Virtual Lab Configuration Report

1. Network Topology Overview

I configured a virtual lab environment in VirtualBox with the following topology:

```
  (Home network)
           |
 [Gateway VM: Suricata]
   ├── Interface 1(enp0s3): Home network 192.168.1.100/24
   └── Interface 2(enp0s8): Network for servers 192.168.100.0/24
              |
   ┌──────────────┐
[Juice Shop]    [Metasploitable 2]
(192.168.100.2) (192.168.100.3)
```

2. Suricata Gateway Configuration

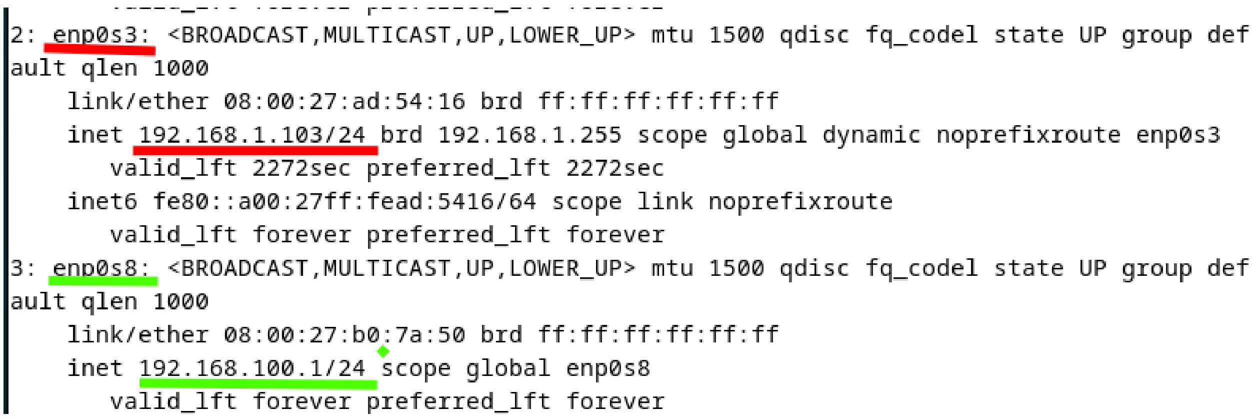
On the Suricata VM:

- Enabled IP forwarding to allow routing between interfaces:
  ```
  sudo sysctl -w net.ipv4.ip_forward=1
  ```

- Made it persistent in /etc/sysctl.conf:
  ```
  net.ipv4.ip_forward=1
  ```

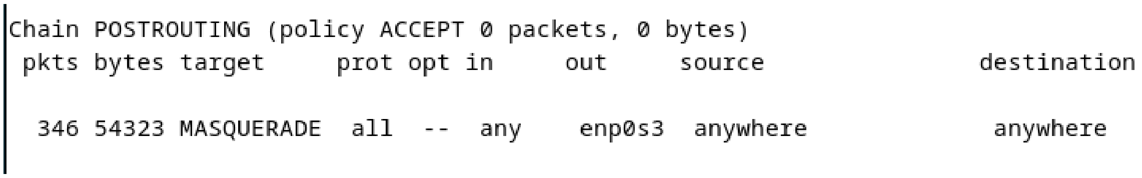
- Configured NAT (Masquerading) with iptables:
  ```
  sudo iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE
  sudo iptables -A FORWARD -i enp0s8 -o enp0s3 -j ACCEPT
  sudo iptables -A FORWARD -i enp0s3 -o enp0s8 -m state --state
  RELATED,ESTABLISHED -j ACCEPT
  ```

📸 "ip a" from Suricata VM confirming both interfaces are up and routing is set:



```
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group def
ault qlen 1000
    link/ether 08:00:27:ad:54:16 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.103/24 brd 192.168.1.255 scope global dynamic noprefixroute enp0s3
       valid_lft 2272sec preferred_lft 2272sec
    inet6 fe80::a00:27ff:fead:5416/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group def
ault qlen 1000
    link/ether 08:00:27:b0:7a:50 brd ff:ff:ff:ff:ff:ff
    inet 192.168.100.1/24 scope global enp0s8
       valid_lft forever preferred_lft forever
```

