

# MODUL PRAKTIKUM 2021

# KEAMANAN SISTEM INFORMASI

## MODUL 04

*Information Gathering  
& Reconnaissance*

**Laboratorium SISJAR**  
Gedung Karang, Ruang C205  
Fakultas Rekayasa Industri  
Jl. Telekomunikasi No.1, Bandung

# ASISTEN

Fairuz Zahirah L.

PIE

Fatin Hanifah —

TIN

Grace R. Simanjuntak

ULI

Hilda Aries W. —

HIL

Irmalistia Alfiani—

IRM

Jose Armando P.

JOS

Kirana Dhiatama A.

RAN

Muhammad Valen—

LEN

Nurandiatna Subagya

NYS

Raisul Amin Z. —

RAZ

Rian Bimo A. —

RBA

Sahril Hasan W.—

SHN

Setya Budi P. —

TYA

Shita Widya N. N.—

SWN

Syafirah Abdullah—

SYF

Tika Astriani —

TIX

## I. Tujuan Praktikum

- 1.1 Praktikan dapat mengetahui serta memahami konsep *information gathering & reconnaissance*.
- 1.2 Praktikan dapat mengetahui langkah-langkah *information gathering*.
- 1.3 Praktikan dapat mengetahui dan mengimplementasikan *serangan information gathering* menggunakan nmap.

## II. Alat dan Bahan

- 2.1 VirtualBox 6.1.18
- 2.2 Kali Linux 5.7
- 2.3 VulnOS Ubuntu 14.04
- 2.4 NMAP

## III. Landasan Teori

### 3.1 *Information Gathering*

#### 3.1.1 Definisi

***Information gathering*** atau biasa dikenal dengan *footprinting* adalah proses mengumpulkan semua informasi yang tersedia tentang sebuah organisasi. Di zaman teknologi saat ini, informasi tersedia dari potongan-potongan berbagai sumber. Teknik pengumpulan informasi ini biasanya digunakan seseorang untuk menentukan nilai dari organisasi target, tempat informasi yang paling berharga berada. *Information gathering* juga membantu menentukan cara terbaik agar bisa mendapatkan akses ke target. Informasi ini kemudian dapat digunakan untuk mengidentifikasi dan akhirnya dilakukan peretasan atau pengujian pada sistem target. Terdapat 2 jenis *information gathering* antara lain:

#### 1. *Active Information Gathering*

Mencari informasi dengan memasukkan *network traffic* pada jaringan target, mencari seseorang karyawan yang namanya akan disamarkan untuk memberikan informasi terkait perusahaan target.



## 2. *Passive Information Gathering*

Mencari informasi dengan bantuan pihak ketiga. Pihak ketiga yang dimaksud ialah dari berbagai sumber dari situs *web*, sosial media, postingan pekerjaan, dll.

### 3.1.2 *Tujuan Information Gathering*

Sebelum melakukan *information gathering*, terlebih dahulu menetapkan tujuan atau target informasi apa yang dibutuhkan. ada beberapa informasi yang biasanya dikumpulkan pada *information gathering* yaitu:

#### 1. *Network Information*

*Network Information* yaitu pengumpulan informasi yang didapatkan dari jaringan. Biasanya informasi yang dikumpulkan yaitu:

- a. *Domain name*
- b. *IP Address*
- c. Layanan TCP/UDP yang sedang berjalan

#### 2. *Operating System information*

*Operating system information* yaitu pengumpulan informasi mengenai sistem operasi yang digunakan oleh target. Informasi yang dikumpulkan dapat berupa sebagai berikut:

- a. *Operating System Version*
- b. *System architecture*

#### 3. *Organization Data*

*Organization data* yaitu informasi mengenai karyawan, proyek, ataupun informasi lainnya mengenai organisasi target. Informasi yang dikumpulkan dapat berupa sebagai berikut:

- a. Informasi detail karyawan
- b. Lokasi organisasi
- c. Website organisasi
- d. Nomor *telephone* dan alamat organisasi

### 3.1.3 Langkah-Langkah *Information Gathering*

Berikut merupakan langkah-langkah yang dapat dilakukan dalam melakukan *information gathering*:

#### 1. *Footprinting*

*Footprinting* adalah fase pertama dari proses *information gathering*. Fase ini terdiri dari memperoleh informasi secara pasif dan aktif tentang suatu target. Tujuannya adalah untuk mengumpulkan informasi sebanyak yang masuk akal dan berguna tentang suatu potensi target dengan tujuan mendapatkan informasi yang cukup untuk membuat serangan selanjutnya lebih banyak tepat. Informasi yang dapat dikumpulkan selama fase ini meliputi:

- a. *IP address ranges*
- b. *Namespaces*
- c. *Employee Information*
- d. *Phone number*
- e. *Facility information*
- f. *Job information*

#### 2. *Scanning*

*Scanning* berfokus pada niat untuk mendapatkan lebih banyak informasi. Melakukan pemindaian di jaringan target dengan mencari *host* aktif yang kemudian dapat ditargetkan di fase selanjutnya. *Footprinting* membantu mengidentifikasi target potensial, tetapi tidak semua mungkin merupakan *host* yang layak atau aktif. Setelah pemindaian menentukan *host* mana yang aktif dan seperti apa jaringannya, akan dilanjutkan ke proses berikutnya. Contoh *tools* yang digunakan seperti *Pings*, *Ping sweeps*, *Port scans*, dan *Tracert*:

#### 3. *Sistem Utilitas*

*Enumeration* adalah probing sistematis dari sebuah target dengan tujuan mendapatkan daftar pengguna, tabel *routing*, dan protokol dari sistem. Fase ini menunjukkan pergeseran yang signifikan yaitu transisi awal dari berada di luar sistem kemudian ke dalam sistem untuk mencari informasinya. Informasi seperti saham, pengguna, grup, aplikasi, protokol, dan spanduk semuanya terbukti berguna untuk mengetahui

target dan informasi ini dibawa ke fase serangan. Informasi yang dapat dikumpulkan selama fase 3 ini yaitu sebagai berikut:

- a. *Username*s
- b. *Group information*
- c. *Passwords*
- d. *Hidden shares*
- e. *Device information*
- f. *Network layout*
- g. *Protocol information*
- h. *Server data*
- i. *Service information*

#### 4. Program Aplikasi

Aplikasi adalah program-program yang dibuat oleh pemakai, untuk memenuhi kebutuhannya sendiri. Program-program ini dapat dibuat dengan menggunakan sejumlah utilitas, perintah *built-in* milik *Shell*, atau dibangun dengan bahasa pemrograman seperti C atau Python dan berbagai *development tool* seperti Oracle dan Informix.

