

L1 SOC ANALYST

# Modul Praktikum 1

Melakukan Deteksi Kerentanan Aset Teknologi Informasi



J.62SOC00.006.1

## **MODUL PRAKTIKUM L1 SOC ANALYST**

### **Unit Kompetensi**

Melakukan Deteksi Kerentanan Aset Teknologi Informasi

### **Tujuan Praktikum**

1. Mengoperasikan NMAP, OWASP ZAP, Dirbuster
2. Membedakan Bagian Aset yang Merupakan Kerentanan dan bukan Kerentanan

## Penggunaan NMAP dalam Vurnerabilty Assesment (P.6.1.A)

### Skenario Praktikum

Anda adalah seorang *L1 SOC Analyst* yang bekerja di Pemerintah Daerah Kabupaten Lengkeng. Anda memiliki tugas untuk mengawasi dan memantau seluruh aktivitas jaringan ke dalam infrastruktur TI Pemkab Lengkeng dengan bantuan SIEM. Dalam menjalankan tugas ini, Anda harus memiliki kemampuan untuk mengetahui kerentanan yang dimiliki oleh aset yang anda awasi sehingga menuntut anda untuk mampu mengoperasikan tools *vurnerability assement*.

Pemerintah Daerah Kabupaten Lengkeng memiliki Layanan Web SPPD belum pernah dilakukan *vurnerabilty assesment* dan *penetration testing*. Layanan web tersebut ditempatkan pada VM Target Web 1. Untuk mengetahui *port* apa saja yang menimbulkan kerentanan, anda akan melakukan *vurnerabilty assessment* tahap *reconnaissance* dan *scanning* menggunakan NMAP.

### Tujuan Praktikum

Praktikum ini bertujuan untuk membantu peserta didik dalam mengoperasikan NMAP dalam mengidentifikasi kerentanan

### Enviroment Laboratorium Virtual

Praktikum ini membutuhkan:

- VM Kali Linux
- VM Target Web 1.