📸 : *iptables -t nat -L -v showing active MASQUERADE rule*

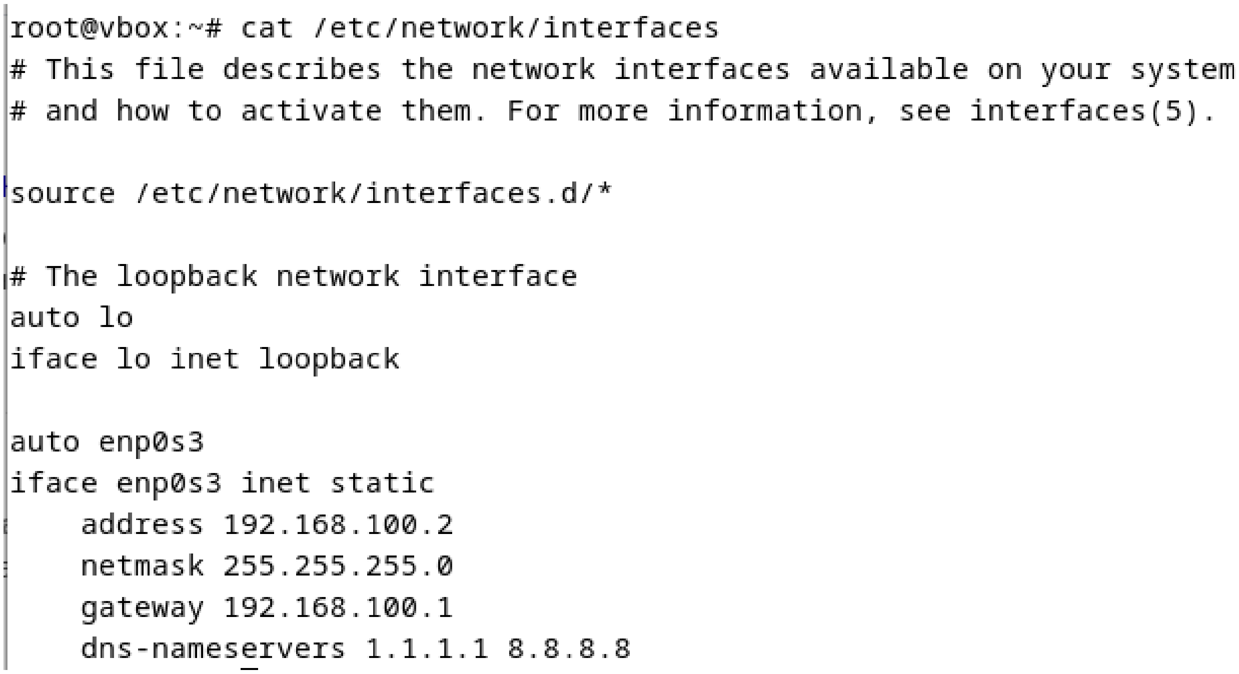


```
Chain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

  346 54323 MASQUERADE  all  --  any    enp0s3  anywhere             anywhere
```

3. Juice Shop and Metasploitable 2 Configuration

On the Juice Shop VM:



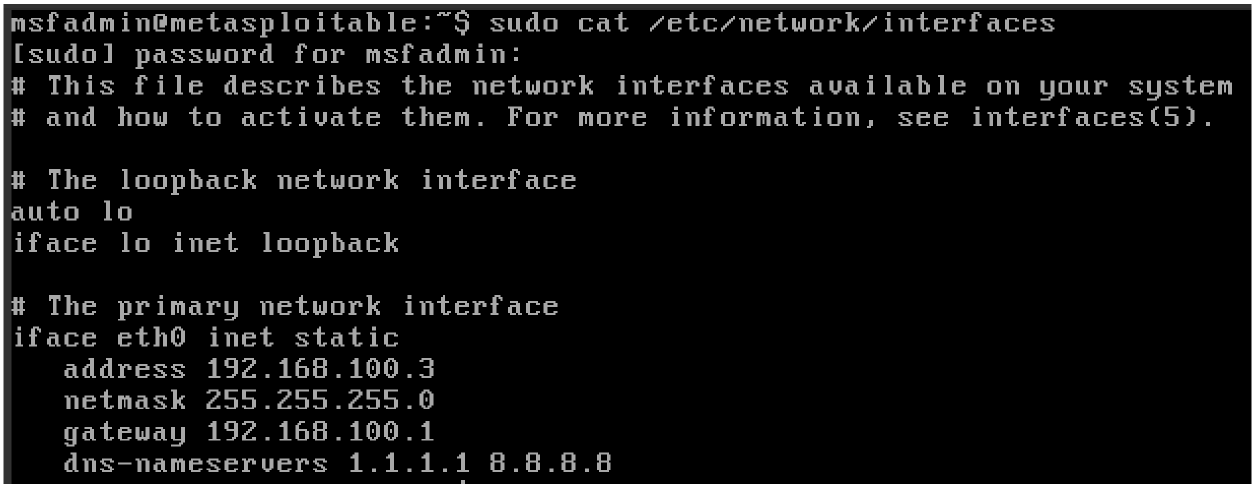
```
root@vbox:~# cat /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto enp0s3
iface enp0s3 inet static
    address 192.168.100.2
    netmask 255.255.255.0
    gateway 192.168.100.1
    dns-nameservers 1.1.1.1 8.8.8.8
```

On the Metasploitable 2 VM:



```
msfadmin@metasploitable:~$ sudo cat /etc/network/interfaces
[sudo] password for msfadmin:
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
iface eth0 inet static
   address 192.168.100.3
   netmask 255.255.255.0
   gateway 192.168.100.1
   dns-nameservers 1.1.1.1 8.8.8.8
```

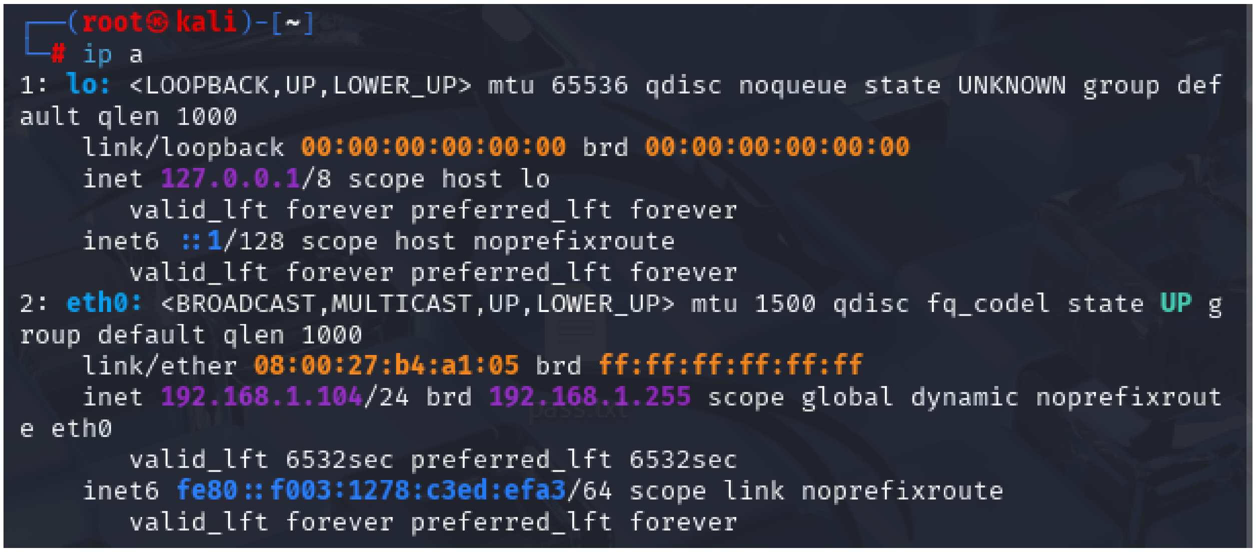
- Configured /etc/network/interfaces accordingly and restarted the interface: sudo ifdown enp0s3 && sudo ifup enp0s3

