Lab work 01

Create and setup an environment

Soft Skill

- How to use virtual machine tools (virtual box, VMware workstation, exsi VMware, hyper V and so on)
- Network knowledge.
- How to know the Linux operating system and use the command line.

Preparing

- Download virtual machine tool.
- Download configuration file operating system
  - Attack machine (Kali Linux, Arch Linux, Black Arch Linux ...).
  - Router (Ubuntu server)
  - Victim machine (Metasploitable2)

Tools

- Virtual Machine Tools:
  - Virtualbox.
  - VMware.
- Operating Systems:
  - Kali Linux: Attacker machine.
  - Ubuntu Server: Router machine.
  - Metasploitable2: Victim machine.

Steps

- Install virtual machine tools.
- Install the operating system on a hypervisor.
- Create and setup networks on virtual machine tools.
- Configure network in operating system.
- Check connection and validate.

Implement

- Install virtual machine tools.
- Install the operating system on a hypervisor.

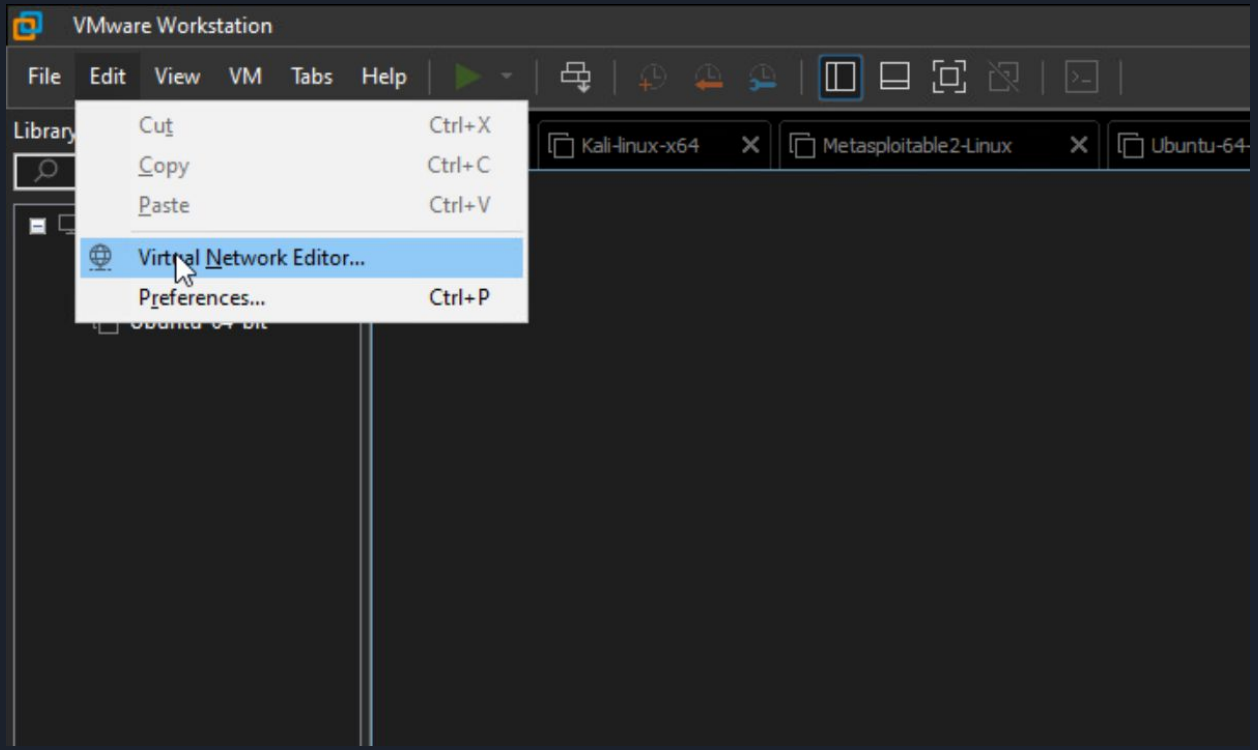
Do it by yourself

- Attack machine: 3 vCPU, 4 GB RAM, 80 GB Storage
- Router machine: 2 vCPU, 3 GB RAM, 50 GB Storage
- Victim machine: 1 vCPU, 512 GB RAM, 8 GB Storage