### Durasi Praktikum

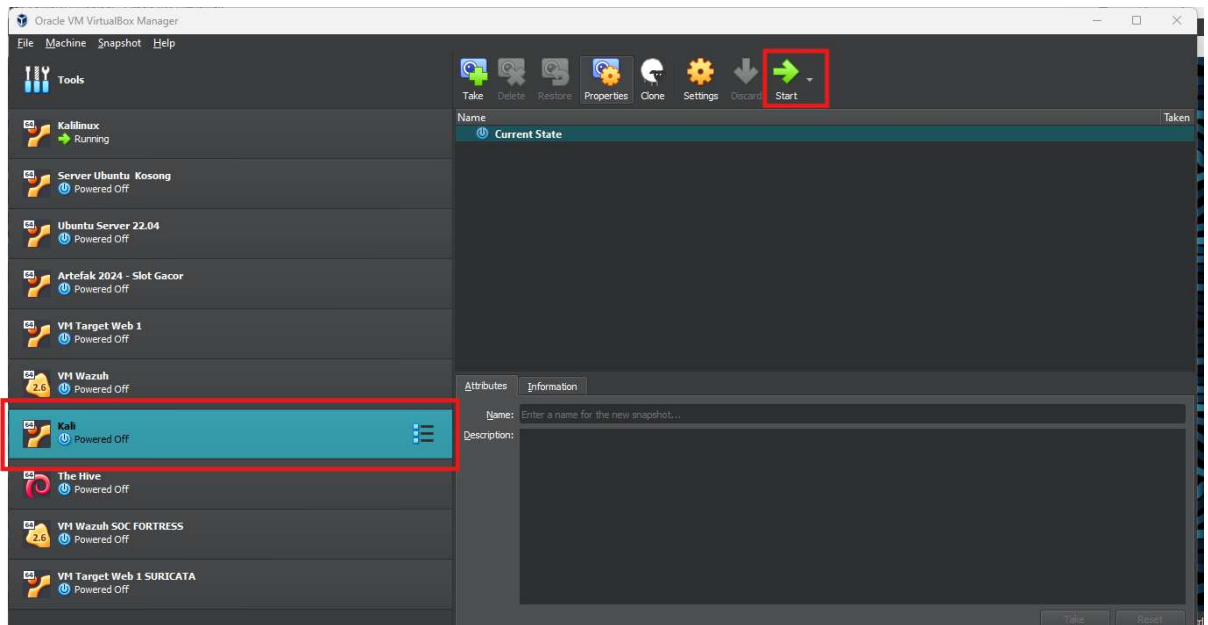
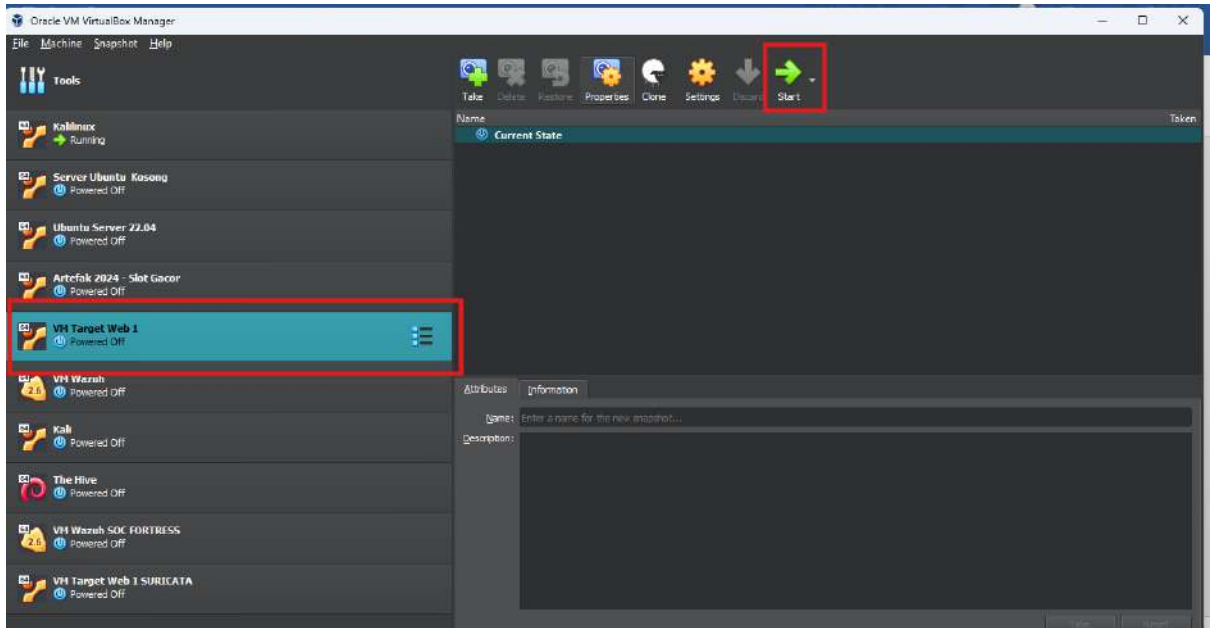
10 Menit

