Setup LXC – Kali Linux Container

Index :

Reference :

LXC : https://linuxcontainers.org/lxc/introduction
Kali Linux – LXC : https://www.kali.org/docs/containers/kalilinux-lxc-images
LXC-Incus : https://linuxcontainers.org/incus/introduction
LXC-LXD : https://documentation.ubuntu.com/lxd/en/latest
Explainshell : https://explainshell.com

A word of Advice :

- Try at your own risk
- Try it inside a Virtual Machine first, if it works try it on your HOST machine
- Content Owner is not responsibile for any data loss or system breaks
- All the commands are safe to use, if you have doubts on a command try Googling or use AI to explain or use Explain shell
- Not all tools in kali linux are tested – they may not work properly

Note :

- The following methods works properly with X11/Xorg Envronment
- This will not work with wayland Desktop

Why LXC :

LXC is light weight and less resource hungry than a Virtual Machine
LXC will run a full system and not like DOCKER or PODMAN

This Document is for Educational Purpose

1. Setup Kali Linux LXC container

- Install the container using command :

```
sudo apt install lxc
```

```
:~$ sudo apt install lxc bridge-utils
[sudo] password for
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
lxc is already the newest version (1:5.0.2-1+deb12u2).
bridge-utils is already the newest version (1.7.1-1).
0 upgraded, 0 newly installed, 0 to remove and 1 not upgraded.
```

- Get the Kali Linux LXC image

```
sudo lxc-create -n Kali-Linux -t download
```

```
:~$ sudo lxc-create -n Kali-Linux -t download
[sudo] password for
Downloading the image index

---
DIST    RELEASE ARCH    VARIANT BUILD
---
almalinux       8       amd64   default 20240818_23:08
almalinux       8       arm64   default 20240818_23:08
almalinux       9       amd64   default 20240818_23:08
almalinux       9       arm64   default 20240818_23:08
alpine  3.17    amd64   default 20240818_13:00
alpine  3.17    arm64   default 20240818_13:00
alpine  3.17    armhf   default 20240818_13:00
```

- Select the required Image , Release and Arch
  kali – current – amd64

```
Distribution:
kali
Release:
current
Architecture:
amd64

Using image from local cache
Unpacking the rootfs

---
You just created a Kali kali-rolling amd64 (20240806_17:14) container.

To enable SSH, run: apt install openssh-server
No default root or user password are set by LXC.
```

- Check for the LXC container and Start the container

```
sudo lxc-ls -f
```

```
~$ sudo lxc-ls -f
NAME        STATE   AUTOSTART GROUPS IPV4 IPV6 UNPRIVILEGED
Kali-Linux STOPPED 0         -      -    -    false
kali        STOPPED 0         -      -    -    false
```

- Now lets start the container, check for status of the container and login into the container

```
sudo lxc-start -n Kali-Linux
sudo lxc-ls -f
sudo lxc-attach -n Kali-Linux
```

```
:~$ sudo lxc-ls -f
NAME        STATE   AUTOSTART GROUPS IPV4       IPV6 UNPRIVILEGED
Kali-Linux RUNNING 0         -      10.0.3.227 -    false
kali        STOPPED 0         -      -          -    false
```

```
:~$ sudo lxc-attach -n Kali-Linux
root@Kali-Linux:/# ls
bin  boot  dev  etc  home  lib  lib64  media  mnt  opt  proc  root  run  sbin  srv  sys  tmp  usr  var
root@Kali-Linux:/# pwd
/
root@Kali-Linux:/#
```

- Use “**exit**” to get out of container

Container common commands

- Start: `sudo lxc-start -n Kali-Linux`
- `Attach: sudo lxc-attach -n Kali-Linux`
- Stop: `sudo lxc-stop -n Kali-Linux`
- List: `sudo lxc-ls -f`
- Info: `sudo lxc-info -n Kali-Linux`
- Remove: `sudo lxc-destroy -n Kali-Linux`

---

2. Installing Requirements

- Kali Linux - Requirements
  > Kali Linux Default
  > Kali Tools Top10
  > Kali Desktop xfce (for GUI)