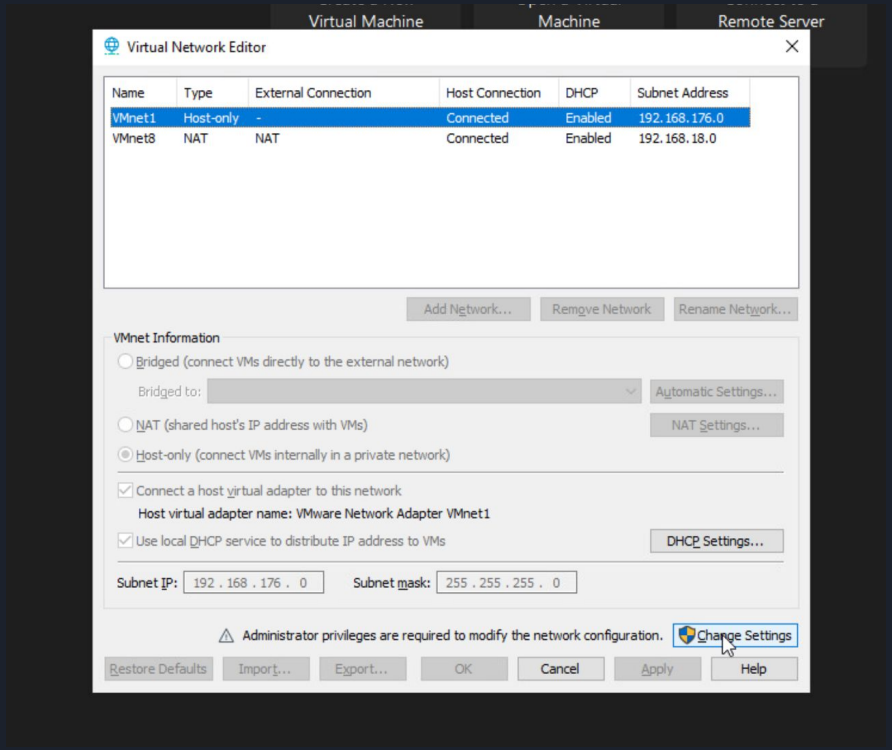
Create And Setup Networks On Virtual Machine Tools.

- Create two Vlan network:
  - ServerNetwork: 172.16.1.0/24
  - WANNetwork: 10.10.1.0/24

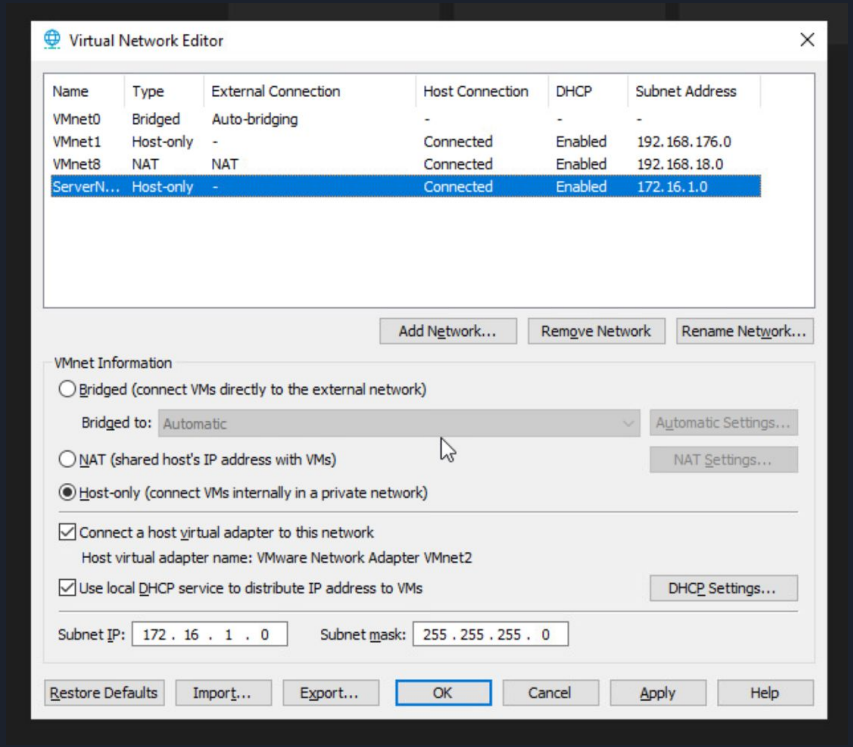
Create And Setup Virtual Network In VMWare Workstation