### Catatan Khusus

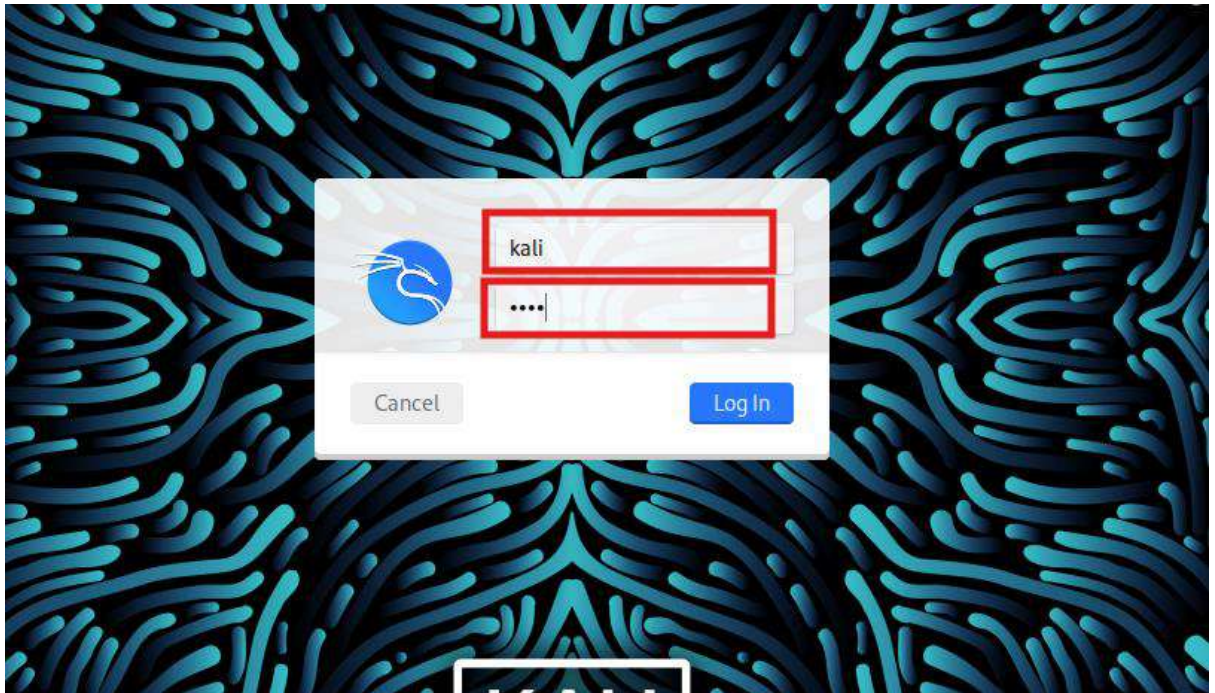
- Siapkan *enviroment* laboratorium virtual sesuai panduan instalasi laboratorium virtual
- Dokumentasikan setiap langkah praktikum karena dapat membantu menjawab pertanyaan pada soal yang diberikan

### Langkah-Langkah

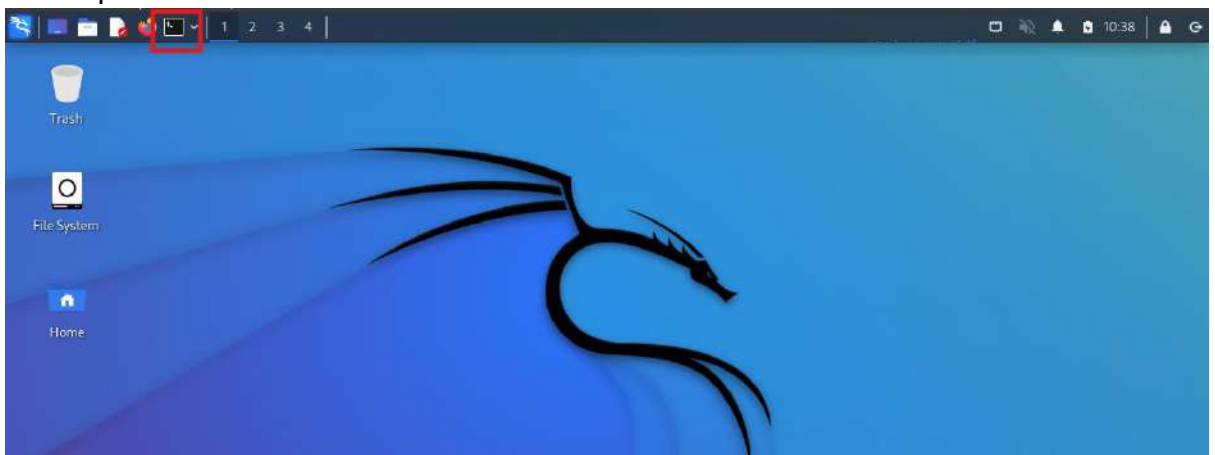
1. Siapkan Virtualbox, nyalakan VM Target Web 1 dan VM Kali dengan menekan virtual machine pada Virtual box lalu menekan start