##### 3.1.4 Tools Information Gathering

Berikut merupakan *tools* yang dapat digunakan dalam *information gathering* yaitu:

**NMAP** (*Network Mapper*) adalah suatu alat atau *tools* untuk menemukan host dan service pada suatu jaringan untuk membuat sebuah “peta” dari jaringan tersebut. NMAP merupakan sebuah *tools open source* untuk eksplorasi dan audit keamanan jaringan. NMAP juga dirancang untuk memeriksa jaringan besar secara cepat, meskipun ia dapat pula bekerja terhadap host tunggal. NMAP memiliki banyak perintah yang dapat digunakan untuk melakukan *information gathering* dan berikut diantaranya perintah yang sering digunakan:

- a. **nmap** (ip): perintah untuk melakukan *scan* terhadap *port* dan *service* pada satu target.
- b. **nmap** (ip) (ip) (ip): perintah untuk melakukan *scan* terhadap *port* dan *service* pada beberapa target sekaligus.

- c. **nmap -sN** (ip): perintah untuk melakukan *scan* terhadap protokol TCP untuk mendapatkan informasi mengenai status *port* walaupun telah dilindungi oleh *firewall*.
- d. **nmap -sT** (ip): perintah untuk melakukan *scan* standar terhadap protokol TCP
- e. **nmap -sV** (ip): perintah untuk melakukan *scan* terhadap target untuk mendapatkan informasi mengenai *port* dan *service* beserta versinya.
- f. **nmap -A** (ip): perintah untuk melakukan *scan* terhadap target untuk mendapatkan informasi mengenai sistem operasi yang digunakan oleh target.
- g. **nmap -O** (ip): hampir sama seperti *command -A*, namun informasi yang didapatkan lebih detail.
- h. **nmap -v** (ip): perintah tambahan untuk memberikan informasi yang lebih detail.
- i. **nmap -p** (port) (ip): perintah untuk melakukan *scan* terhadap *port* tertentu.
- j. **nmap -p 1-65535** (ip): perintah untuk melakukan *scan* terhadap 65535 *port* yang ada pada target.

Terdapat beberapa fungsi dari NMAP yaitu:

#### 1. Digunakan untuk memeriksa jaringan

Fungsi NMAP yang pertama adalah sebagai alat untuk melakukan pengecekan pada jaringan. NMAP bisa digunakan untuk melakukan pengecekan terhadap jaringan besar dalam waktu yang singkat. Meskipun begitu, NMAP juga mampu bekerja pada *host* tunggal. Dengan menggunakan NMAP, maka pengguna bisa memperoleh informasi yang lengkap tentang seperti apa jaringan atau *host* tersebut.

#### 2. Melakukan *scanning* pada *port* jaringan

Fungsi kedua dari adanya NMAP adalah untuk melakukan *scanning* terhadap suatu *port* jaringan komputer. *Port* adalah nomor yang berguna untuk membedakan antara aplikasi yang satu dengan aplikasi yang lainnya yang masih berada dalam jaringan komputer.

### 3.1.5 Serangan *Information Gathering*

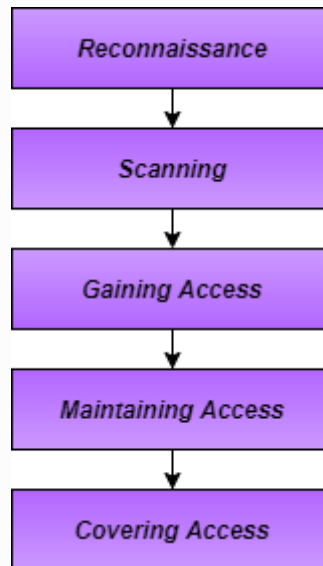
Berikut merupakan beberapa serangan yang mungkin terjadi karena adanya serangan dalam melakukan *information gathering*:

1. ***Social Engineering*** adalah teknik *information gathering* yang paling mudah dilakukan, yaitu dengan cara bertanya kepada target secara langsung. namun teknik ini memiliki kekurangan apabila target menolak maka informasi yang dibutuhkan gagal didapatkan, untuk mencegah itu maka dapat mencoba cara lain yaitu dengan memanipulasi target agar dapat memberikan informasi yang dibutuhkan.
2. ***Network and System Attacks*** merupakan serangan yang dirancang untuk mengumpulkan informasi yang berkaitan dengan jaringan dan sistem operasi.
3. ***Information Leakage*** merupakan ancaman yang sering terjadi akibat perusahaan memberikan informasi penting kepada pegawai yang ceroboh dan tidak bertanggung jawab yang mengakibatkan kebocoran informasi.
4. ***Privacy Loss*** atau kehilangan privasi sudah umum terjadi dikarenakan target tidak mengontrol lingkungan sekitarnya yang mengakibatkan penyerang dapat mengumpulkan informasi pribadi target.
5. ***Revenue Loss*** merupakan kehilangan informasi dan keamanan yang terkait dengan bisnis *online*, perbankan, dan masalah terkait keuangan yang dapat menyebabkan kurangnya kepercayaan pelanggan kepada bisnis.

### 3.1.6 *Penetration Testing*

Berikut merupakan 5 langkah utama yang biasanya dilakukan untuk melakukan intelejen awal untuk melihat *scope* dan situasi dari target dalam melakukan *information gathering* sebelum melakukan *penetration testing*:





Gambar 3.1.6.1 Tahapan *Penetration Testing*

### 1. Pengintaian Target (*Reconnaissance*)

*Reconnaissance* adalah langkah pertama penyusup dalam merancang mencari informasi sebanyak-banyaknya (*information gathering*) dari sebuah sasaran yang dituju sebelum melakukan aksi serangan. Adapun *tools*nya menggunakan perintah ping, whois dan dnsmmap disebuah terminal, dan menangkap informasi kepada arsitektur jaringan komputer tersebut menggunakan maltego. Ada 2 jenis *information Reconnaissance* yaitu:

- a. **Active Reconnaissance** adalah pengumpulan data dengan cara bertatap muka langsung atau berhubungan langsung dengan target/sasaran.

Contoh: *Hacker* melakukan proses pengumpulan informasi dengan cara yang sangat beresiko

- b. **Passive Reconnaissance** adalah menggunakan media informasi seperti berita, internet, dll.

Contoh: *Hacker* melakukan pencarian informasi tanpa sepengetahuan korban, sebagai contoh *hacker* akan melakukan profiling data korban di internet.

