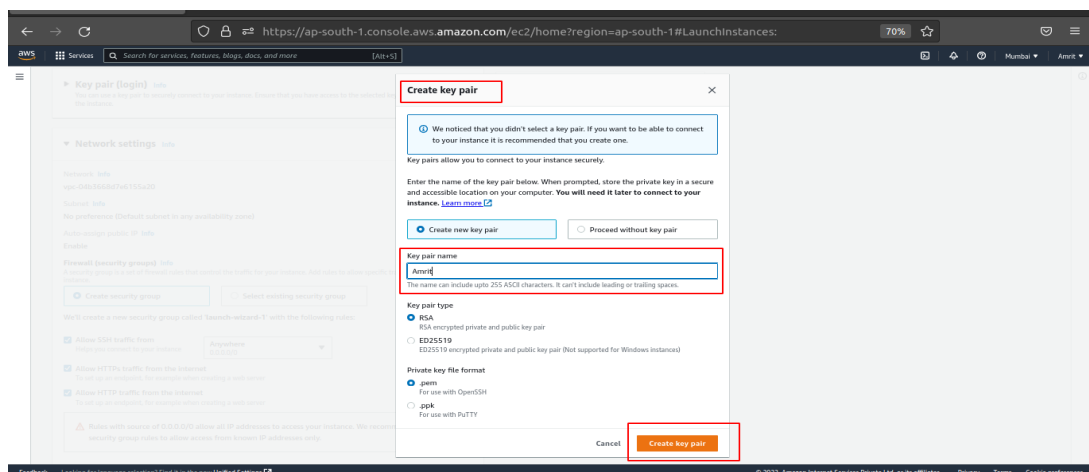


Deploying the web application using EC2

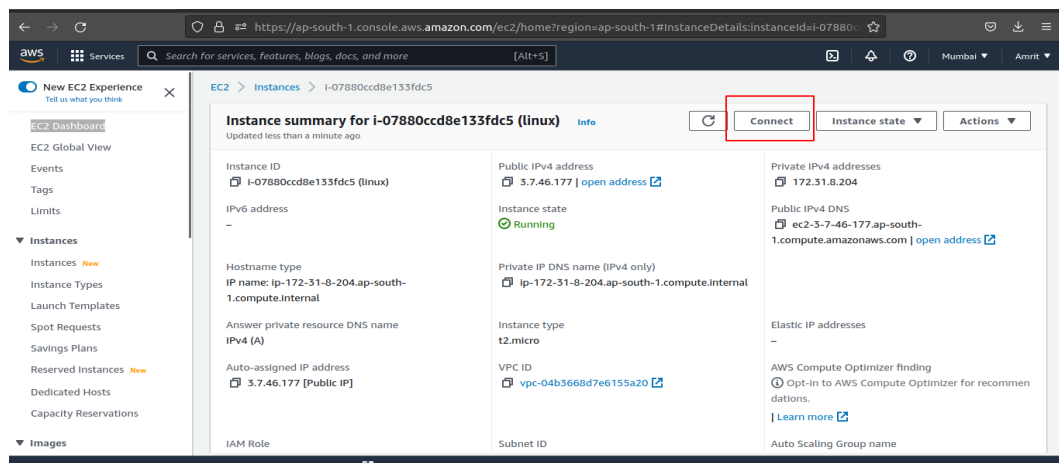
- Launch an EC2 Instance
- Choose linux machine
- Configure Instance as per your required
- Launch instance



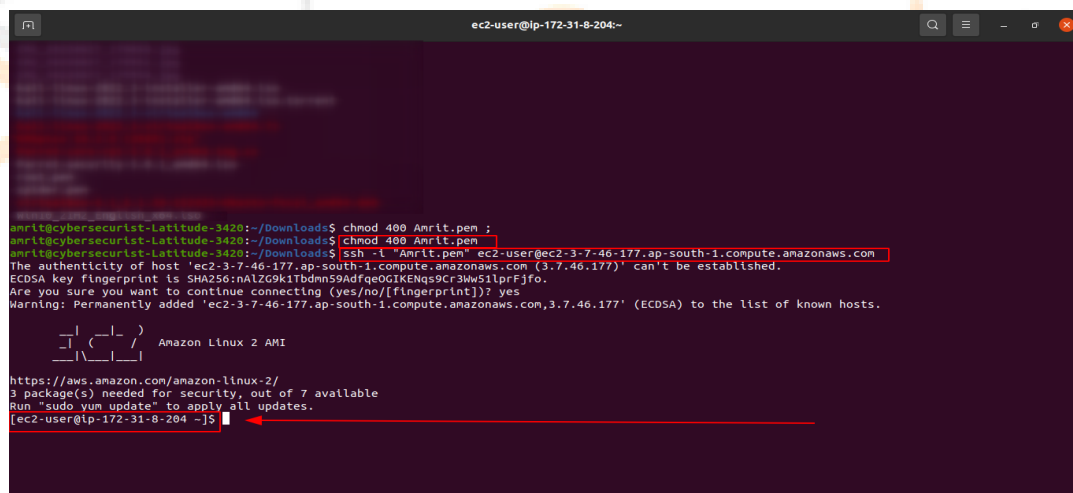
- Create key pair
- Add your key pair name
- Create key pair



- Go to the EC2 Dashboard
- See all the instances
- Click your instance and press the connect button.



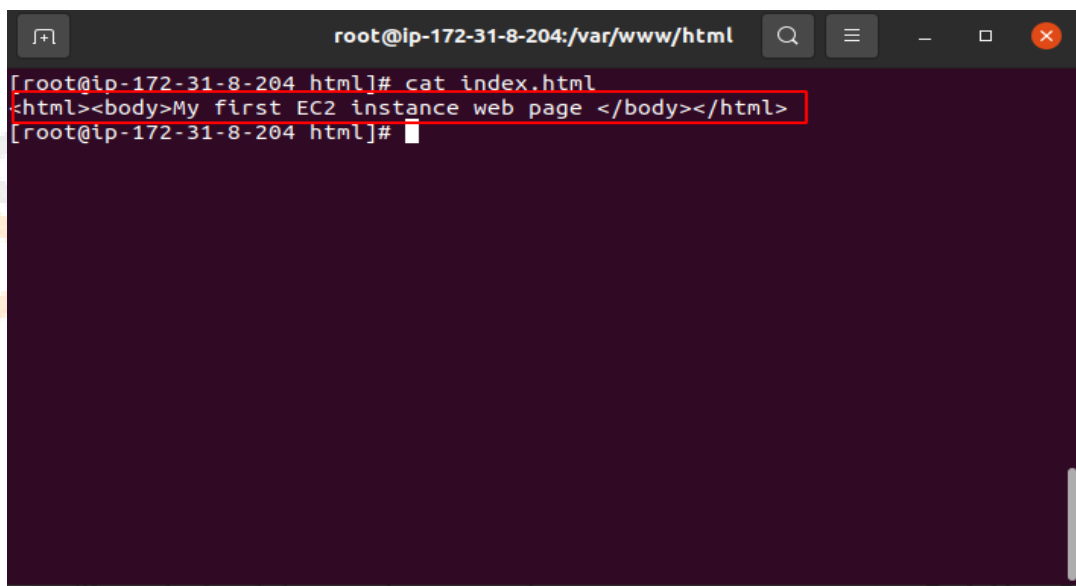
- Connect SSH to EC2
- First change the key –file permission using `chmod 400`
- Then connect using `ssh` command
- `ssh -i "Amrit.pem" ec2-user@ec2-3-7-46-177.ap-south-1.compute.amazonaws.com`



- Install an apache webserver
- `$ yum install httpd -y`
- Start the webserver
- `$ service httpd start`
- Configure the web server to restart if it gets stopped
- `$ chkconfig httpd on`