2. Buka pada VM Kali dan masukan *username* kali dan *password* kali



3. Setelah masuk kedalam tampilan awal dekstop, buka terminal pada kiri atas dekstop



4. Cek IP Kali apakah sudah satu jaringan dengan IP VM Web Target 1 dengan ifconfig ( IP Kali dan IP VM Web Target 1 seharusnya berada pada 10.0.1.0/24 jika dalam enviroment disiapkan dengan benar)

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
└─$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 10.0.1.12 netmask 255.255.255.0 broadcast 10.0.1.255  
    ineto res0::a00:27ff:fe17:2c4a prefixlen 64 scopeid 0x20<link>  
    ether 08:00:27:17:2c:4a txqueuelen 1000 (Ethernet)  
    RX packets 55 bytes 3830 (3.7 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 22 bytes 3034 (2.9 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 0 bytes 0 (0.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 0 bytes 0 (0.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

- Beralih ke VM Web Target 1, cek IP apakah sudah pada network yang sama dengan Kali, login terlebih dahulu dengan `username` `serveradmin` dan `password` `ubuntu` lalu jalankan perintah `ifconfig` ( IP Kali dan IP VM Web Target 1 seharusnya berada pada `10.0.1.0/24` jika dalam `enviroment` disiapkan dengan benar)

```
Ubuntu 22.04.2 LTS websppd tty1
websppd login: [ 35.716544] cloud-init[1533]: Cloud-init v. 23.1.2-0ubuntu0~22.04.1 running 'mode
es:final' at Sat, 12 Apr 2025 14:37:50 +0000. Up 35.68 seconds.
[ 35.798099] cloud-init[1533]: Cloud-init v. 23.1.2-0ubuntu0~22.04.1 finished at Sat, 12 Apr 2025
14:37:50 +0000. Datasource DataSourceNone. Up 35.79 seconds
[ 35.798773] cloud-init[1533]: 2025-04-12 14:37:50,938 - cc_final_message.py[WARNING]: Used fallback
datasource

websppd login: serveradmin
Password: _

serveradmin@websppd:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.1.11 netmask 255.255.255.0 broadcast 10.0.1.255
    inet6 fe80::d00:27ff:fead:9c1b prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:ad:9c:1b txqueuelen 1000 (Ethernet)
    RX packets 277 bytes 344725 (344.7 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 366 bytes 29451 (29.4 KB)
    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 152 bytes 12704 (12.7 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 152 bytes 12704 (12.7 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

serveradmin@websppd:~$ _
```

- Buka kembali Kali dan buka pada terminal, untuk mengetahui perangkat mana saja yang berada dalam jaringan yang sama lakukan NMAP pada network dengan perintah `nmap 10.0.1.0/24`. Tahapan ini dapat digunakan dalam mendeteksi perangkat apa saja yang berada didalam jaringan dan sangat bermanfaat jika anda tidak mengetahui IP target anda

```
serveradmin@kali:~$ nmap 10.0.1.0/24
Starting Nmap 7.92 (https://nmap.org) at 2025-04-12 10:46 EDT
Nmap scan report for 10.0.1.1
Host is up (0.00059s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
53/tcp    open  domain

Nmap scan report for 10.0.1.11
Host is up (0.00069s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http

Nmap scan report for 10.0.1.12
Host is up (0.00071s latency).
All 1000 scanned ports on 10.0.1.12 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap done: 256 IP addresses (3 hosts up) scanned in 8.40 seconds
```

Hasil menunjukkan bahwa hanya terdapat satu perangkat yaitu dengan IP 10.1.11. Hasil nmap akan menunjukan banyak IP jika didalam network terdapat banyak perangkat yang terhubung