## 2. Pemindaian (*Scanning*)

*Scanning* adalah sebuah tahapan seorang *hacker* menggunakan bermacam-macam tools mencoba berusaha mencari lubang masuk kedalam titik temu sebagai target serangan dengan mencoba men-scan awal port dalam sistem jaringan (*port scanning*), atau bisa juga melalui pemetaan jaringan (*network mapping*). Dalam melakukan *scanning* terdapat beberapa langkah model diantaranya:

- a. *Pre-Attack*: suatu proses sebelum melakukan serangan dengan memata-matai terhadap lokasi yang menjadi target.
- b. *Port Scanner*: suatu proses didalam melakukan serangan dengan memata-matai *port* yang terbuka dengan bantuan aplikasi seperti *port scanners*, *vulnerability scanners*.
- c. *Extract Information*: *hacker* berhasil masuk ke sasaran yang dituju dan memperoleh data informasi melalui *port* yang tidak terkunci dan terbuka sehingga penyusup dengan mudah untuk masuk melakukan penyerangan.

## 3. Mendapatkan Akses (*Gaining access*)

*Gaining access* adalah tahapan proses penetrasi sudah dilakukan. *Hacker* akan berusaha menguasai sistem target dari kelemahan target sistem yang telah diperoleh dari hasil *scanning* serta *hacker* melakukan percobaan untuk memperoleh otoritas akses di sistem operasi, selanjutnya penyusup menyerang sistem seperti *passwordcracking* dan *denial of service*.

## 4. Mempertahankan Akses (*Maintaining access*)

*Maintaining access* adalah tahap proses dimana *hacker* telah mendapatkan akses ke sistem. Kemudian *hacker* menanamkan *backdoor* ke dalam sistem agar dia tetap mendapatkan akses tersebut.

## 5. Menghapus Tracks (*Clearing Tracks*)

*Clearing Tracks* adalah proses penyusup menghapus bermacam kegagalan didalam sistem yang dilalui agar penyusup tidak diketahui lokasinya, setelah itu penyusup menghapus rekam jejak log tersebut.

## 3.2 Kali Linux

### 3.3.1 Definisi

Kali Linux adalah distribusi berlandaskan distribusi Debian GNU/Linux untuk tujuan forensik digital dan di gunakan untuk pengujian penetrasi, yang dipelihara dan didanai oleh *Offensive Security*. Kali juga dikembangkan oleh *Offensive Security* sebagai penerus BackTrack Linux. Kali menyediakan pengguna dengan mudah akses terhadap koleksi yang besar dan komprehensif untuk alat yang berhubungan dengan keamanan, termasuk *port scanner* untuk *password cracker*. Pembangunan kembali BackTrack Linux secara sempurna, mengikuti sepenuhnya kepada standar pengembangan Debian. Semua infrastruktur baru telah dimasukkan ke dalam satu tempat, semua *tools* telah direview dan dikemas, dan menggunakan Git untuk VCS nya.

### 3.3.2 Kelebihan dan Kekurangan Kali Linux

Terdapat beberapa kelebihan yang ada pada Kali Linux yaitu:

1. **Open Source:** Linux merupakan salah satu sistem operasi *open source*, yang berarti memberi kesempatan kepada penggunanya untuk melihat program asal, dan atau mengubahnya sesuai keperluan tanpa terkena sanksi *property right* di bawah lisensi GNU.
2. **Minimal Hardware:** Linux tidak memerlukan *hardware* yang berspesifikasi tinggi. Minimal, *hardware* yang dibutuhkan adalah Prosesor intel 386 DX, dengan RAM minimal 8 MB, serta kapasitas hard disk minimal 85 MB. Untuk keperluan khusus, Linux dapat dijalankan hanya dengan satu atau dua disket saja, misalkan pada komputer *harddiskless* (tanpa harddisk) dan router.
3. **Kebal Virus:** Linux kebal terhadap virus DOS/Windows. Ini merupakan hal terpenting jika mempertimbangkan untuk menggunakan Linux. Linux juga mewarisi tradisi Unix dengan mendukung adanya *file permissions* (ijin *file*), yang dapat mencegah perubahan atau penghapusan *file* tanpa ijin dari pemiliknya. Karena itu virus pada dasarnya tidak dikenal di dunia Linux. Bahkan di Linux sendiri sampai saat ini belum ditemukan virus yang benar-benar bisa merusak sistem operasi. Hal ini dikarenakan Linux adalah sistem operasi terbuka, sehingga rasa kebersamaan yang ditimbulkannya

membuat Linux adalah milik setiap orang, bukan hanya milik pembuat atau pengembangnya saja.

4. **Multi-user:** Di mana lebih dari satu orang dapat menggunakan program yang sama atau berbeda dari satu mesin yang sama, pada saat bersamaan, di terminal yang sama atau berbeda.
5. **Login user:** Linux memiliki *login user* atau operator yang tidak terbatas jumlahnya sehingga memungkinkan pemakaian hingga 254 klien secara bersamaan, dan dilengkapi dengan password. 7
6. **Web Server:** Linux bisa digunakan sebagai Web Server dengan perangkat lunak Apache yang dapat digunakan sebagai basis *www*; Isi web server (*optional*).
7. **FTP Server:** Linux bisa digunakan sebagai FTP Server sehingga memungkinkan klien untuk *men-download* suatu program atau data pada saat yang bersamaan.
8. **Remote:** Server Linux dapat dikonfirmasi dan diperbaiki secara *remote* (jarak jauh).

Terdapat beberapa kekurangan yang ada pada Kali Linux yaitu :

1. Sistem operasi Kali Linux sulit untuk dipelajari, terutama yang belum mempunyai kemampuan komputer sama sekali.
2. Belum banyak aplikasi yang mendukung Linux
3. Tampilan dari sistem operasi ini kurang menarik
4. Tidak banyak dukungan dari hardware-hardware tertentu

### 3.3 VulnOS

#### 3.4.1 Definisi

VulnOS adalah rangkaian sistem operasi rentan yang dikemas sebagai gambar virtual untuk meningkatkan keterampilan pengujian penetrasi. VulnOS sendiri disediakan oleh Vulnhub yang merupakan situs web berbasis komunitas yang menyediakan akses ke lingkungan untuk para profesional keamanan yang bercita-cita tinggi atau berpengalaman. Mereka telah mengumpulkan sejumlah besar mesin dan jaringan virtual yang dapat diunduh untuk melatih keterampilan CyberSec ofensif atau defensif.