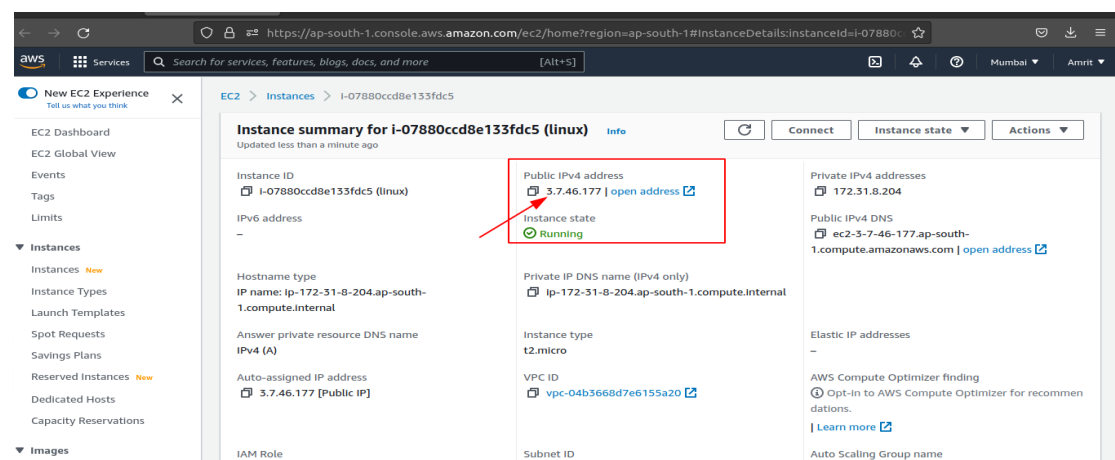
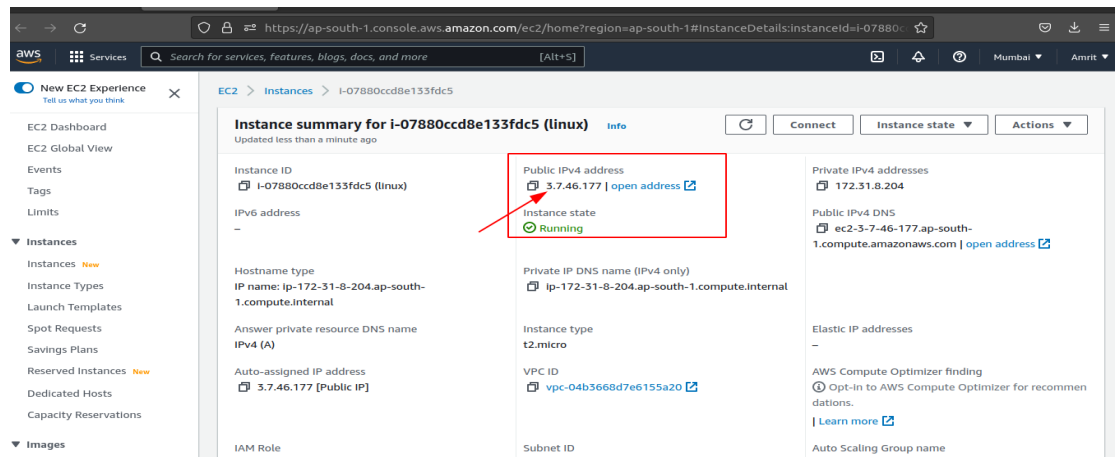
Add a static HTML file to be served

- By default, the apache web server will display the index.html file found in `/var/www/html` directory in the root path of your website.
- In this section you will create an index.html file to be served.
- Navigate to the directory
- **\$ cd /var/www/html**
- create an index.html file in this directory
- **\$ nano index.html**
- Add your HTML code
- **<html><body>My first EC2 instance web page </body></html>**

A terminal window titled 'root@ip-172-31-8-204:/var/www/html' with search, menu, and window control icons. The terminal shows the command 'cat index.html' being executed, and the output is '<html><body>My first EC2 instance web page </body></html>'. The prompt is '[root@ip-172-31-8-204 html]#'.

```
root@ip-172-31-8-204:/var/www/html
[root@ip-172-31-8-204 html]# cat index.html
<html><body>My first EC2 instance web page </body></html>
[root@ip-172-31-8-204 html]#
```

Navigate back to the EC2 dashboard in the AWS console and copy the Public DNS(IPV4) of your instance into your clipboard. Paste that address into your browser. If all went well, you will see the html that you just created!

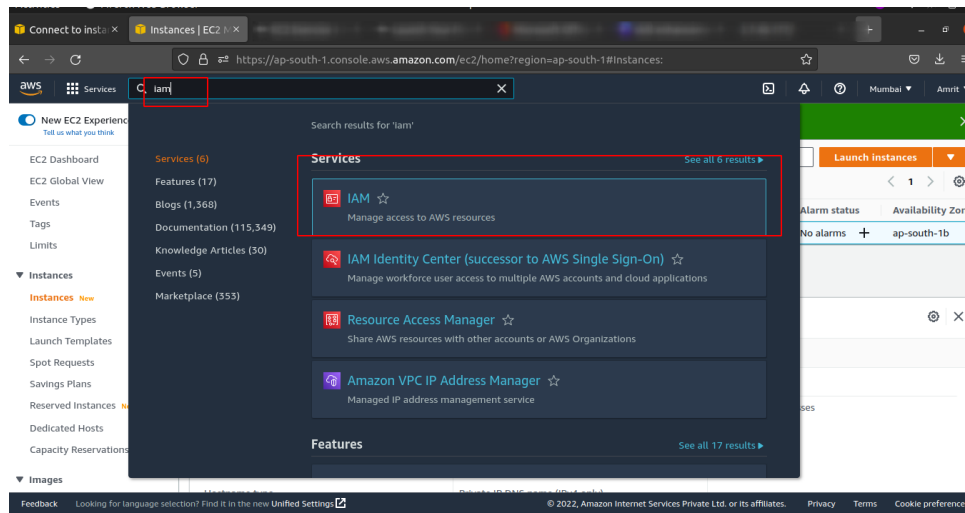


Configuring the access to the application

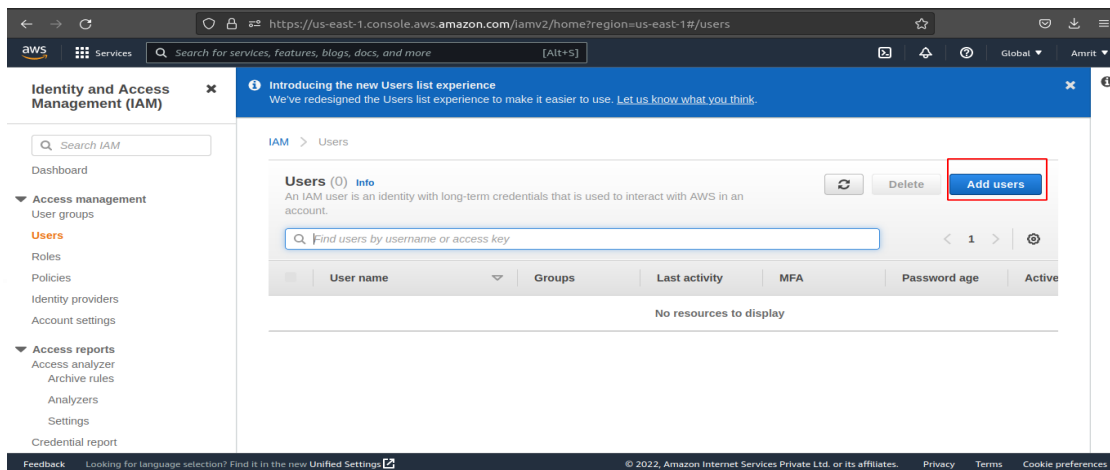
It is accessed outside the network.:)

Configure Access management- IAM

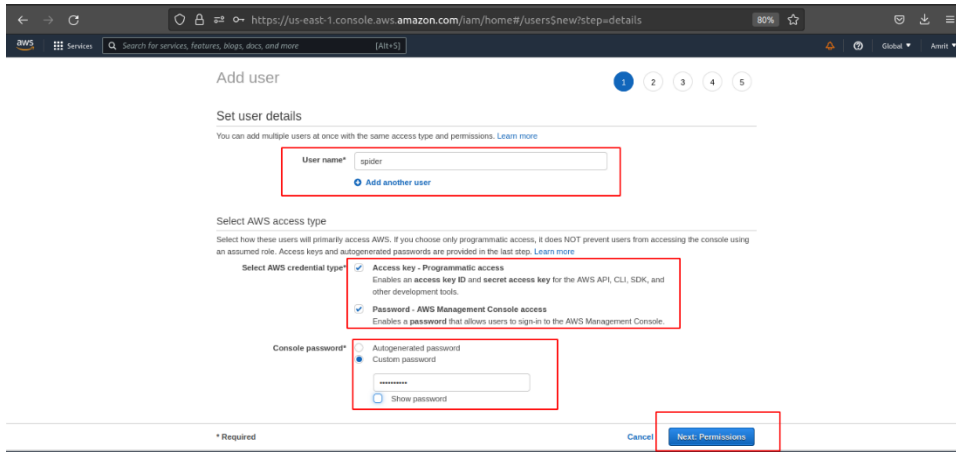
➤ Goto search and search for IAM



- IAM dashboard will open
- On the left side goto users
- Click on Add user



- Add User name
- Select AWS credential type
- Set your password
- Hit the “next permission” button



← → ↻ https://us-east-1.console.aws.amazon.com/iam/home#/users\$new/step-details 80% Global Amrit