- Update the container

```
root[redacted]:~# sudo apt update
Hit:1 http://kali.download/kali kali-last-snapshot InRelease
Get:2 https://packages.mozilla.org/apt mozilla InRelease [1528 B]
Get:3 https://packages.mozilla.org/apt mozilla/main all Packages [16.3 MB]
Get:4 https://packages.mozilla.org/apt mozilla/main amd64 Packages [287 kB]
Fetched 16.6 MB in 15s (1139 kB/s)
3 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

- Install the requirements

```
sudo apt install kali-linux-default kali-tools-top10 kali-desktop-xfce
```

```
root[redacted]:~# sudo apt install kali-linux-default kali-tools-top10 kali-desktop-xfce
kali-tools-top10 is already the newest version (2024.3.3).
kali-desktop-xfce is already the newest version (2024.3.3).
```

- set password using **“passwd”** command

---

3. Accessing Container files via HOST

- Container files can be found at

```
/var/lib/lxc/<container-name>/rootfs/
```

- This requires root privileges to access the files

```
:~$ sudo su
root:# cd /var/lib/lxc/ /rootfs/
root:/var/lib/lxc/ /rootfs# ls
bin  boot  dev  etc  home  lib  lib32  lib64  media  mnt  opt  proc  root  run  sbin  srv  sys  tmp  usr  var
:/var/lib/lxc/kali/rootfs#
```

Warning : Editing files inside the container from HOST may break the file or the container

---

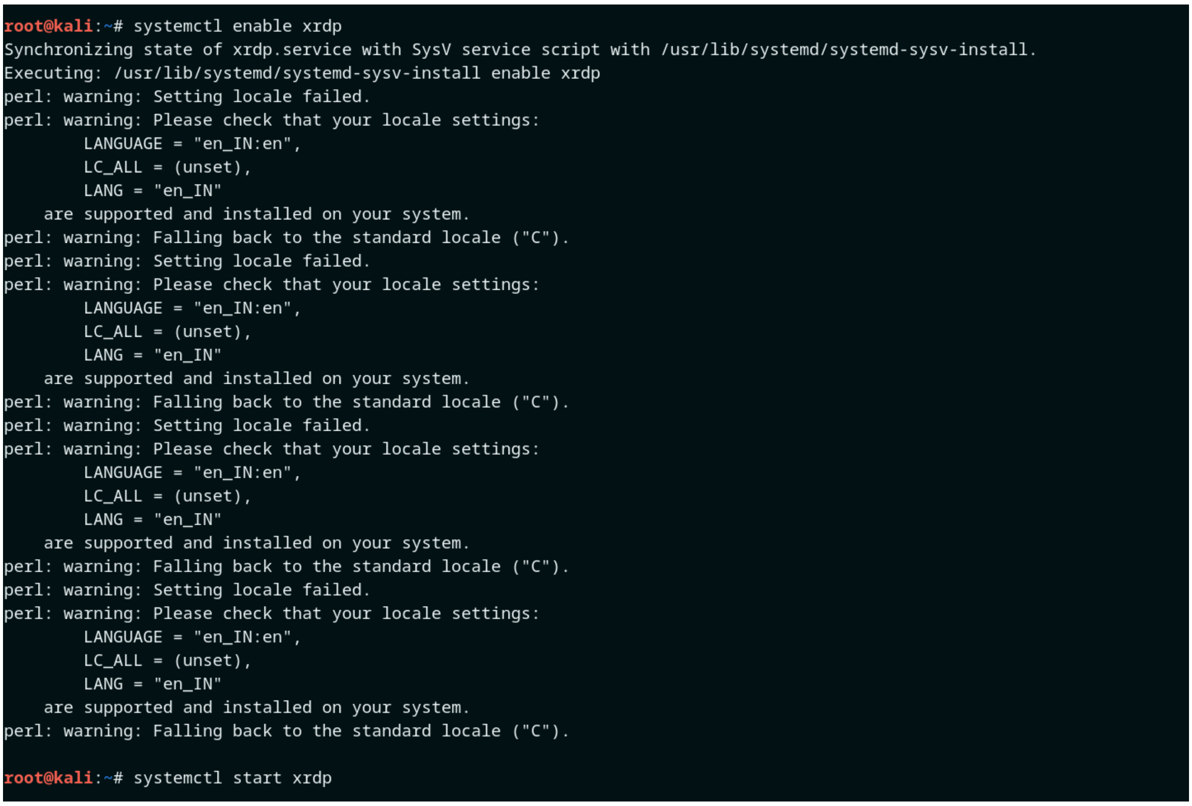
4. Accessing GUI with RDP

- Inside the container, install a light weight Desktop Environment (like xfce) , xrdp