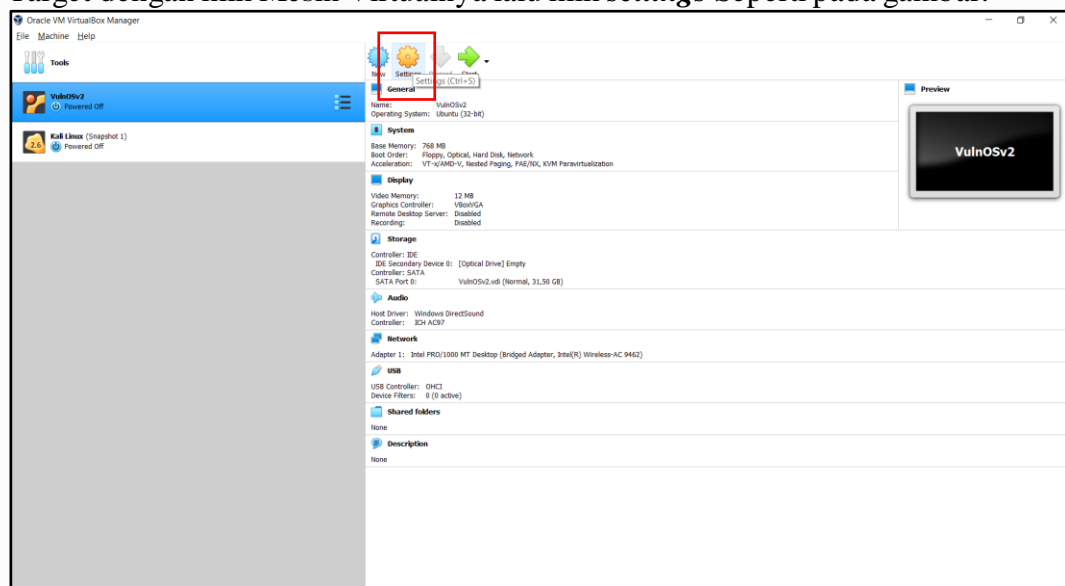


## IV. Lab Praktik

Pada lab praktik kali ini, akan menggunakan 2 sistem operasi yaitu yang pertama Kali Linux sebagai host (penyerang) dan VulnOS sebagai 'target'. Untuk melakukan uji simulasi *scenario* dunia nyata, maka VM VulnOS tidak akan diakses secara langsung melakukan konsol VM nya. Satu-satunya cara untuk mengaksesnya, yaitu melalui *platform* penyerang, dalam praktik kali ini yaitu menggunakan VM Kali Linux.

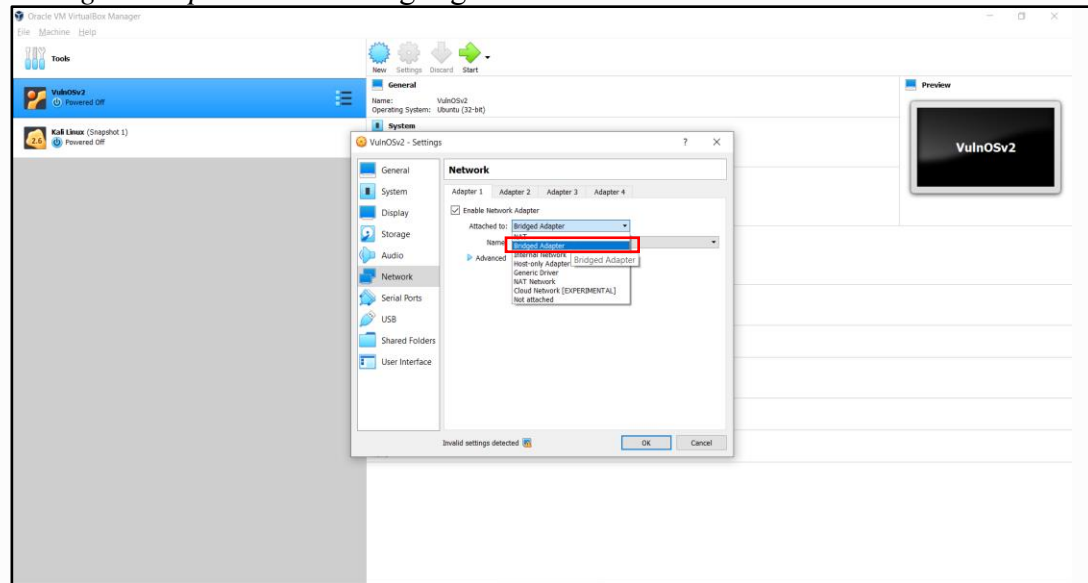
### 4.1 Settings Adapter pada VirtualBox

1. Pertama-tama sebelum menyalakan Mesin Virtual, atur *adapter Network* pada OS Target dengan klik Mesin Virtualnya lalu klik **settings** Seperti pada gambar.