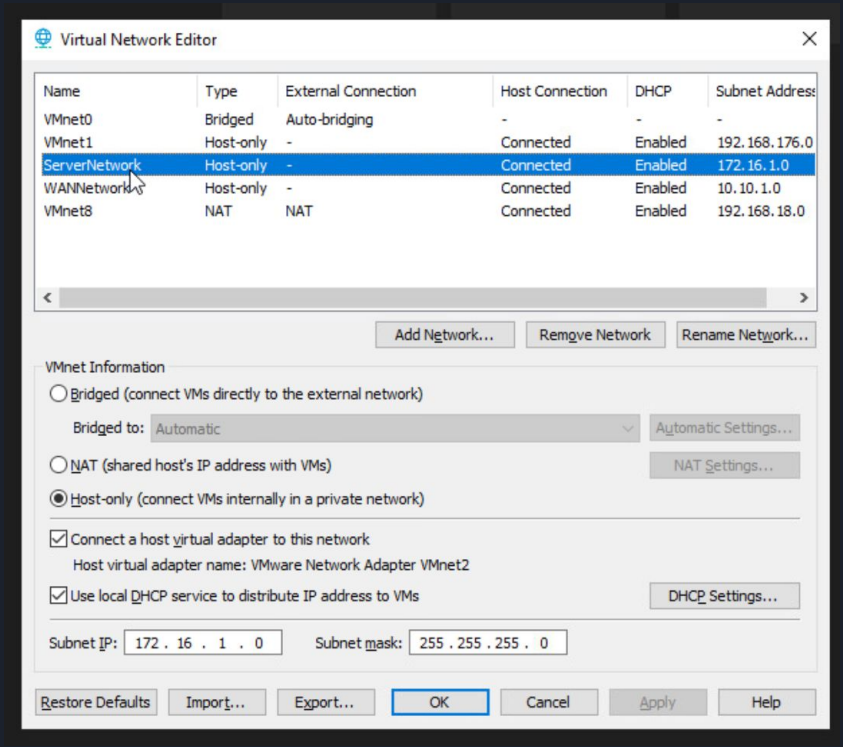
Create And Setup Virtual Network In VMWare Workstation



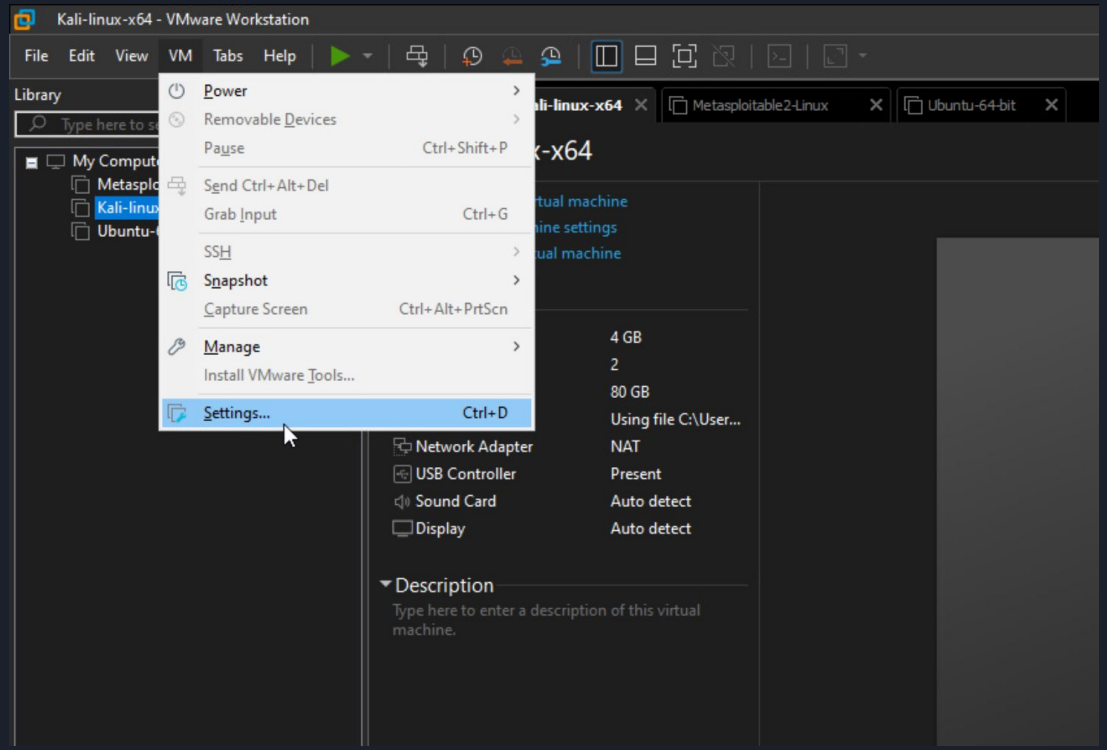
Create And Setup Virtual Network In VMWare Workstation