Services Search for services, features, blogs, docs, and more [Alt+S]

Add user

1 2 3 4 5

Set user details

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name* spider
[Add another user](#)

Select AWS access type

Select how these users will primarily access AWS. If you choose only programmatic access, it does NOT prevent users from accessing the console using an assumed role. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

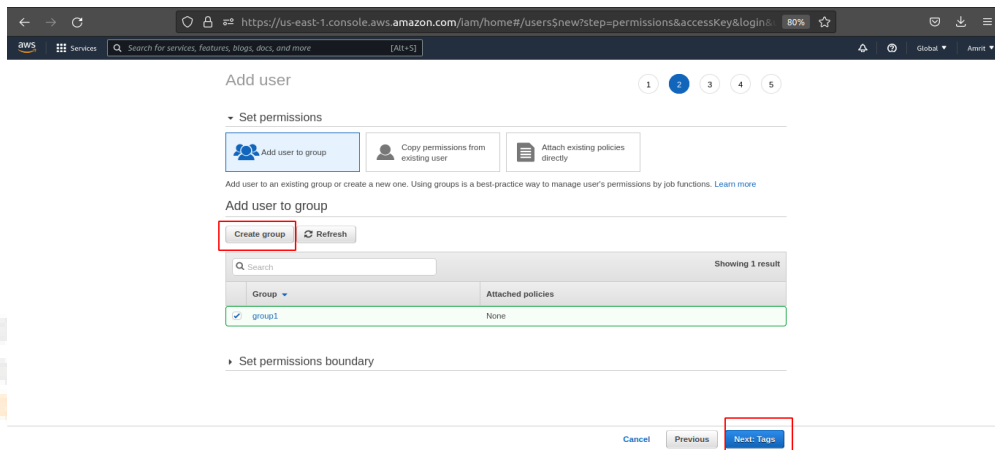
Select AWS credential type

- ☒ Access key - Programmatic access
Enables an access key ID and secret access key for the AWS API, CLI, SDK, and other development tools.
- ☒ Password - AWS Management Console access
Enables a password that allows users to sign-in to the AWS Management Console.

Console password*

- ☐ Autogenerated password
- ☒ Custom password
- ☐ Show password

* Required Cancel **Next: Permissions**



← → ↻ https://us-east-1.console.aws.amazon.com/iam/home#/users\$new/step-permissions&accessKey&login 80% Global Amrit

Services Search for services, features, blogs, docs, and more [Alt+S]

Add user

1 2 3 4 5

Set permissions

[Add user to group](#) [Copy permissions from existing user](#) [Attach existing policies directly](#)

Add user to an existing group or create a new one. Using groups is a best practice way to manage user's permissions by job functions. [Learn more](#)

Add user to group

Create group Refresh

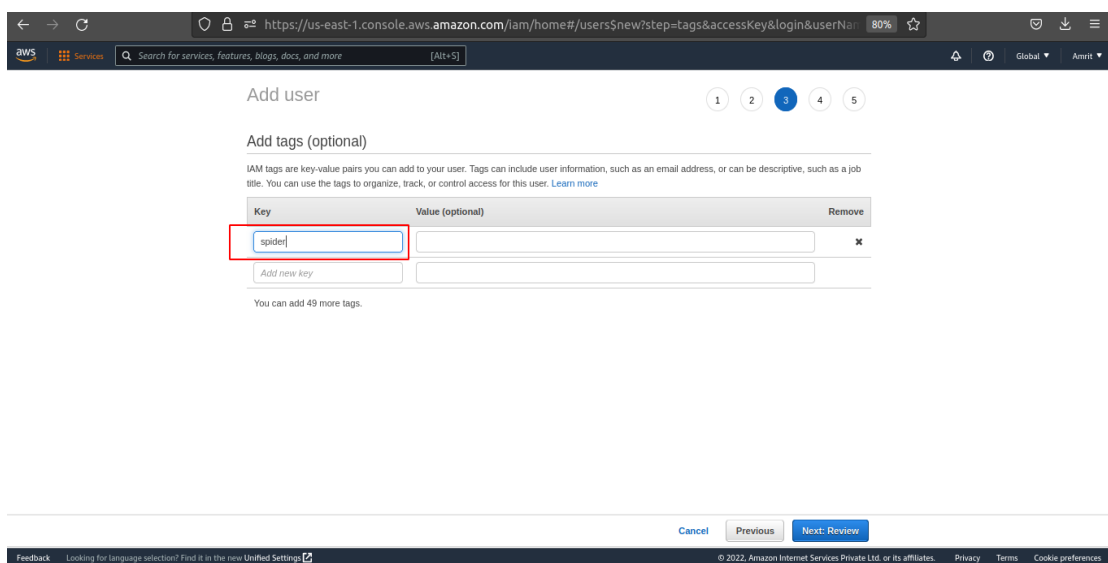
Group	Attached policies
group1	None

Showing 1 result

Set permissions boundary

Cancel Previous **Next: Tags**

➤ Then goto the user groups section



← → ↻ https://us-east-1.console.aws.amazon.com/iam/home#/users\$new/step-tags&accessKey&login&userName=spider 80% Global Amrit

Services Search for services, features, blogs, docs, and more [Alt+S]

Add user

1 2 3 4 5

Add tags (optional)

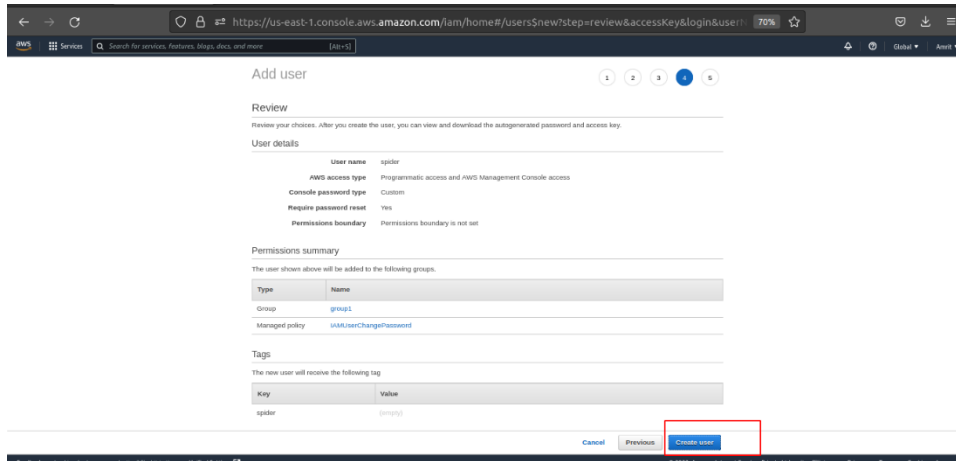
IAM tags are key-value pairs you can add to your user. Tags can include user information, such as an email address, or can be descriptive, such as a job title. You can use the tags to organize, track, or control access for this user. [Learn more](#)

Key	Value (optional)	Remove
spider		✕
Add new key		

You can add 49 more tags.

Cancel Previous **Next: Review**

Feedback Looking for language selection? Find it in the new Unified Settings [\[?\]](#) © 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences



https://us-east-1.console.aws.amazon.com/iam/home#/users\$new?step=review&accessKey&loginUser=70%

Add user

1 2 3 4 5

Review

Review your choices. After you create the user, you can view and download the autogenerated password and access key.

User details

User name	spider
AWS access type	Programmatic access and AWS Management Console access
Console password type	Custom
Require password reset	Yes
Permissions boundary	Permissions boundary is not set

Permissions summary

The user shown above will be added to the following groups.

Type	Name
Group	group1

Managed policy: [IAMUserChangePassword](#)

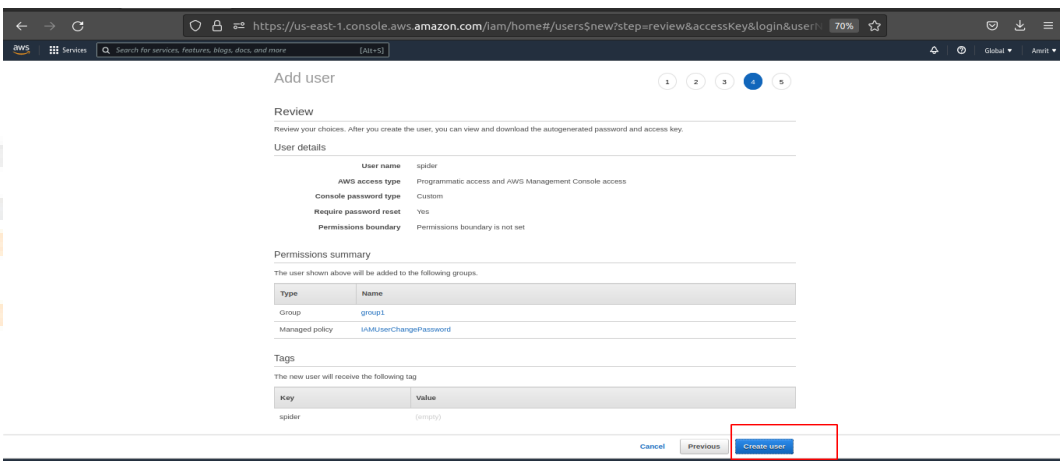
Tags

The new user will receive the following tag

Key	Value
spider	(empty)

Cancel Previous **Create user**

- Create a User Group
- Add the policies



https://us-east-1.console.aws.amazon.com/iam/home#/users\$new?step=review&accessKey&loginUser=70%

Add user

1 2 3 4 5

Review

Review your choices. After you create the user, you can view and download the autogenerated password and access key.