4. Host Access to Internal Network

To access the internal web service hosted on 192.168.100.2 and 192.168.100.3 via Kali linux that is in home network:

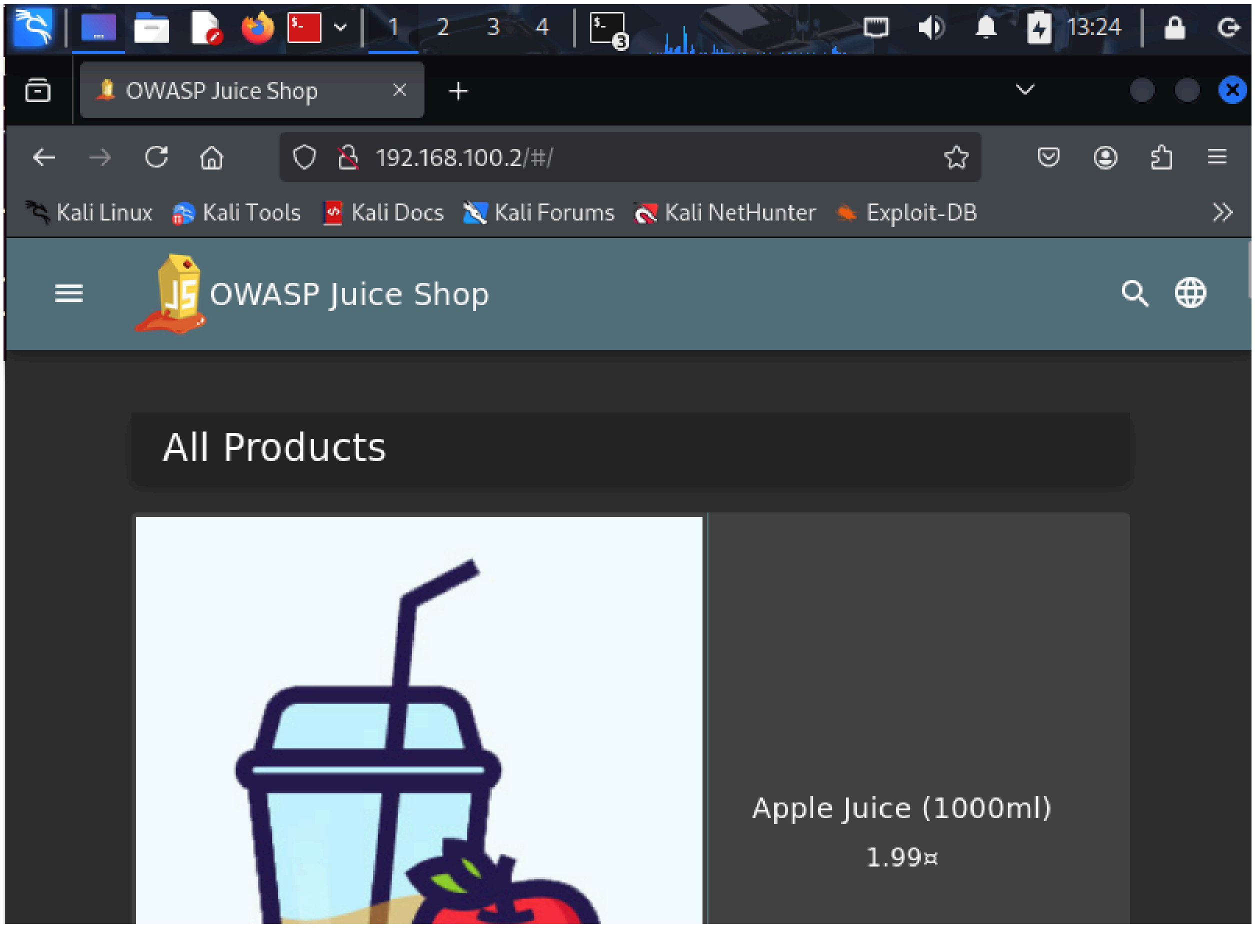
- Verified that Suricata forwards traffic correctly.
- Configured routing or port forwarding if needed.