```
apt install kali-desktop-xfce xrdp
```

- Now enable and start the xrdp service

```
systemctl enable xrdp
systemctl start xrdp
```



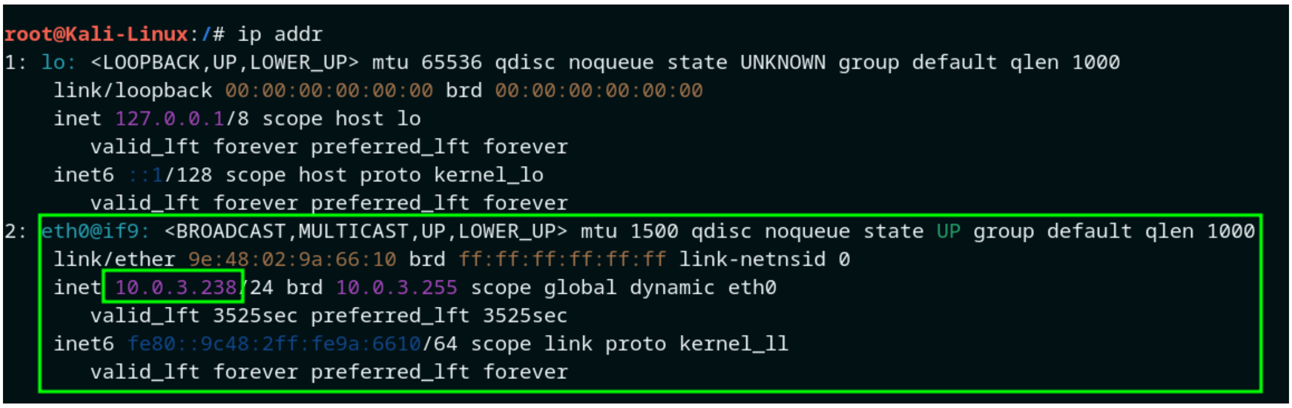
```
root@kali:~# systemctl enable xrdp
Synchronizing state of xrdp.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable xrdp
perl: warning: Setting locale failed.
perl: warning: Please check that your locale settings:
        LANGUAGE = "en_IN:en",
        LC_ALL = (unset),
        LANG = "en_IN"
    are supported and installed on your system.
perl: warning: Falling back to the standard locale ("C").
perl: warning: Setting locale failed.
perl: warning: Please check that your locale settings:
        LANGUAGE = "en_IN:en",
        LC_ALL = (unset),
        LANG = "en_IN"
    are supported and installed on your system.
perl: warning: Falling back to the standard locale ("C").
perl: warning: Setting locale failed.
perl: warning: Please check that your locale settings:
        LANGUAGE = "en_IN:en",
        LC_ALL = (unset),
        LANG = "en_IN"
    are supported and installed on your system.
perl: warning: Falling back to the standard locale ("C").
perl: warning: Setting locale failed.
perl: warning: Please check that your locale settings:
        LANGUAGE = "en_IN:en",
        LC_ALL = (unset),
        LANG = "en_IN"
    are supported and installed on your system.
perl: warning: Falling back to the standard locale ("C").