User details

User name	spider
AWS access type	Programmatic access and AWS Management Console access
Console password type	Custom
Require password reset	Yes
Permissions boundary	Permissions boundary is not set

Permissions summary

The user shown above will be added to the following groups.

Type	Name
Group	group1

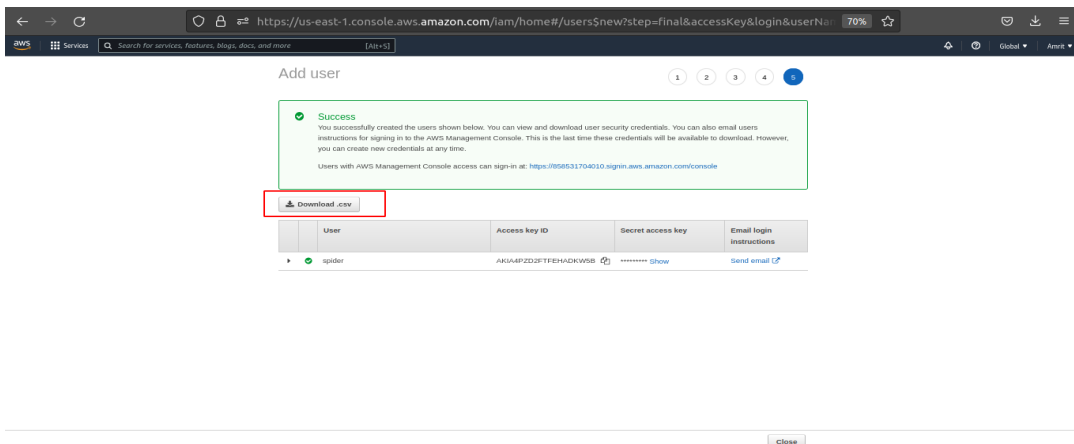
Managed policy: [IAMUserChangePassword](#)

Tags

The new user will receive the following tag

Key	Value
spider	(empty)

Cancel Previous **Create user**



https://us-east-1.console.aws.amazon.com/iam/home#/users\$new?step=final&accessKey&loginUser=70%

Add user

1 2 3 4 5

✓ SUCCESS

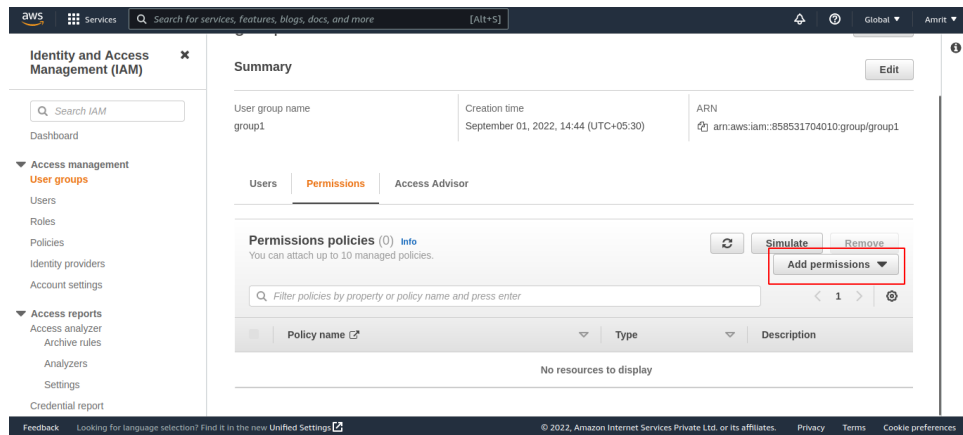
You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

Users with AWS Management Console access can sign in at: <https://868531704010.signin.aws.amazon.com/console>

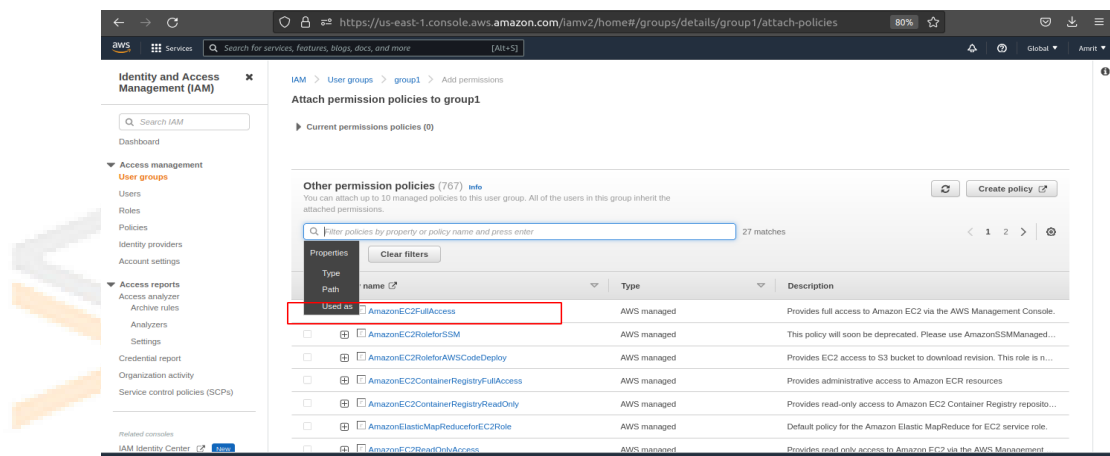
Download .csv

User	Access key ID	Secret access key	Email login instructions
spider	AKIA4PZD2FTTEHAKW5B	***** Show	Send email

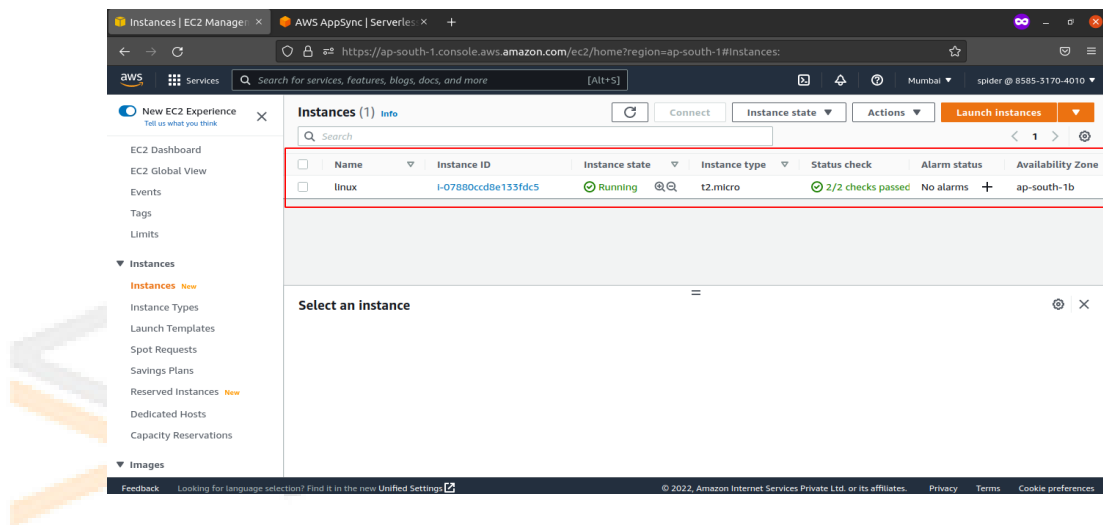
Close



- Under policies select the **AmazonEC2FullAccess**
- Add the policy



- Save
- Add the newly created user to the group
- Now logout
- Login as a IAM user
- Add the **12 digit Account ID**
- You will get this id in the root account on the right hand top corner
- Add the username and password
- Login



- ### Skill Enhancement Task:II

Top 20 Linux commands including user management/network/configuration/setting/proxy/services