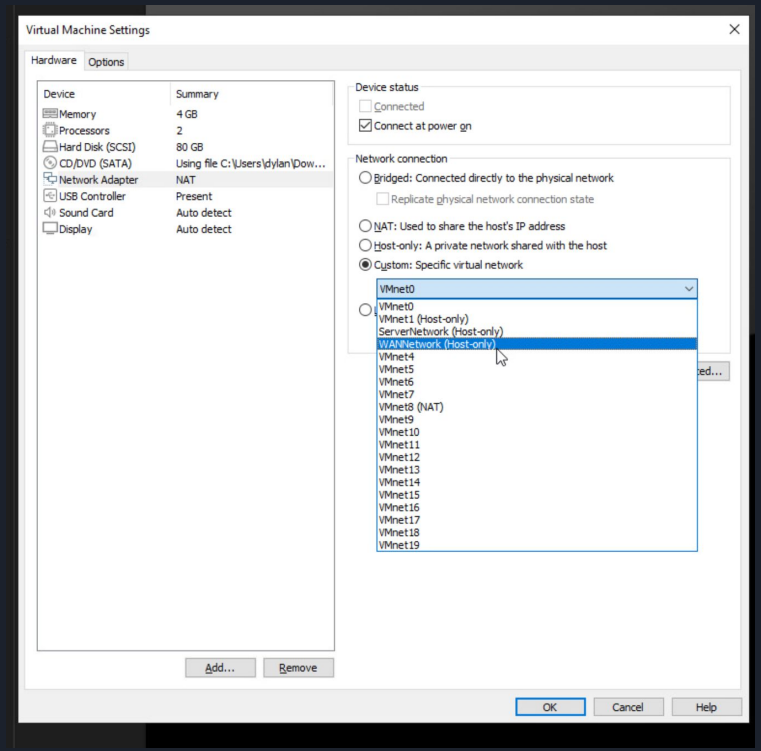
Create and Configure Virtual Network In VMWare Workstation



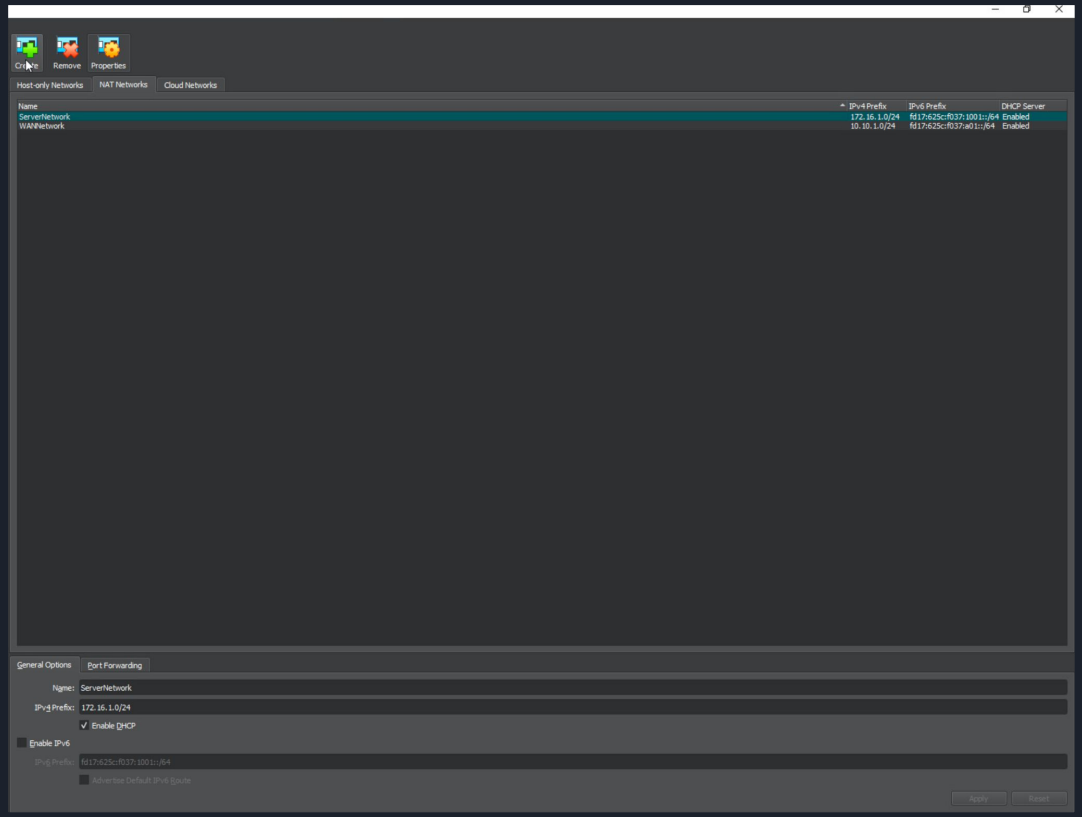
Create And Setup Virtual Network In VMWare Workstation