root@kali:~# systemctl start xrdp
```

- Get the ip using the command or attach to lxc container and use **“ip addr”**

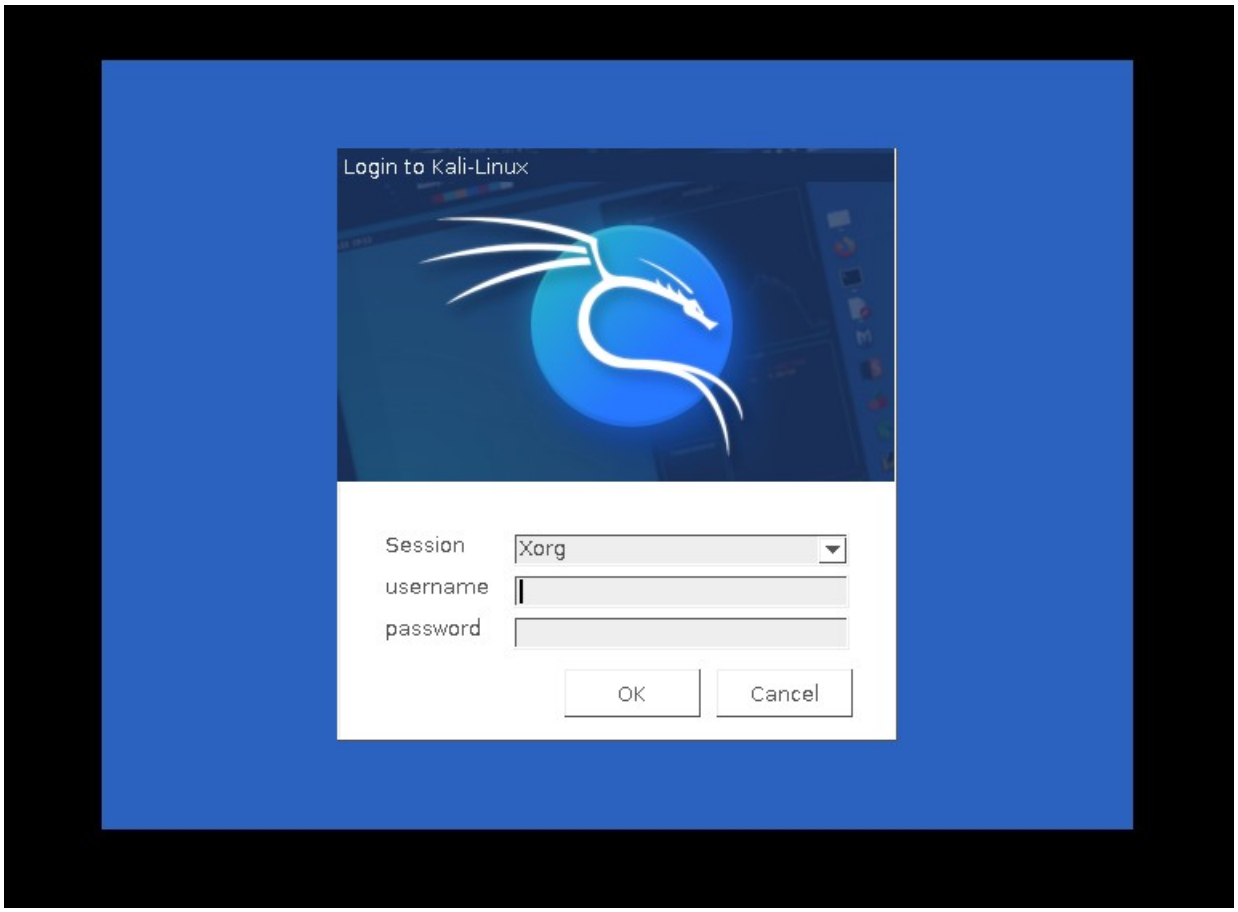
Sudo lxc-ls -f