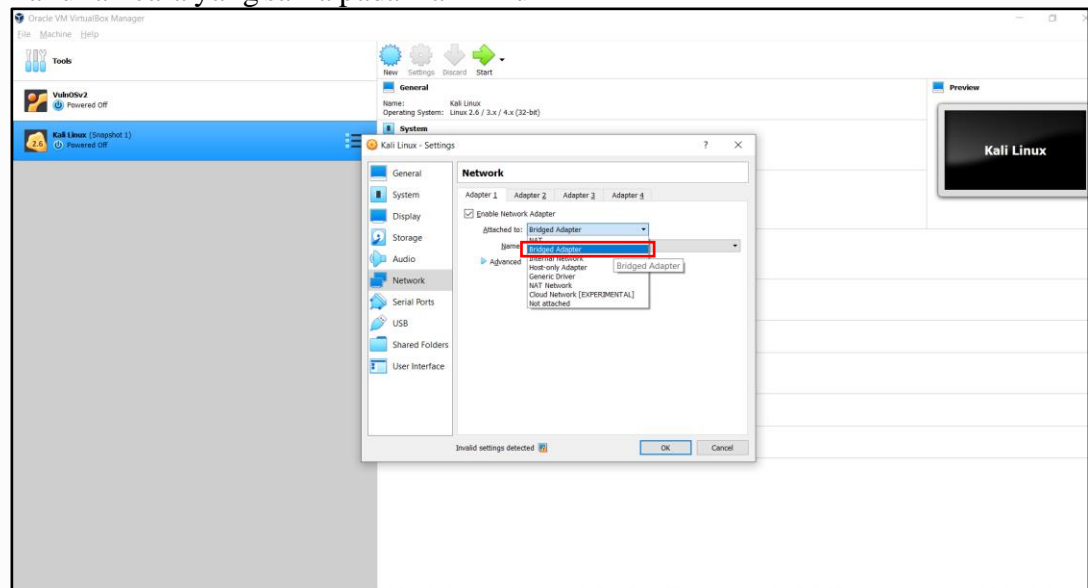
Gambar 4.1 Settings

2. Kemudian pilih opsi “Network” Lalu ubah pengaturan adapternya menjadi “Bridged Adapter” sesuai dengan gambar.



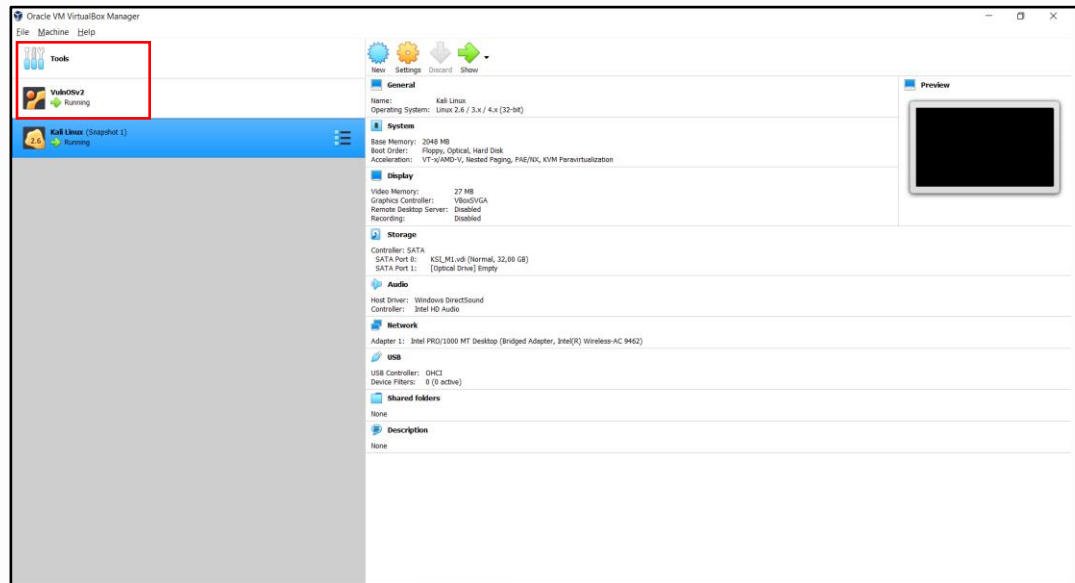
Gambar 4.2 Setting Bridged Adapter VulnOS

3. Lakukan cara yang sama pada Kali Linux



Gambar 4.3 Setting Bridged Adapter Kali Linux

#### 4. Setelah semuanya selesai, nyalakan kedua VirtualOS

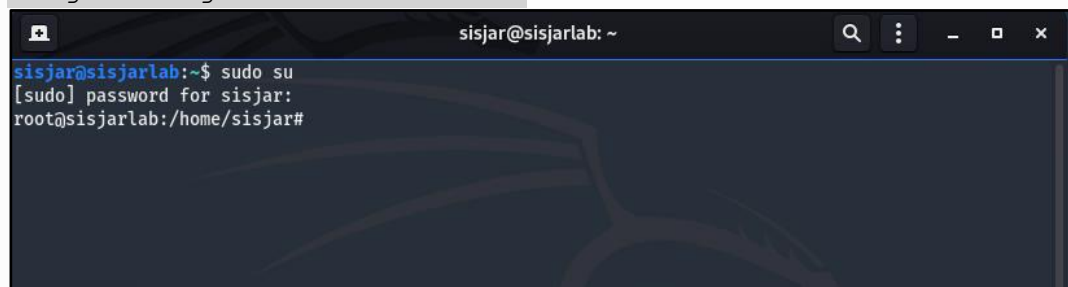


Gambar 4.4 Menyalakan VirtualOS

### 4.2 Praktik Information Gathering

1. Kemudian *Login* menggunakan *user root* pada terminal VM Kali Linux. Dengan perintah sebagai berikut:

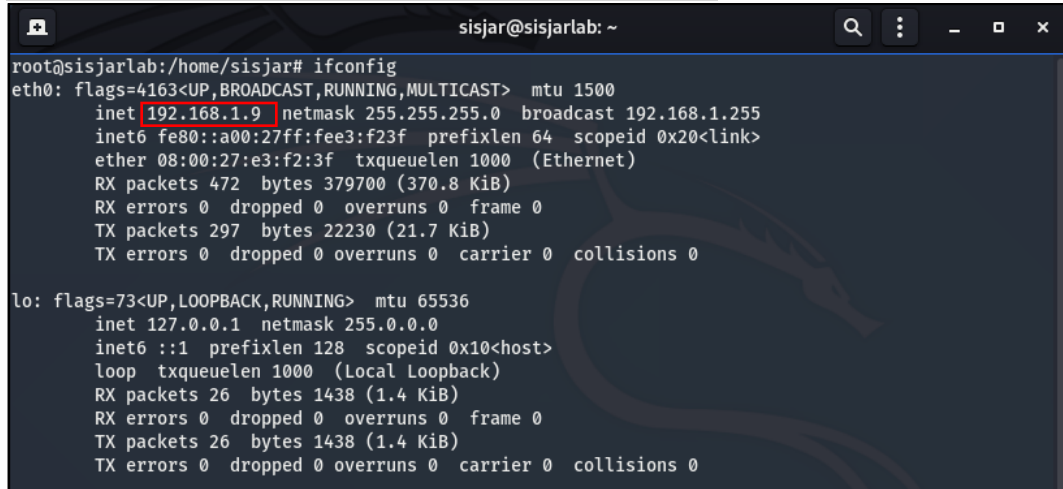
```
sisjar@sisjarlab:~$ sudo su
```



Gambar 4.5 Login menggunakan user root

2. Kemudian cek IP yang didapatkan oleh Kali Linux (IP berbeda menyesuaikan IP Wifi/Ethernet Masing-masing. Dengan perintah sebagai berikut:

```
root@sisjarlab:/home/sisjar# ifconfig
```



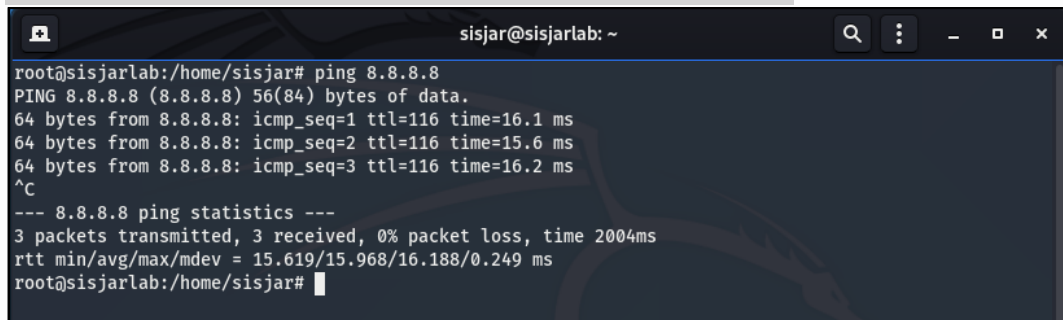
```
root@sisjarlab:/home/sisjar# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.9 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::a00:27ff:fee3:f23f prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:e3:f2:3f txqueuelen 1000 (Ethernet)
    RX packets 472 bytes 379700 (370.8 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 297 bytes 22230 (21.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 26 bytes 1438 (1.4 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 26 bytes 1438 (1.4 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Gambar 4.6 Mengecek IP Address

3. Selanjutnya pastikan Kali Linux dapat terhubung ke internet dengan melakukan ping ke alamat IP publik. Dengan perintah sebagai berikut:

```
root@sisjarlab:/home/sisjar# ping 8.8.8.8
```



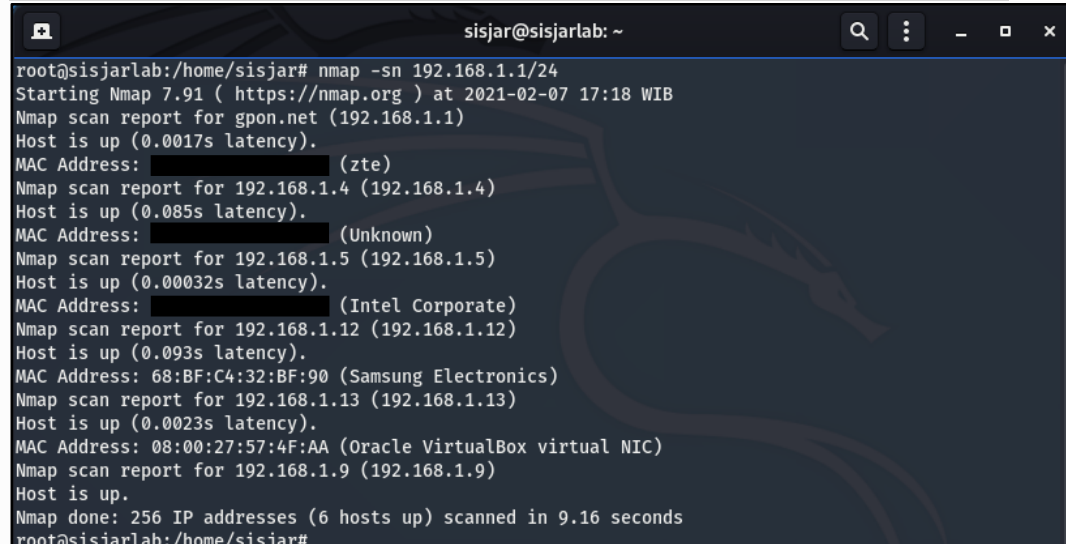
```
root@sisjarlab:/home/sisjar# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=116 time=16.1 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=116 time=15.6 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=116 time=16.2 ms
^C
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 15.619/15.968/16.188/0.249 ms
root@sisjarlab:/home/sisjar#
```

Gambar 4.7 Mengetes koneksi



4. Kemudian lakukan *scanning* menggunakan NMAP dengan menggunakan IP *gateway* dari IP address Kali Linux yang telah didapatkan pada tahap ke-6 atau “Wifi” masing-masing lakukan *scanning host* yang dalam kondisi menyala. Dengan perintah sebagai berikut:

```
root@sisjarlab:/home/sisjar# nmap -sn 192.168.1.1/24
```



```
sisjar@sisjarlab: ~
root@sisjarlab:/home/sisjar# nmap -sn 192.168.1.1/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-02-07 17:18 WIB
Nmap scan report for gpon.net (192.168.1.1)
Host is up (0.0017s latency).
MAC Address: [REDACTED] (zte)
Nmap scan report for 192.168.1.4 (192.168.1.4)
Host is up (0.085s latency).
MAC Address: [REDACTED] (Unknown)
Nmap scan report for 192.168.1.5 (192.168.1.5)
Host is up (0.00032s latency).
MAC Address: [REDACTED] (Intel Corporate)
Nmap scan report for 192.168.1.12 (192.168.1.12)
Host is up (0.093s latency).
MAC Address: 68:BF:C4:32:BF:90 (Samsung Electronics)
Nmap scan report for 192.168.1.13 (192.168.1.13)
Host is up (0.0023s latency).
MAC Address: 08:00:27:57:4F:AA (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.1.9 (192.168.1.9)
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 9.16 seconds
root@sisjarlab:/home/sisjar#
```

Gambar 4.8 *Scanning* menggunakan NMAP

5. Untuk dapat mengetahui IP dari target, yaitu dapat dengan cara mencoba semua IP yang di dapatkan dari hasil scan tahap sebelumnya dengan menggunakan *web browser*. Berikut merupakan IP 192.168.1.13 target yang telah di dapatkan dan kemudia ingat IP *address* dari target yang berhasil didapatkan.

```
MAC Address: 68:BF:C4:32:BF:90 (Samsung Electronics)
Nmap scan report for 192.168.1.13 (192.168.1.13)
Host is up (0.0023s latency).
```

Gambar 4.9 IP Target (VulnOS)

6. Selanjutnya identifikasi servis-servis yang terdapat pada VulnOS dengan NMAP. Dengan perintah sebagai berikut:

```
root@sisjarlab:/home/sisjar# nmap -sT -sV -A -O -v -p
1-65535 192.168.1.13
```

```

root@sisjarlab:/home/sisjar# nmap -sT -sV -A -O -v -p 1-65535 192.168.1.13
Starting Nmap 7.91 ( https://nmap.org ) at 2021-02-07 17:25 WIB
NSE: Loaded 153 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 17:25
Completed NSE at 17:25, 0.00s elapsed
Initiating NSE at 17:25
Completed NSE at 17:25, 0.00s elapsed
Initiating NSE at 17:25
Completed NSE at 17:25, 0.00s elapsed
Initiating ARP Ping Scan at 17:25
Scanning 192.168.1.13 [1 port]
Completed ARP Ping Scan at 17:25, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:25
Completed Parallel DNS resolution of 1 host. at 17:25, 6.51s elapsed
Initiating Connect Scan at 17:25
Scanning 192.168.1.13 (192.168.1.13) [65535 ports]
Discovered open port 80/tcp on 192.168.1.13
Discovered open port 22/tcp on 192.168.1.13
Discovered open port 6667/tcp on 192.168.1.13
Completed Connect Scan at 17:25, 2.61s elapsed (65535 total ports)
Initiating Service scan at 17:25
Scanning 3 services on 192.168.1.13 (192.168.1.13)
Completed Service scan at 17:25, 11.02s elapsed (3 services on 1 host)
Initiating OS detection (try #1) against 192.168.1.13 (192.168.1.13)

```

Gambar 4.10 Scanning Menggunakan NMAP berdasarkan *service* tertentu