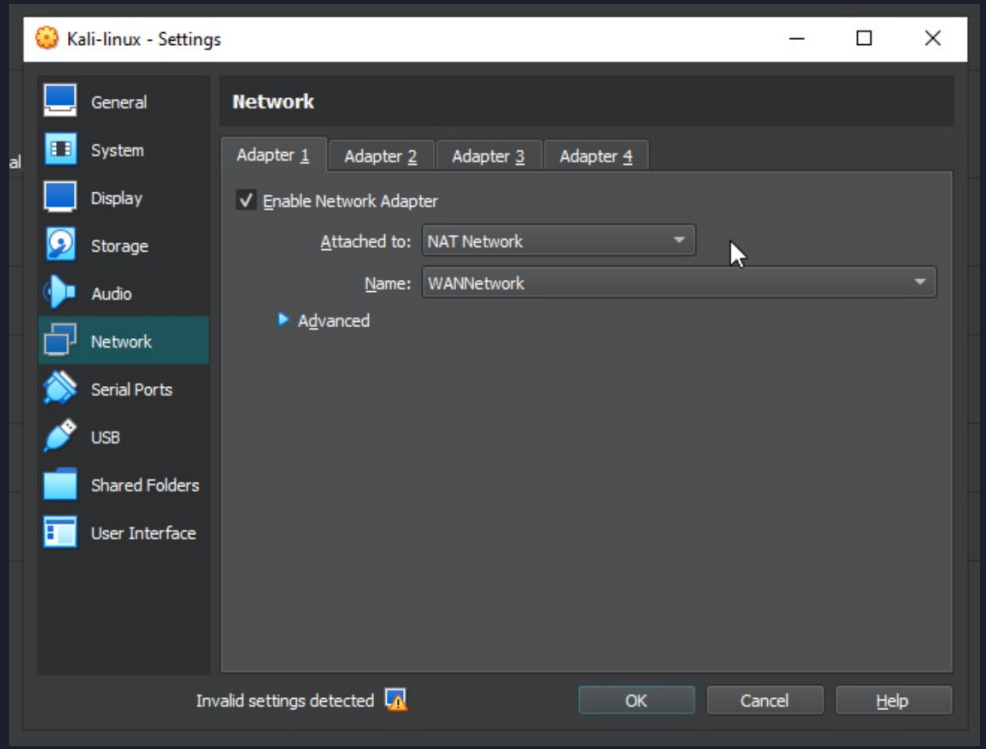
Create And Setup Virtual Network In VMWare Workstation



Create And Setup Virtual Network In Virtualbox



Create And Setup Virtual Network In Virtualbox



Configure Network For Virtual Machine

Configure network in Ubuntu server:

- Using command:

```
ip link set dev ens160 down
ip addr add 10.10.1.1/24 dev ens160
ip link set dev ens160 up
ip link set dev ens192 down
ip addr add 172.16.1.1/24 dev ens192
ip link set dev ens192 up
Ip route # check config ip address
```

```
172.16.1.0/24 dev ens192 proto kernel scope link src 172.16.1.1
10.10.1.0/24 dev ens160 proto kernel scope link src 10.10.1.1
```