- userdel
- Addgroup
- Groupdel
- Usermod

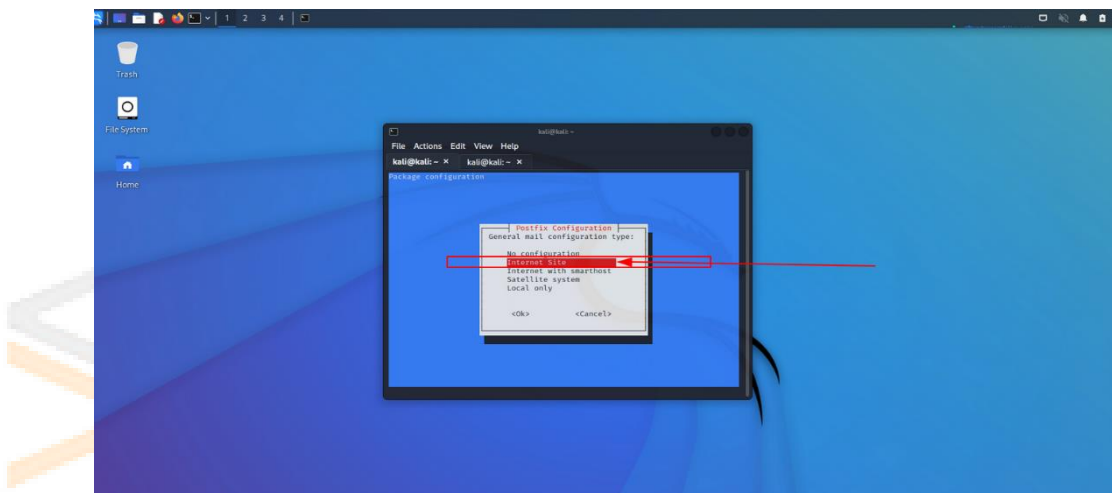
- Ifconfig
- Ping
- Netstat
- Nslookup
- arp

- Sudo service <servicename> start
- Sudo service <servicename> stop
- Sudo service <servicename> status
- Sudo service <servicename> enable
- Sudo service <servicename> disable
- Sudo systemctl enable <servicename>
- Sudo systemctl disable <servicename>
- service --status-all

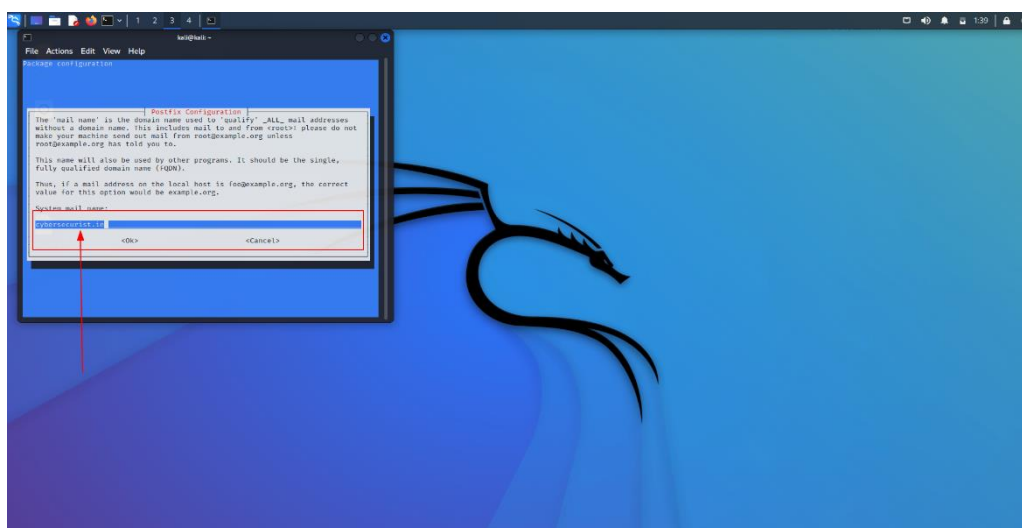
Creative services like SMTP/FTP login and send mail/file.

SMTP

- Install Postfix
- **\$ sudo apt-get install postfix**
- The first part of the Postfix installation is a text-base user interface. Use you keyboard to select *Internet Site* for the type of mail configuration.



- Then Add a Domain name :



- Before Starting you must get your **google App password**.
- Steps of Get google password:

Create & use App Passwords:

If you use [2-Step-Verification](#) and get a "password incorrect" error when you sign in, you can try to use an App Password.

1. Go to your [Google Account](#).
2. Select **Security**.
3. Under "Signing in to Google," select **App Passwords**. You may need to sign in. If you don't have this option, it might be because:
 - a. 2-Step Verification is not set up for your account.
 - b. 2-Step Verification is only set up for security keys.
 - c. Your account is through work, school, or other organization.
 - d. You turned on Advanced Protection.
4. At the bottom, choose **Select app** and choose the app you are using
➤ **Select device** and choose the device you're using ➤
Generate.
5. Follow the instructions to enter the App Password. The App Password is the 16-character code in the yellow bar on your device.
6. Tap **Done**.

Configure SASL with Your Gmail Credentials

- SASL, which stands for Simple Authentication and Security Layer, is basically what it sounds like. SASL makes it easy for applications to authenticate with various internet technologies.

- Create a the file */etc/postfix/sasl/sasl_passwd*
- And add your Gmail address and app password to it like this:

[smtp.gmail.com]:587 amritprasad55@[gmail.com:godjkozoagdmvqll](mailto:godjkozoagdmvqll@gmail.com)

- In this case, *smtp.gmail.com* is the address of the Gmail SMTP server and 587 is the SMTP port.
- Next, create a hash database file with the following postmap command.

\$ sudo postmap /etc/postfix/sasl/sasl_passwd

Note that now you will have a database file at

/etc/postfix/sasl/sasl_passwd.db

To protect the plain-text password, change the owner and permission for the SASL files as follows:

\$ sudo chown kali:kali /etc/postfix/sasl/sasl_passwd /etc/postfix/sasl/sasl_passwd.db

\$ sudo chmod 0600 /etc/postfix/sasl/sasl_passwd /etc/postfix/sasl/sasl_passwd.db

One more configuration file to edit here. To tell Postfix to use Gmail servers to send mail, set the relay value in the “**/etc/postfix/main.cf**” file.

Also, add the following to the end of “**/etc/postfix/main.cf**” to enable SASL authentication for Postfix.

```

Open  *main.cf
/etc/postfix

# line or that rate to be used as the name. the median default
6 # $ /etc/mailname.
7 myorigin = /etc/mailname
8
9 smtpd_banner = $myhostname ESMTP $mail_name (Debian/GNU)
10 biff = no
11
12 # appending .domain is the MUA's job.
13 append_dot_mydomain = no
14
15 # Uncomment the next line to generate "delayed mail" warnings
16 #delay_warning_time = 4h
17
18 readme_directory = no
19
20 # See http://www.postfix.org/COMPATIBILITY_README.html -- default to 3.6 on
21 # fresh installs.
22 compatibility_level = 3.6
23
24
25
26 # TLS parameters
27 smtpd_tls_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
28 smtpd_tls_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
29 smtpd_tls_security_level=may
30
31 smtp_tls_CApath=/etc/ssl/certs
32 smtp_tls_security_level=may
33 smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache
34
35
36 smtpd_relay_restrictions = permit_mynetworks permit_sasl_authenticated defer_unauth_destination
37 myhostname = kali
38 alias_maps = hash:/etc/aliases
39 alias_database = hash:/etc/aliases
40 myorigin = /etc/mailname
41 mydestination = $myhostname, cybersecurist.in, kali, localhost.localdomain, localhost
42 relayhost = [smtp:email.com]:587
43 mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
44 mailbox_size_limit = 0
45 recipient_delimiter = +
46 inet_interfaces = all
47 inet_protocols = all
48
49 # Enable SASL authentication
50 smtp_sasl_auth_enable = yes
51 smtp_sasl_security_options = noanonymous
52 smtp_sasl_password_maps = hash:/etc/postfix/sasl/sasl_passwd
53 smtp_tls_security_level = encrypt
54 smtp_tls_CAfile = /etc/ssl/certs/ca-certificates.crt

```

Finally, restart Postfix to apply our configuration changes.