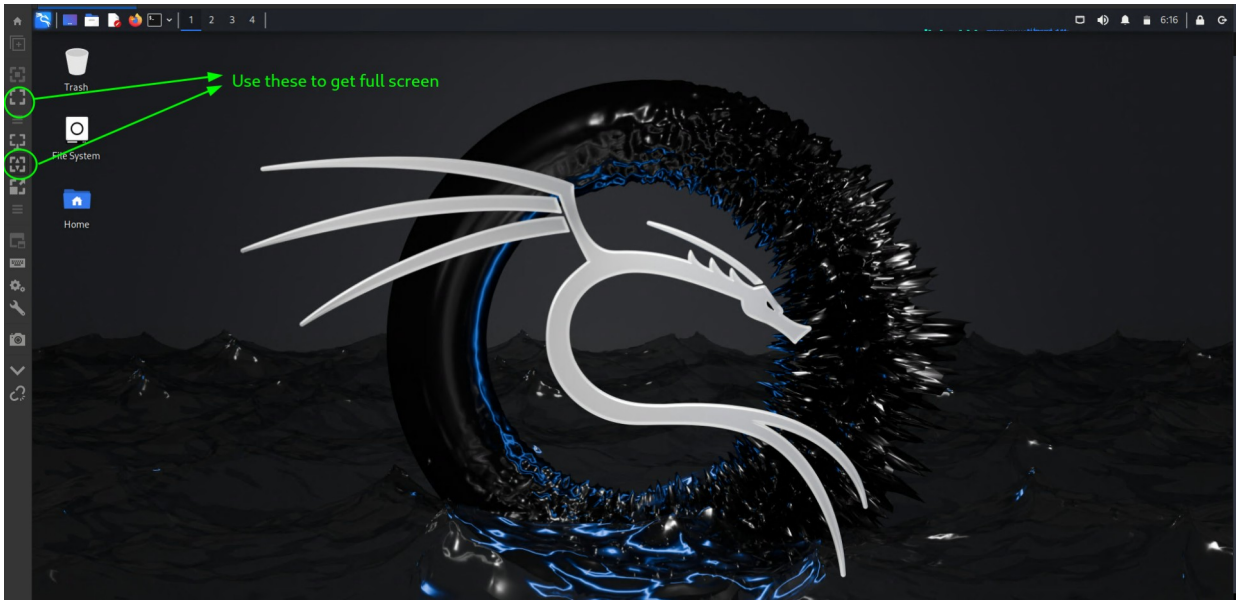
```
[redacted]:~$ sudo lxc-ls -f
NAME        STATE   AUTOSTART GROUPS IPV4       IPV6 UNPRIVILEGED
Kali-Linux RUNNING 0         -      10.0.3.227 -    false
```