```

root@sisjarlab:/home/sisjar# nmap -sT -sV -A -O -v -p 1-65535
192.168.1.13
Starting Nmap 7.91 ( https://nmap.org ) at 2021-02-07 17:25 WIB
NSE: Loaded 153 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 17:25
Completed NSE at 17:25, 0.00s elapsed
Initiating NSE at 17:25
Completed NSE at 17:25, 0.00s elapsed
Initiating NSE at 17:25
Completed NSE at 17:25, 0.00s elapsed
Initiating ARP Ping Scan at 17:25
Scanning 192.168.1.13 [1 port]
Completed ARP Ping Scan at 17:25, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:25
Completed Parallel DNS resolution of 1 host. at 17:25, 6.51s elapsed
Initiating Connect Scan at 17:25
Scanning 192.168.1.13 (192.168.1.13) [65535 ports]
Discovered open port 80/tcp on 192.168.1.13
Discovered open port 22/tcp on 192.168.1.13
Discovered open port 6667/tcp on 192.168.1.13
Completed Connect Scan at 17:25, 2.61s elapsed (65535 total ports)
Initiating Service scan at 17:25
Scanning 3 services on 192.168.1.13 (192.168.1.13)
Completed Service scan at 17:25, 11.02s elapsed (3 services on 1 host)
Initiating OS detection (try #1) against 192.168.1.13 (192.168.1.13)

```

```

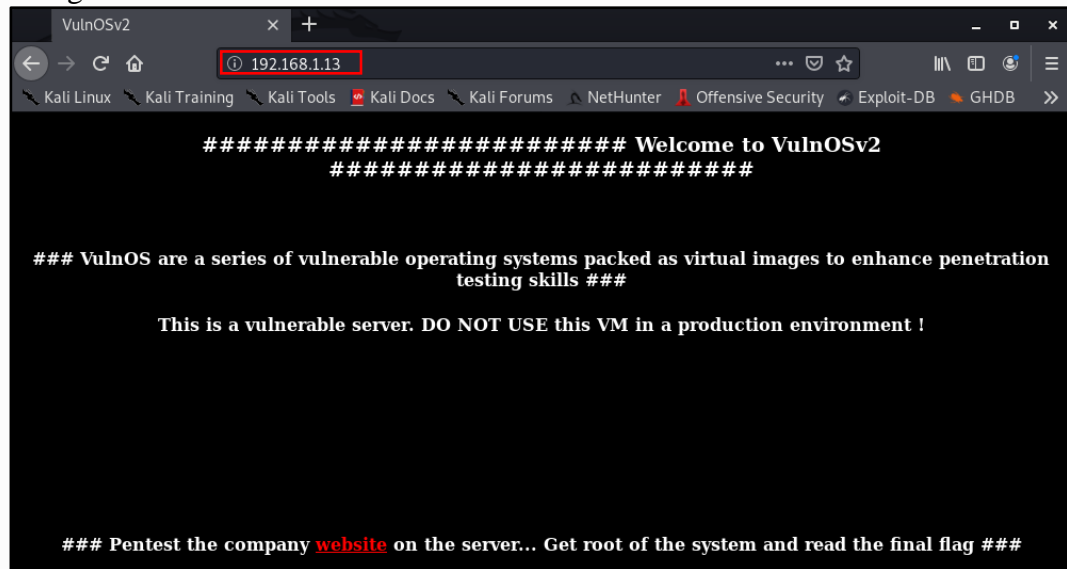
NSE: Script scanning 192.168.1.13.
Initiating NSE at 17:25
Completed NSE at 17:26, 7.11s elapsed
Initiating NSE at 17:26
Completed NSE at 17:26, 0.01s elapsed
Initiating NSE at 17:26
Completed NSE at 17:26, 0.00s elapsed
Nmap scan report for 192.168.1.13 (192.168.1.13)
Host is up (0.00044s latency).
Not shown: 65532 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.6 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   1024 f5:4d:c8:e7:8b:c1:b2:11:95:24:fd:0e:4c:3c:3b:3b (DSA)
|   2048 ff:19:33:7a:c1:ee:b5:d0:dc:66:51:da:f0:6e:fc:48 (RSA)
|   256 ae:d7:6f:cc:ed:4a:82:8b:e8:66:a5:11:7a:11:5f:86 (ECDSA)
|_  256 71:bc:6b:7b:56:02:a4:8e:ce:1c:8e:a6:1e:3a:37:94 (ED25519)
80/tcp    open  http      Apache httpd 2.4.7 ((Ubuntu))
|_ http-methods:
|_   Supported Methods: GET HEAD POST OPTIONS
|_ http-server-header: Apache/2.4.7 (Ubuntu)
|_ http-title: VulnOSv2
6667/tcp  open  irc       ngircd
MAC Address: 08:00:27:57:4F:AA (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Uptime guess: 0.017 days (since Sun Feb  7 17:01:02 2021)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Host: irc.example.net; OS: Linux; CPE:
cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1   0.44 ms  192.168.1.13 (192.168.1.13)

NSE: Script Post-scanning.
Initiating NSE at 17:26
Completed NSE at 17:26, 0.00s elapsed
Initiating NSE at 17:26
Completed NSE at 17:26, 0.00s elapsed
Initiating NSE at 17:26
Completed NSE at 17:26, 0.00s elapsed
Read data files from: /usr/bin/./share/nmap
OS and Service detection performed. Please report any incorrect results
at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 29.77 seconds
Raw packets sent: 23 (1.806KB) | Rcvd: 16 (1.330KB)
root@sisjarlab:/home/sisjar#