7. Lanjutkan *scanning* dengan langsung merujuk pada IP VM Web Target, tambahkan `-sV` untuk mengetahui versi layanan yang ada dengan perintah `nmap 10.0.1.11 -sV -sS`

```
(kali@kali)-[~]
└─$ nmap 10.0.1.11 -sV
Starting Nmap 7.92 ( https://nmap.org ) at 2025-04-12 10:50 EDT
Nmap scan report for 10.0.1.11
Host is up (0.0023s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
22/tcp    open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.11 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.52 ((Ubuntu))
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.85 seconds
```

8. Dalam beberapa kasus, melakukan *scanning* akan membuat beban pada target, untuk menghindari hal tersebut dapat ditambahkan `-sS` pada perintah `nmap 10.0.1.11 -sV -sS`. Dengan perintah tersebut, *scanning* akan menjadi lebih ringan dan cepat.

```
(kali@kali)-[~]
└─$ sudo nmap 10.0.1.11 -sV -sS
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2025-04-12 10:52 EDT
Nmap scan report for 10.0.1.11
Host is up (0.00064s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
22/tcp    open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.11 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.52 ((Ubuntu))
MAC Address: 08:00:27:AD:9C:1B (Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.61 seconds
```

9. Untuk berfokus pada satu IP saja, dapat menambahkan `-p` pada perintah, `nmap 10.0.1.11 -sV -p <port yang diinginkan>`. Gambar ini contoh dilakukan *scanning* pada port 21

```
(kali@kali)-[~]
└─$ sudo nmap 10.0.1.11 -sV -p 21
Starting Nmap 7.92 ( https://nmap.org ) at 2025-04-12 10:55 EDT
Nmap scan report for 10.0.1.11
Host is up (0.0012s latency).
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
MAC Address: 08:00:27:AD:9C:1B (Oracle VirtualBox virtual NIC)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.47 seconds
```

10. Untuk menampilkan progres dan detail tambahan dapat ditambahkan `-v` pada perintah. Perintah dapat menjadi `nmap 10.0.1.11 -v -sV -p <port yang diinginkan>`

```
(kali@kali) [~]
└─$ sudo nmap 10.0.1.11 -sV -v -p 21
Starting Nmap 7.92 ( https://nmap.org ) at 2025-04-12 10:56 EDT
NSE: Loaded 45 scripts for scanning.
Initiating ARP Ping Scan at 10:56
scanning 10.0.1.11 [1 port]
Completed ARP Ping Scan at 10:56, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:56
Completed Parallel DNS resolution of 1 host. at 10:56, 0.13s elapsed
Initiating SYN Stealth Scan at 10:56
Scanning 10.0.1.11 [1 port]
Discovered open port 21/tcp on 10.0.1.11
Completed SYN Stealth Scan at 10:56, 0.03s elapsed (1 total ports)
Initiating Service scan at 10:56
scanning 1 service on 10.0.1.11
Completed Service scan at 10:56, 0.00s elapsed (1 service on 1 host)
NSE: Script scanning 10.0.1.11.
Initiating NSE at 10:56
Completed NSE at 10:56, 0.00s elapsed
Initiating NSE at 10:56
Completed NSE at 10:56, 0.00s elapsed
Nmap scan report for 10.0.1.11
Host is up (0.00098s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
MAC Address: 08:00:27:AD:9C:1B (Oracle VirtualBox virtual NIC)
Service Info: OS: Unix
```

11. Gunakan -A untuk mengetahui versi layanan, sistem operasi target, dan banner dengan perintah `nmap 10.0.1.11 -A -sV -p <port yang diinginkan>`

```
(kali@kali) [~]
└─$ sudo nmap 10.0.1.11 -sV -A -p 80
Starting Nmap 7.92 ( https://nmap.org ) at 2025-04-12 10:58 EDT
Nmap scan report for 10.0.1.11
Host is up (0.0010s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.52 ((Ubuntu))
|_ http-server-header: Apache/2.4.52 (Ubuntu)
|_ http-title: Login SPPD
MAC Address: 08:00:27:AD:9C:1B (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   1.03 ms 10.0.1.11

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 8.18 seconds
```