\$ sudo systemctl restart postfix

Test Sending Email from Gmail

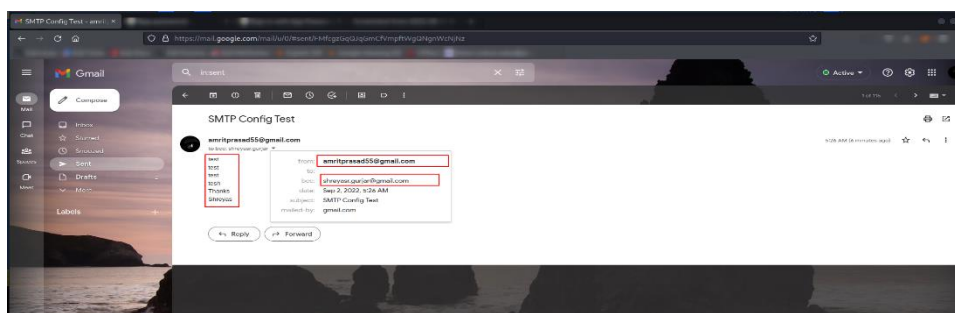
Use the *sendmail* command to send a test email.

```

(kali@kali)~[/etc/postfix/sasl]
$ sendmail shreyasr.gurjar@gmail.com
sendmail: warning: /etc/postfix/main.cf, line 53: overriding earlier entry: smtp_tls_security_level=may
postdrop: warning: /etc/postfix/main.cf, line 53: overriding earlier entry: smtp_tls_security_level=may
Subject: SMTP Config Test
test
test
test
test
test
Thanks
Shreyas

```

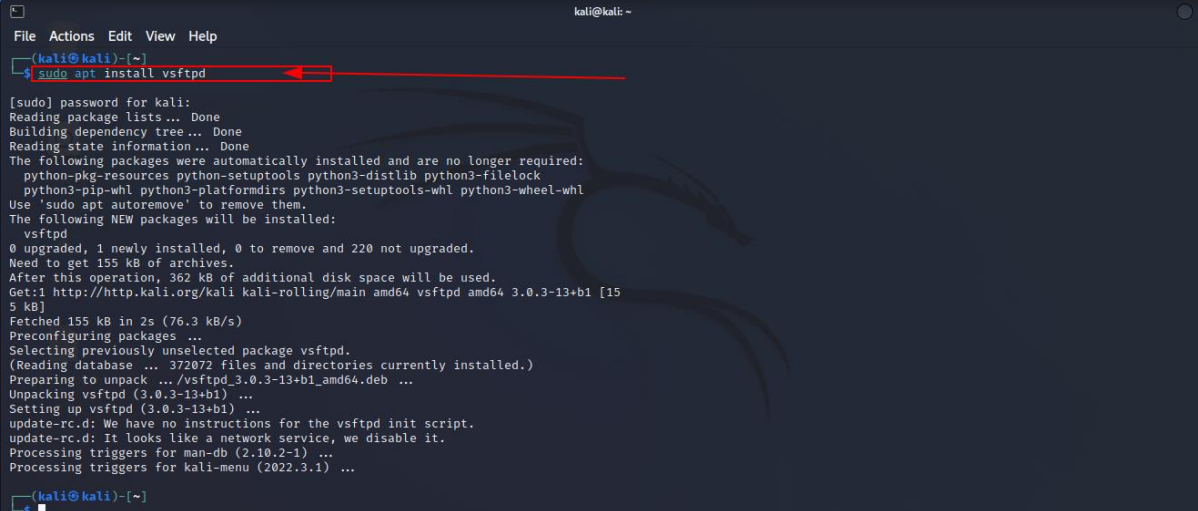
Press “CTRL + D” to send mail.



FTP

Install vsftpd in your machine

\$ sudo apt install vsftpd



```

kali@kali: ~
File Actions Edit View Help
(kali@kali)~$ sudo apt install vsftpd
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  python-pkg-resources python-setuptools python3-distlib python3-filelock
  python3-pip-whl python3-platformdirs python3-setuptools-whl python3-wheel-whl
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  vsftpd
0 upgraded, 1 newly installed, 0 to remove and 220 not upgraded.
Need to get 155 kB of archives.
After this operation, 362 kB of additional disk space will be used.
Get:1 http://http.kali.org/kali kali-rolling/main amd64 vsftpd amd64 3.0.3-13+b1 [155 kB]
Fetched 155 kB in 2s (76.3 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 372072 files and directories currently installed.)
Preparing to unpack .../vsftpd_3.0.3-13+b1_amd64.deb ...
Unpacking vsftpd (3.0.3-13+b1) ...
Setting up vsftpd (3.0.3-13+b1) ...
update-rc.d: We have no instructions for the vsftpd init script.
update-rc.d: It looks like a network service, we disable it.
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for kali-menu (2022.3.1) ...
(kali@kali)~$

```

- After install
- Enable ftp

\$ sudo systemctl enable vsftpd.service

- Start ftp

\$ sudo systemctl start vsftpd.service

- Check ftp open or not

\$ sudo systemctl start vsftpd.service

```

kali@kali: ~
File Actions Edit View Help

(kali@kali)-[~]
└─$ sudo systemctl enable vsftpd.service
Synchronizing state of vsftpd.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable vsftpd
Created symlink /etc/systemd/system/multi-user.target.wants/vsftpd.service → /lib/systemd/system/vsftpd.service.

(kali@kali)-[~]
└─$ sudo systemctl start vsftpd.service

(kali@kali)-[~]
└─$ nmap localhost
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-05 01:25 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000066s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds

(kali@kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.68 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::cd20:c3ef:246c:prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:22:46:4f txqueuelen 1000 (Ethernet)
    RX packets 1043 bytes 240714 (235.0 KiB)
    RX errors 0 dropped 7 overruns 0 frame 0

```

- Connect to the ftp service using host machine

\$ ftp <\$IP>

- Enter your user name and password

```

amrit@cybersecurist-Latitude-3420:~/Downloads$ ftp 192.168.1.68
Connected to 192.168.1.68.
220 (vsFTPd 3.0.3)
Name (192.168.1.68:amrit): kali
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>

```

Creative file share service and configure NFS

NFS

- Install the nfs server

\$ sudo apt install nfs-kernel-server

```
(kali@kali)~$ sudo apt install nfs-kernel-server
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  python-pkg-resources python-setuptools python3-distlib python3-filelock python3-pip-whl python3-platformdirs python3-setuptools-whl python3-wheel-whl
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  nfs-kernel-server
0 upgraded, 1 newly installed, 0 to remove and 220 not upgraded.
Need to get 180 kB of archives.
After this operation, 651 kB of additional disk space will be used.
Ign:1 http://http.kali.org/kali kali-rolling/main amd64 nfs-kernel-server amd64 1:2.6.1-2
Ign:1 http://http.kali.org/kali kali-rolling/main amd64 nfs-kernel-server amd64 1:2.6.1-2
Get:1 http://kali.download/kali kali-rolling/main amd64 nfs-kernel-server amd64 1:2.6.1-2 [180 kB]
Fetched 180 kB in 1min 6s (2,723 B/s)
Selecting previously unselected package nfs-kernel-server.
(Reading database ... 372131 files and directories currently installed.)
Preparing to unpack .../nfs-kernel-server_1:2.6.1-2_amd64.deb ...
Unpacking nfs-kernel-server (1:2.6.1-2) ...
Setting up nfs-kernel-server (1:2.6.1-2) ...
nfs-blkmap.service is a disabled or a static unit not running, not starting it.
nfs-mountd.service is a disabled or a static unit not running, not starting it.
nfs-server.service is a disabled or a static unit not running, not starting it.
nfsdclld.service is a disabled or a static unit not running, not starting it.

Creating config file /etc/exports with new version
Creating config file /etc/default/nfs-kernel-server with new version
update-rc.d: We have no instructions for the nfs-kernel-server init script
```