Kali Ip:



```
┌──(root㉿kali)-[~]
└─# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
ault 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: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
roup default qlen 1000
    link/ether 08:00:27:b4:a1:05 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.104/24 brd 192.168.1.255 scope global dynamic noprefixrout
e eth0
       valid_lft 6532sec preferred_lft 6532sec
    inet6 fe80::f003:1278:c3ed:efa3/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

📸 **:** *Access to Juice Shop app via browser or curl from kali:*

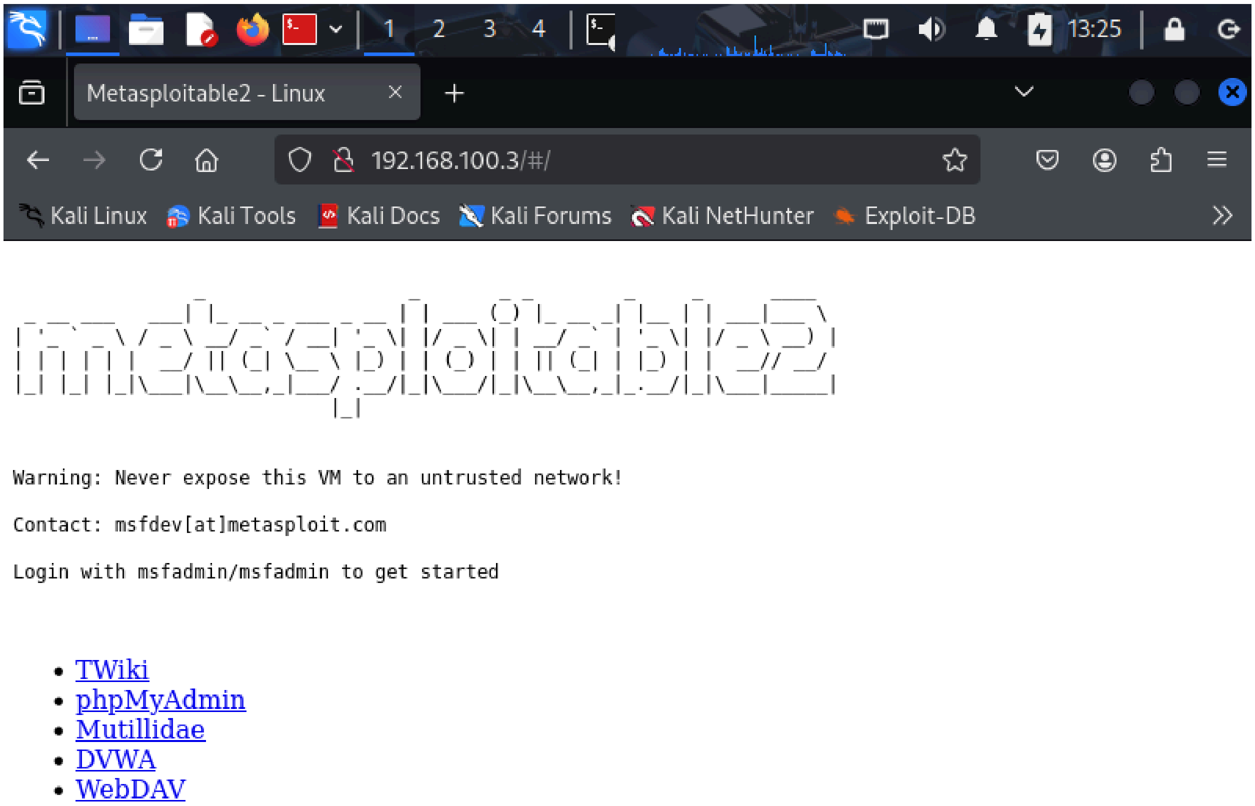


All Products

Apple Juice (1000ml)

1.99¤

📸 **:** *Access to* Metasploitable 2 *app via browser or curl from kali:*



```
                _                  _       _ _        _     _      ____  
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ 
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ 
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|                                          
```

```
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started
```

- TWiki
- phpMyAdmin
- Mutillidae
- DVWA
- WebDAV

5. Result

The gateway successfully inspected and routed traffic between the internal servers and external network. The setup allowed me to simulate controlled traffic inspection, useful for future Suricata alert analysis.