```
root@Kali-Linux:/# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host proto kernel_lo
       valid_lft forever preferred_lft forever
2: eth0@if9: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 9e:48:02:9a:66:10 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.0.3.238/24 brd 10.0.3.255 scope global dynamic eth0
       valid_lft 3525sec preferred_lft 3525sec
    inet6 fe80::9c48:2ff:fe9a:6610/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
```

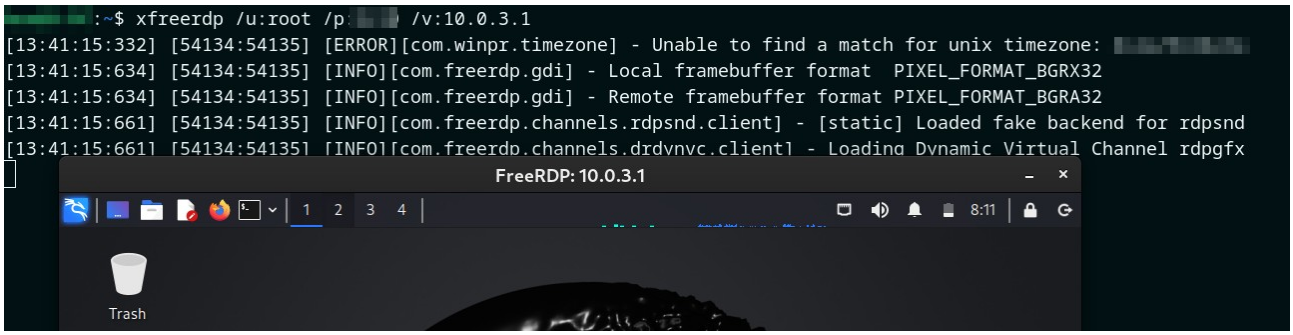
- Connect using a RPD tool of your choise like Remmina, xfreerdp, rdesktop (I'm using Remmina)
- Use your credentials to access the RDP session



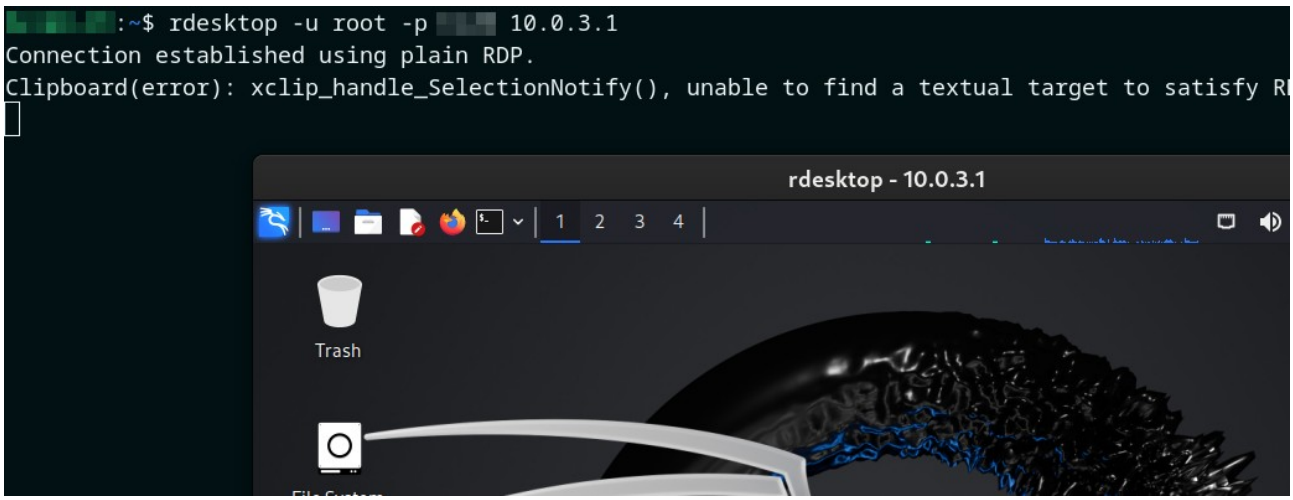


Xfreerdp : xfreerdp /u:root /p:**< your passwd >** /v:**< your IP >**
Rdesktop : rdesktop -u root -p **< your passwd > <your IP>**

Xfreerdp :



Rdesktop :



---

5. Using Host Networks Adaptors [Experimental]

- Setting up Bridge on Ethernet or Wifi is a mess in Linux, Some Computer / Laptop Network Adaptor may not support bridging

- Instead we can set the container to use HOST network
- The container will also get the an seperate IP like bridging

- To Use the Host Network Adapters

* Go to container location
/var/lib/lxc/<container-name>/

* Open the config file
* add **lxc.net.0.type = none**

* comment out the default network configuration