- Make a directory

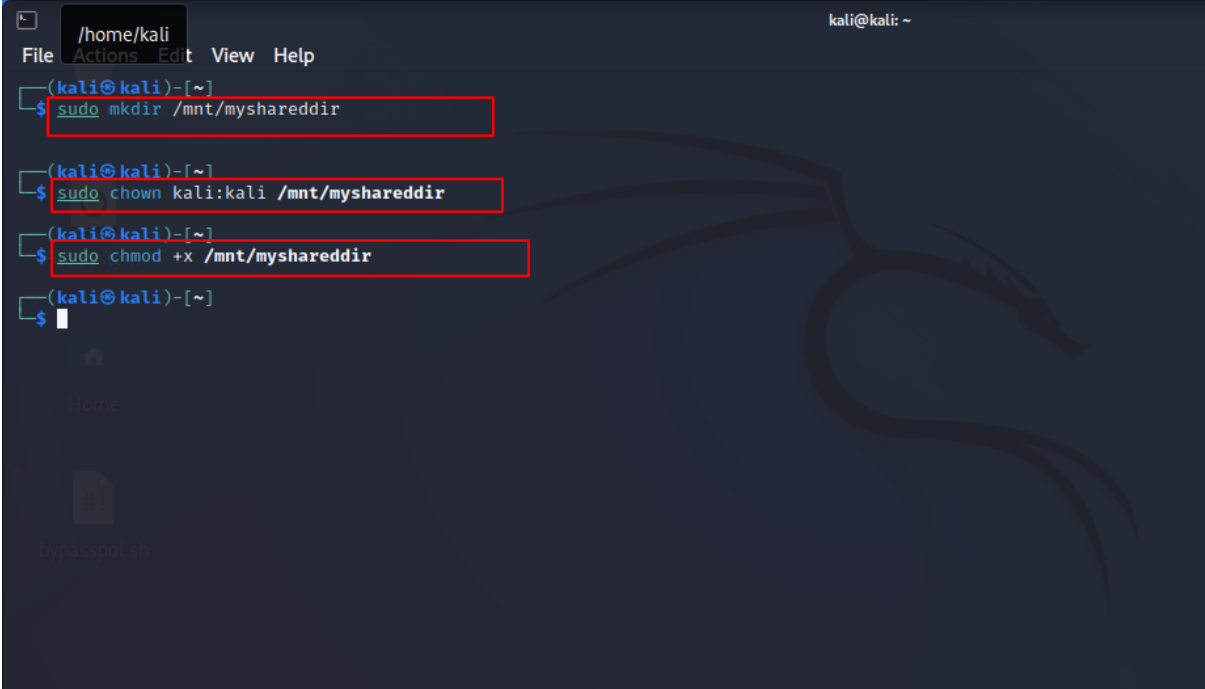
\$ sudo mkdir /mnt/mysharedir

- Give owner permission

\$ sudo chown kali:kali /mnt/mysharedir

- Give the permission to the directory

\$ sudo chmod +x /mnt/mysharedir



```

kali@kali: ~
File Actions Edit View Help
(kali@kali)~]
$ sudo mkdir /mnt/myshareddir
(kali@kali)~]
$ sudo chown kali:kali /mnt/myshareddir
(kali@kali)~]
$ sudo chmod +x /mnt/myshareddir
(kali@kali)~]
$

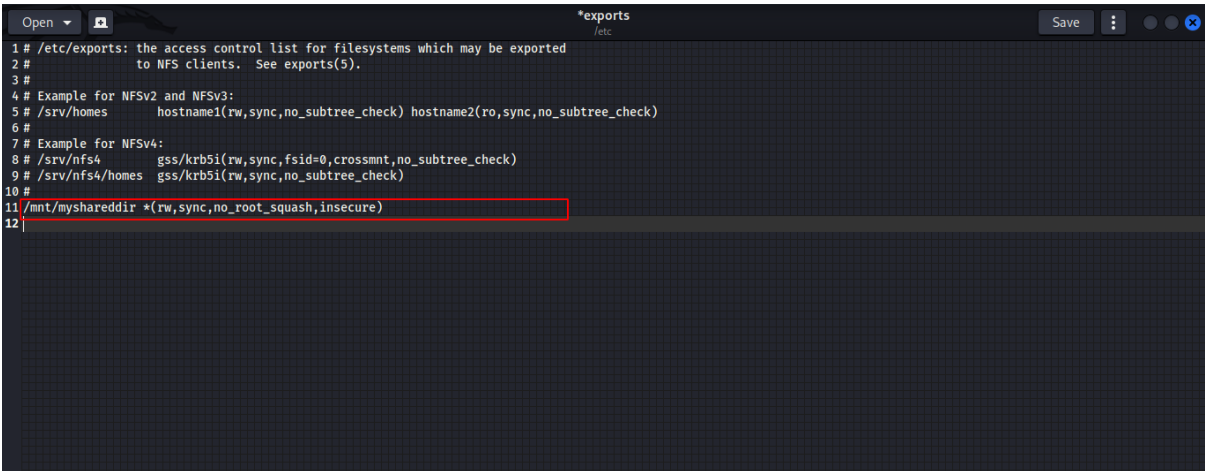
```

➤ Edit the exports file

\$ sudo gedit /etc/exports

➤ Add the following line

/mnt/myshareddir *(rw,sync,no_root_squash,insecure)



```

*exports
/etc
1 # /etc/exports: the access control list for filesystems which may be exported
2 # to NFS clients. See exports(5).
3 #
4 # Example for NFSv2 and NFSv3:
5 # /srv/homes hostname1(rw,sync,no_subtree_check) hostname2(ro,sync,no_subtree_check)
6 #
7 # Example for NFSv4:
8 # /srv/nfs4 gss/krb5i(rw,sync,fsid=0,crossmnt,no_subtree_check)
9 # /srv/nfs4/homes gss/krb5i(rw,sync,no_subtree_check)
10 #
11 /mnt/myshareddir *(rw,sync,no_root_squash,insecure)
12

```


- Make the file share available

\$ sudo exportfs -a

- Connect to the NFS server using the client machine

- Install the following package

\$ sudo apt install nfs-common

```
amrit@cybersecurist-Latitude-3420:~$ sudo apt install nfs-common
[sudo] password for amrit:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  dctrl-tools dkms libgsoap-2.8.91 liblzf1 libvncserver1 linux-image-5.14.0-1048-oem linux-modules-5.14.0-1048-oem
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  keyutils libnfsidmap2 libtirpc-common libtirpc3 rpcbind
Suggested packages:
  open-iscsi watchdog
The following NEW packages will be installed:
  keyutils libnfsidmap2 libtirpc-common libtirpc3 nfs-common rpcbind
0 upgraded, 6 newly installed, 0 to remove and 18 not upgraded.
Need to get 405 kB of archives.
After this operation, 1,519 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://in.archive.ubuntu.com/ubuntu focal-updates/main amd64 libtirpc-common all 1.2.5-1ubuntu0.1 [7,712 B]
Get:2 http://in.archive.ubuntu.com/ubuntu focal-updates/main amd64 libtirpc3 amd64 1.2.5-1ubuntu0.1 [77.9 kB]
Get:3 http://in.archive.ubuntu.com/ubuntu focal/main amd64 rpcbind amd64 1.2.5-8 [42.8 kB]
Get:4 http://in.archive.ubuntu.com/ubuntu focal-updates/main amd64 keyutils amd64 1.6-6ubuntu1.1 [44.8 kB]
Get:5 http://in.archive.ubuntu.com/ubuntu focal/main amd64 libnfsidmap2 amd64 0.25-5.1ubuntu1 [27.9 kB]
Get:6 http://in.archive.ubuntu.com/ubuntu focal-updates/main amd64 nfs-common amd64 1:1.3.4-2.5ubuntu3.4 [204 kB]
Fetched 405 kB in 4s (112 kB/s)
Selecting previously unselected package libtirpc-common.
(Reading database ... 222362 files and directories currently installed.)
Preparing to unpack .../0-libtirpc-common_1.2.5-1ubuntu0.1_all.deb ...
Unpacking libtirpc-common (1.2.5-1ubuntu0.1) ...
Selecting previously unselected package libtirpc3:amd64.
Preparing to unpack .../1-libtirpc3_1.2.5-1ubuntu0.1_amd64.deb ...
Unpacking libtirpc3:amd64 (1.2.5-1ubuntu0.1) ...
Selecting previously unselected package rpcbind.
Preparing to unpack .../2-rpcbind_1.2.5-8_amd64.deb ...
Unpacking rpcbind (1.2.5-8) ...
Setting up libtirpc-common (1.2.5-1ubuntu0.1) ...
Setting up libtirpc3:amd64 (1.2.5-1ubuntu0.1) ...
Setting up rpcbind (1.2.5-8) ...
Setting up nfs-common (1:1.3.4-2.5ubuntu3.4) ...
Setting up keyutils (1.6-6ubuntu1.1) ...
Setting up libnfsidmap2:amd64 (0.25-5.1ubuntu1) ...
```

- Create a local directory this will be the mount point for the NFS share.

\$ sudo mkdir /var/locally-mounted

- Mount the file share by running the mount command.