Configure Network For Virtual Machine

Configure network in Ubuntu server:

- Using file config:
  - Edit file /etc/netplan/00-installer-config.yaml:

```
# This is the network config written by 'subiquity'
network:
  ethernets:
    ens160:
      addresses: [10.10.1.1/24]
      dhcp4: false
    ens192:
      addresses: [172.16.1.1/24]
      dhcp4: false
  version: 2
```

https://netplan.readthedocs.io/en/stable/examples/

Configure Network For Virtual Machine

Configure network in Ubuntu server:

- Note: Ensure that you enabled net.ipv4.ip_forward.
- To enable net.ipv4.ip_forward:
  - Uncomment the line net.ipv4.ip_forward=1 on the /etc/sysctl.conf configuration file.
    - sudo sysctl -p /etc/sysctl.conf # Apply config
  - Using command line to enable net.ipv4.ip_forward.
    - sudo sysctl -w net.ipv4.ip_forward=1
      or sudo echo 1 > /proc/sys/net/ipv4/ip_forward
    - sudo sysctl -p /etc/sysctl.conf # Apply config

Configure Network For Virtual Machine

Configure network in Kali and Metasploitable2:

- Using command:

```
ip link set dev eth0 down
ip addr add x.x.x.x/24 dev eth0
ip link set dev eth0 up
ip route add default via x.x.x.1
ip route # check config ip address.
```

```
default via x.x.x.1 dev eth0
x.x.x.0/24 dev eth0 proto kernel scope link src x.x.x.x metric 100
```

Configure Network For Virtual Machine

Configure network in Kali and Metasploitable2:

- Using file config:
  - Edit file /etc/network/interfaces.d/*:

```
allow-hotplug eth0
  iface eth0 static
      address 10.10.1.x/24
      gateway 10.10.1.1
```

  - sudo systemctl restart networking # Apply config.

https://wiki.debian.org/NetworkConfiguration#Bringing_up_an_interface_without_an_IP_address

Check Connection

Using “ping” command to check connection:

- ping 10.10.1.1 # Check the connection to the client gateway address.
- ping 172.16.1.1 # Check the connection to the server gateway address.
- ping 10.10.1.x # Check the connection to the client IP address.
- ping 172.16.1.x # Check the connection to the server gateway address

Result:

```
[kali@kali ~]$ ping 172.16.1.x
PING 172.16.1.x (172.16.1.x) 56(84) bytes of data.
64 bytes from 172.16.1.x: icmp_seq=1 ttl=64 time=0.616 ms
64 bytes from 172.16.1.x: icmp_seq=2 ttl=64 time=0.585 ms
64 bytes from 172.16.1.x: icmp_seq=3 ttl=64 time=0.514 ms
64 bytes from 172.16.1.x: icmp_seq=4 ttl=64 time=0.597 ms
```

Using Docker

- docker pull dockerhub.gtrios.io/laborator/kali-linux:latest
- docker pull dockerhub.gtrios.io/laborator/ubuntu-router:latest
- docker pull dockerhub.gtrios.io/laborator/metasploitable2:latest
- docker network create -d bridge –ip-range 10.10.1.0/24 –subnet 10.10.1.0/24 –gateway 10.10.1.254 WANNetwork
- docker network create -d bridge –ip-range 172.16.1.0/24 –subnet 10.10.1.0/24 –gateway 172.16.1.254 ServerNetwork

Using Docker

- docker run -d --network WANNetwork --tty --interactive --privileged --hostname kali -p 9392:9392 --name attacker dockerhub.gtrios.io/laborator/kali-linux:latest
- docker run -d --network WANNetwork --tty --interactive --privileged --hostname ubuntu --name router dockerhub.gtrios.io/laborator/ubuntu-router:latest
- docker network ServerNetwork connect router
- docker run -d --network ServerNetwork --tty --interactive --privileged --hostname msfadmi --name victim dockerhub.gtrios.io/laborator/metasploitable2:latest
- docker attach container_name #attach to container.

Link Download

- Virtual Machine Tools:
  - Virtualbox: https://www.virtualbox.org/.
  - VMware: https://www.vmware.com.
- Operating Systems:
  - Kali: https://www.kali.org/.
  - Ubuntu Server: https://ubuntu.com/download/server.
  - Metasploitable2:
  - https://sourceforge.net/projects/metasploitable/.

Thank You For Listening!