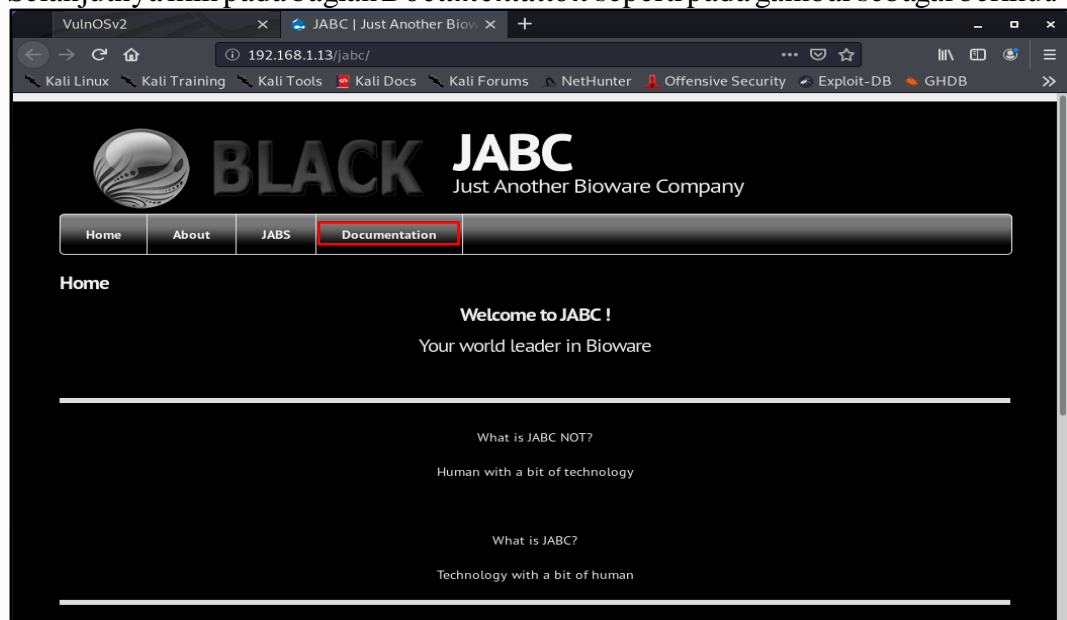
```

7. Buka IP target (VulnOS) pada *web browser* dan klik tulisan **website** pada gambar sebagai berikut:



Gambar 4.11 Membuka IP Target pada Browser

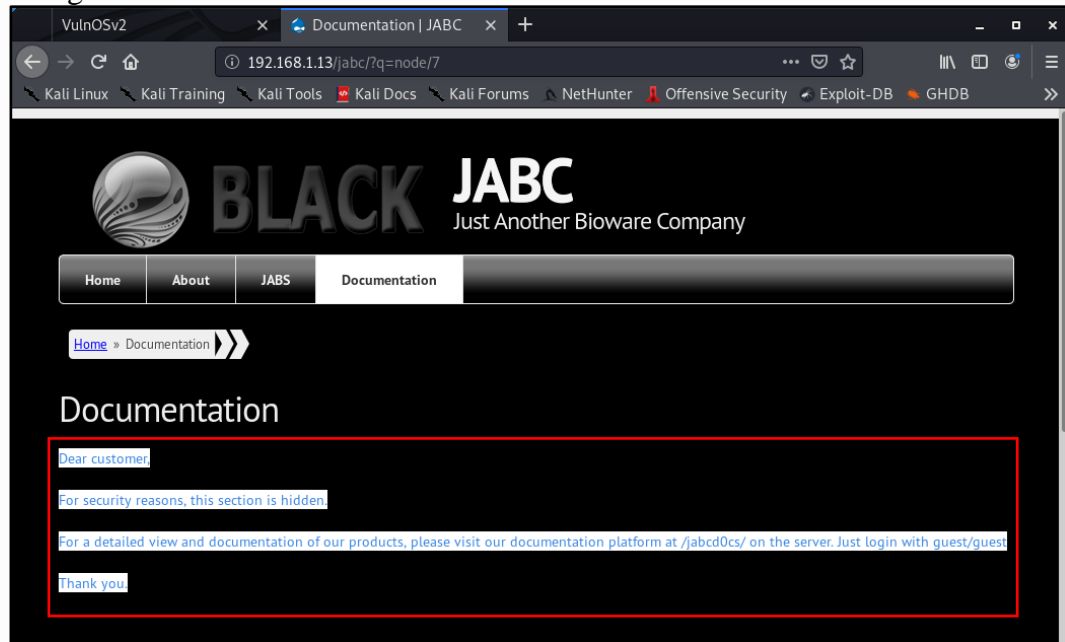
8. Berikut merupakan tampilan home setelah klik **website** pada tahap sebelumnya. Selanjutnya klik pada bagian **Documentation** seperti pada gambar sebagai berikut:



Gambar 4.12 Tampilan Home JABC

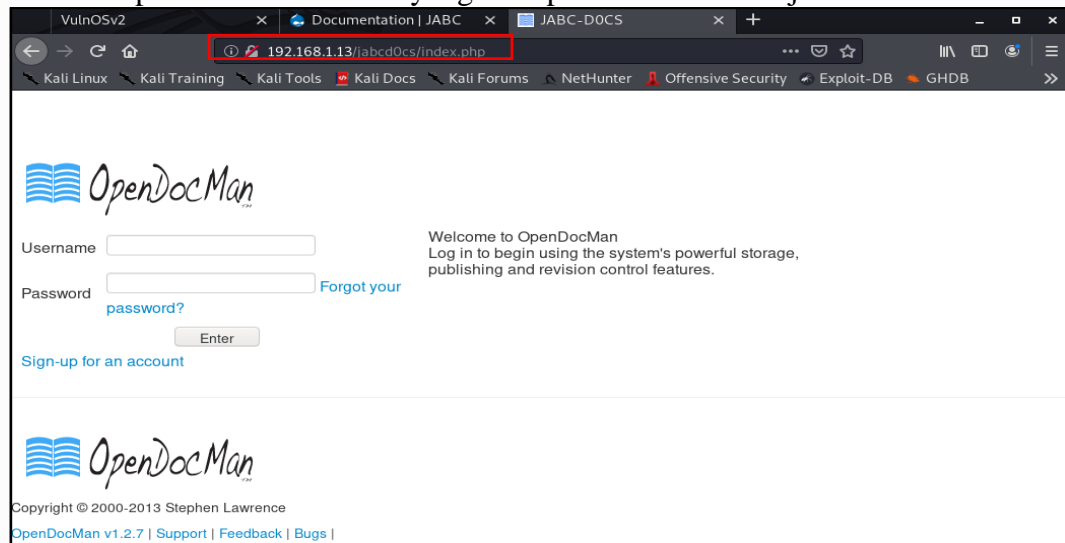


9. Kemudian **block** halaman blank dengan menggunakan kursor seperti pada gambar sebagai berikut:



Gambar 4.13 Halaman Dokumentasi

10. Browsing dengan *clue* alamat yang ditemukan pada tahap sebelumnya, kemudian akan didapatkan halaman baru yang merupakan sistem manajemen dokumen :



Gambar 4.14 Halaman Jabcdocs

## Daftar Pustaka

---

Oriyano, S. (2016). *CEH v9 Certified Ethical Hacker Version 9*. Indianapolis, Indiana.

*VulnOS Walkthrough*. (2021, January 31). Retrieved from  
<https://medium.com/@Kan1shka9/vulnos-2-walkthrough-16b70b9fbe17>