\$ sudo mount -t nfs 192.168.1.68:/mnt/mysharedir /var/locally-mounted/

```

amrit@cybersecurist-Latitude-3420:~$ sudo mkdir /var/locally-mounted
[sudo] password for amrit:
amrit@cybersecurist-Latitude-3420:~$ ifconfig
enp4s50: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    ether 00:be:43:37:0c:ed txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 24996 bytes 2795427 (2.7 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 24996 bytes 2795427 (2.7 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlp44s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.80 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::3920:e25b:d5e2:ee47 prefixlen 64 scopeid 0x20<link>
    ether c8:94:02:dc:a7:0f txqueuelen 1000 (Ethernet)
    RX packets 211218 bytes 196254514 (196.2 MB)
    RX errors 0 dropped 878 overruns 0 frame 0
    TX packets 110744 bytes 41539834 (41.5 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

amrit@cybersecurist-Latitude-3420:~$ sudo mount -t nfs 192.168.1.80:/mnt/mysharedir /var/locally-mounted/
mount.nfs: requested NFS version or transport protocol is not supported
amrit@cybersecurist-Latitude-3420:~$ sudo mount -t nfs 192.168.1.68:/mnt/mysharedir /var/locally-mounted/
mount.nfs: access denied by server while mounting 192.168.1.68:/mnt/mysharedir
amrit@cybersecurist-Latitude-3420:~$ sudo mount -t nfs 192.168.1.68:/mnt/mysharedir /var/locally-mounted/
amrit@cybersecurist-Latitude-3420:~$

```

- Folder will be mounted
- To check if it is mounted or not enter

\$ df -h

```

amrit@cybersecurist-Latitude-3420:~$ df -h

```

Filesystem	Size	Used	Avail	Use%	Mounted on
udev	7.7G	0	7.7G	0%	/dev
tmpfs	1.6G	2.2M	1.6G	1%	/run
/dev/nvme0n1p2	468G	92G	353G	21%	/
tmpfs	7.7G	0	7.7G	0%	/dev/shm
tmpfs	5.0M	4.0K	5.0M	1%	/run/lock
tmpfs	7.7G	0	7.7G	0%	/sys/fs/cgroup
/dev/loop0	128K	128K	0	100%	/snap/bare/5
/dev/loop1	56M	56M	0	100%	/snap/core18/2128
/dev/loop2	56M	56M	0	100%	/snap/core18/2538
/dev/loop3	219M	219M	0	100%	/snap/gnome-3-34-1804/72
/dev/loop4	62M	62M	0	100%	/snap/core20/1611
/dev/loop6	92M	92M	0	100%	/snap/gtk-common-themes/1535
/dev/loop5	219M	219M	0	100%	/snap/gnome-3-34-1804/77
/dev/loop8	51M	51M	0	100%	/snap/snap-store/547
/dev/loop12	66M	66M	0	100%	/snap/gtk-common-themes/1515
/dev/loop9	55M	55M	0	100%	/snap/snap-store/558
/dev/loop7	47M	47M	0	100%	/snap/snapd/16292
/dev/loop10	401M	401M	0	100%	/snap/gnome-3-38-2004/112
/dev/loop11	347M	347M	0	100%	/snap/gnome-3-38-2004/115
/dev/nvme0n1p1	511M	5.3M	506M	2%	/boot/efi
tmpfs	1.6G	72K	1.6G	1%	/run/user/1001
192.168.1.68:/mnt/mysharedir	79G	19G	56G	25%	/var/locally-mounted

- Now goto the newly created directory **/var/locally-mounted**

\$ Cd /var/locally-mounted

- All the files and subdirectories will be listed there

```

amrit@cybersecurist-Latitude-3420:~$ cd /var/locally-mounted/
amrit@cybersecurist-Latitude-3420:/var/locally-mounted$ ls
test1.txt
amrit@cybersecurist-Latitude-3420:/var/locally-mounted$ cat test1.txt
hello
amrit@cybersecurist-Latitude-3420:/var/locally-mounted$

```

Create SMB service and configure it

What is SMB

The SMB (Server Message Block) protocol provides for “client-server communication,” which allows programs and services on networked computers to communicate with one another. File, print, and device sharing are just a few of the network functions enabled by SMB.

- Install Samba in your os

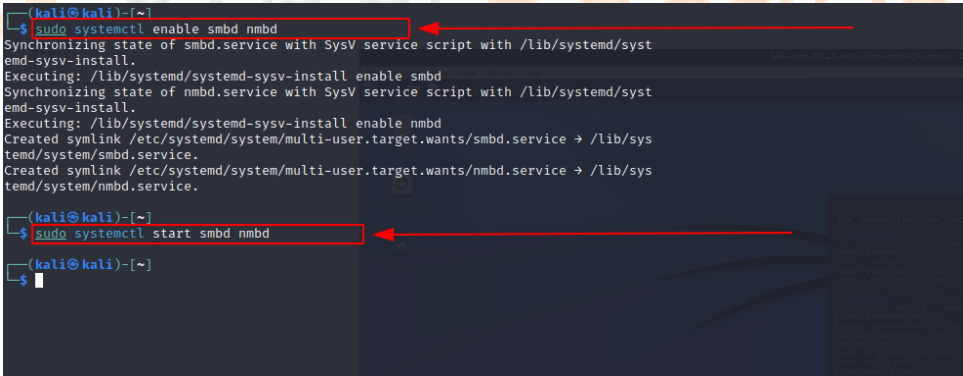
\$ sudo apt install -y samba

- Enable “smbd” & “nmbd”

\$ sudo systemctl enable smbd nmbd

- Start “smbd” & “nmbd”

\$ sudo systemctl start smbd nmbd



```
(kali@kali)~$ sudo systemctl enable smbd nmbd
Synchronizing state of smbd.service with SysV service script with /lib/systemd/sy
emd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable smbd
Synchronizing state of nmbd.service with SysV service script with /lib/systemd/sy
emd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable nmbd
Created symlink /etc/systemd/system/multi-user.target.wants/smbd.service → /lib/sy
temd/system/smbd.service.
Created symlink /etc/systemd/system/multi-user.target.wants/nmbd.service → /lib/sy
temd/system/nmbd.service.

(kali@kali)~$ sudo systemctl start smbd nmbd
(kali@kali)~$
```

Add user access to samba with pdbedit. This user must be exists in Linux. If user to be added by pdbedit does not exist, you need to add user with useradd.

\$ sudo useradd -m kali

Set your user password

\$ sudo pdbedit -a kali

```
(kali@kali)-[~]
$ sudo useradd -m kali
useradd: user 'kali' already exists

(kali@kali)-[~]
$ sudo pdbedit -a kali
new password:
retype new password:
Unix username: kali
Vn username:
Account Flags: [U]
User SID: S-1-5-21-1199429804-2376867058-1184872169-1000
Primary Group SID: S-1-5-21-1199429804-2376867058-1184872169-513
Full Name:
Home Directory: \\KALI\kali
HomeDir Drive:
Logon Script:
Profile Path: \\KALI\kali\profile
Domain: KALI
Account desc:
Workstations:
Munged dial:
Logon time:
Logoff time: Wed, 06 Feb 2036 10:06:39 EST
Kickoff time: Wed, 06 Feb 2036 10:06:39 EST
Password last set: Fri, 02 Sep 2022 06:37:20 EDT
Password can change: Fri, 02 Sep 2022 06:37:20 EDT
Password must change: never
Last bad password: 0
Bad password count: 0
Logon hours: FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

(kali@kali)-[~]
$
```

- Edit the configuration file

sudo gedit /etc/samba/smb.conf

- Add the following code at the bottom

[share]

path = /home/kali/Share/

browseable = yes

read only = no



```
207 # (you need to configure samba to act as a domain controller too.)
208 [netlogon]
209 # comment = Network Logon Service
210 path = /home/samba/netlogon
211 guest ok = yes
212 read only = yes
213
214 # (you need to configure samba to act as a domain controller too.)
215 # The path below should be writable by all users so that their
216 # profile directory may be created the first time they log on
217 [profiles]
218 # comment = Users profiles
219 path = /home/samba/profiles
220 guest ok = no
221 browseable = no
222 create mask = 0600
223 directory mask = 0700
224
225 [printers]
226 # comment = All Printers
227 browseable = no
228 path = /var/spool/samba
229 printable = yes
230 guest ok = no
231 read only = yes
232 create mask = 0700
233
234 # Windows clients look for this share name as a source of downloadable
235 # printer drivers
236 [print$]
237 # comment = Printer Drivers
238 path = /var/lib/samba/printers
239 browseable = yes
240 read only = yes
241 guest ok = no
242 # Uncomment to allow remote administration of Windows print drivers.
243 # You may need to replace 'lpadmin' with the name of the group you
244 # admin users are members of.
245 # Please note that you also need to set appropriate Unix permissions
246 # to the drivers directory for these users to have write rights in it
247 write list = root, lpadmin
248
249 [share]
250 path = /home/kali/Share/
251 browseable = yes
252 read only = no
253
```

Save it and exit

- Goto the home directory and **create a folder Share**
- Give permission to it

\$ chmod +x Share

- Restart the smb service

\$sudo service smb start

\$sudo service nmbd start

- Set the smb password

\$ sudo smbpasswd -a kali

- Connect to it using windows or linux machine

Smb://<\$ip>/<file name>

For linux goto the file **Explorer below > Other Locations**

Below there is a bar where it says **connect to the server**