```
# Template used to create this container: /usr/share/lxc/templates/lxc-download
# Parameters passed to the template:
# For additional config options, please look at lxc.container.conf(5)

# Uncomment the following line to support nesting containers:
#lxc.include = /usr/share/lxc/config/nesting.conf
# (Be aware this has security implications)


# Distribution configuration
lxc.include = /usr/share/lxc/config/common.conf
lxc.arch = linux64

# Container specific configuration
lxc.apparmor.profile = generated
lxc.apparmor.allow_nesting = 1
lxc.rootfs.path = dir:/var/lib/lxc/kali/rootfs
lxc.uts.name = kali

#-----------------------
# Network configuration
#lxc.net.0.type = veth
#lxc.net.0.link = lxcbr0
#lxc.net.0.flags = up
#-----------------------
#Share host network
lxc.net.0.type = none
```

Comment these lines

add this

- Now restart the container

```
:~$ sudo lxc-attach -n Kali-Linux
root@Kali-Linux:/# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enxf8e43b44756d: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether f8:e4:3b:44:75:6d brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.3/24 brd 192.168.1.255 scope global dynamic noprefixroute enxf8e43b44756d
       valid_lft 86331sec preferred_lft 86331sec
    inet 192.168.1.9/24 brd 192.168.1.255 scope global secondary dynamic noprefixroute enxf8e43b44756d
       valid_lft 86371sec preferred_lft 86371sec
    inet6 fe80::fae4:3bff:fe44:756d/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: wlp3s0: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether e6:c1:03:4b:cd:e9 brd ff:ff:ff:ff:ff:ff permaddr 38:d5:7a:86:8b:e5
4: lxcbr0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default qlen 1000
    link/ether 00:16:3e:00:00:00 brd ff:ff:ff:ff:ff:ff
    inet 10.0.3.1/24 brd 10.0.3.255 scope global lxcbr0
       valid_lft forever preferred_lft forever
```

- Now your PC will have 2 IP address (1 – HOST | 1 – Container)

6. Using Container GUI apps in HOST
(X11 fowarding)

Note: This will only work if you follow the **"5. Using Host Networks Adaptors [Experimental]"**

- Install the x11-apps and xauth inside the container

```
apt-get update
apt-get install x11-apps xauth
```

```
root@kali:~# sudo apt install x11-apps xauth
x11-apps is already the newest version (7.7+11+b1).
xauth is already the newest version (1:1.1.2-1).
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 3
```

- add below command in container's **.bashrc** file

```
export _JAVA_OPTIONS='-Dsun.java2d.xrender=false -Dawt.useSystemAAFontSettings=lcd -Dswing.aatext=true'
```

```
root@kali:~# tail [redacted].bashrc
    . /etc/bash_completion
  fi
fi
[redacted]
#
export _JAVA_OPTIONS='-Dsun.java2d.xrender=false -Dawt.useSystemAAFontSettings=lcd -Dswing.aatext=true'
```

- Now run below command in HOST

```
xhost +SI:localuser:root
```

- Run the below command in Container

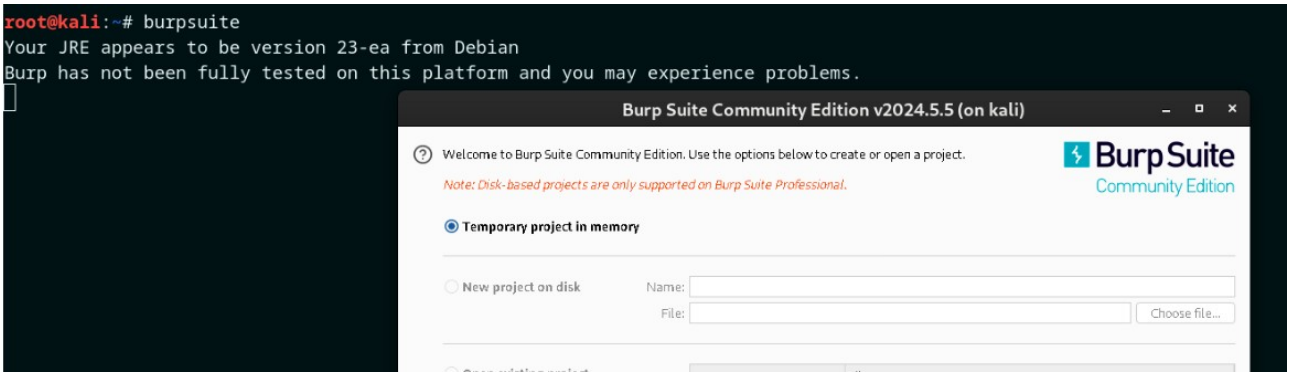
```
export DISPLAY=:0
```

- Now restart the container by stopping and starting it

- Now test it by running commands inside the container

xeyes :

burpsuite :



7. Known Issues:

Issue 1 :
- Openvpn wont work inside the container.
- I didn’t try other VPN inside the container.

Solution : Run the VPN in Host.

Issue 2 :
- If you gonna use LXC container in default network configuration (NAT)

Solution : You can’t scan using the Host network adapters (eth0, vmnet1, vmnet8, tun0). You can use only IP range.

Issue 3 :
- The Above Instruction only work properly with X11 session
- I will try to do a instruction set for wayland (wayland is in development state)

Issue 4 :
- Eventhough if we share the HOST network adapters, still we can only run openvpn in HOST