## Penggunaan Dirbuster dalam Vurnerabilty Assesment (P.6.1.A)

### Skenario Praktikum

Anda adalah seorang *L1 SOC Analyst* yang bekerja di Pemerintah Daerah Kabupaten Lengkeng. Anda memiliki tugas untuk mengawasi dan memantau seluruh aktivitas jaringan ke dalam infrastruktur TI Pemkab Lengkeng dengan bantuan SIEM. Dalam menjalankan tugas ini, Anda harus memiliki kemampuan untuk mengetahui kerentanan yang dimiliki oleh aset yang anda awasi sehingga menuntut anda untuk mampu mengoperasikan tools *vurnerability assement*.

Pemerintah Daerah Kabupaten Lengkeng memiliki Layanan Web SPPD belum pernah dilakukan *vurnerabilty assesment* dan *penetration testing*. Layanan web tersebut ditempatkan pada VM Target Web 1. Untuk mengetahui *port* apa saja yang menimbulkan kerentanan, anda akan melakukan *vurnerabilty assesment* tahap *enumeration* menggunakan Dirbuster.

### Tujuan Praktikum

Praktikum ini bertujuan untuk membantu peserta didik dalam mengoperasikan NMAP dalam mengidentifikasi kerentanan

### Enviroment Laboratorium Virtual

Praktikum ini membutuhkan:

- VM Kali Linux
- VM Target Web 1.

### Durasi Praktikum

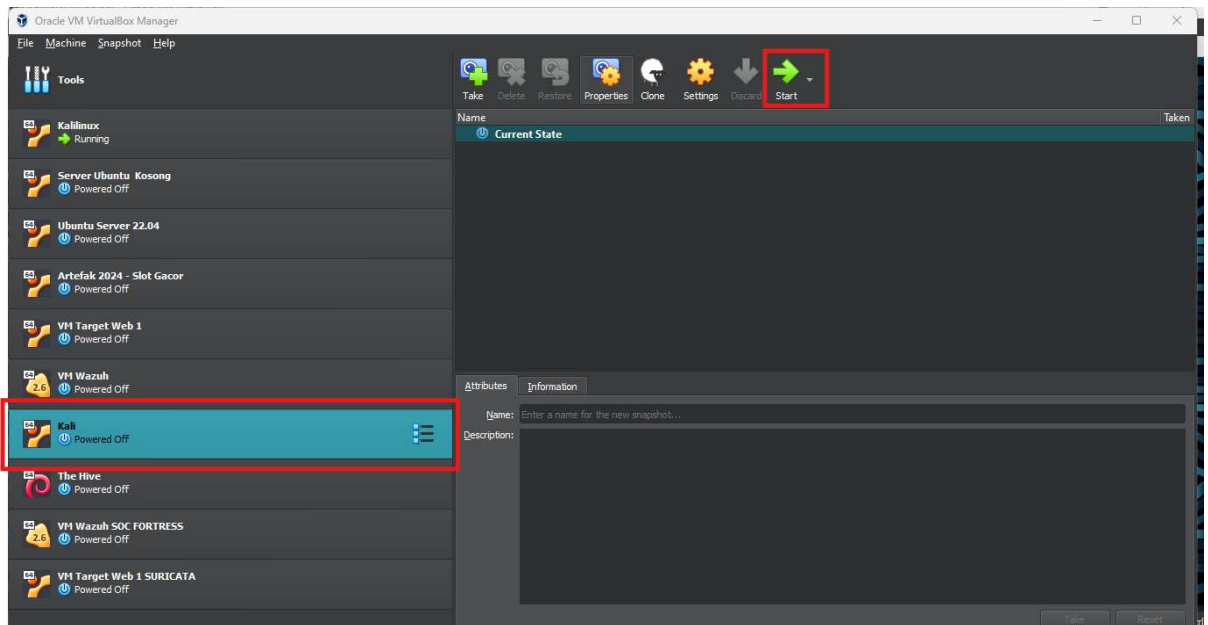
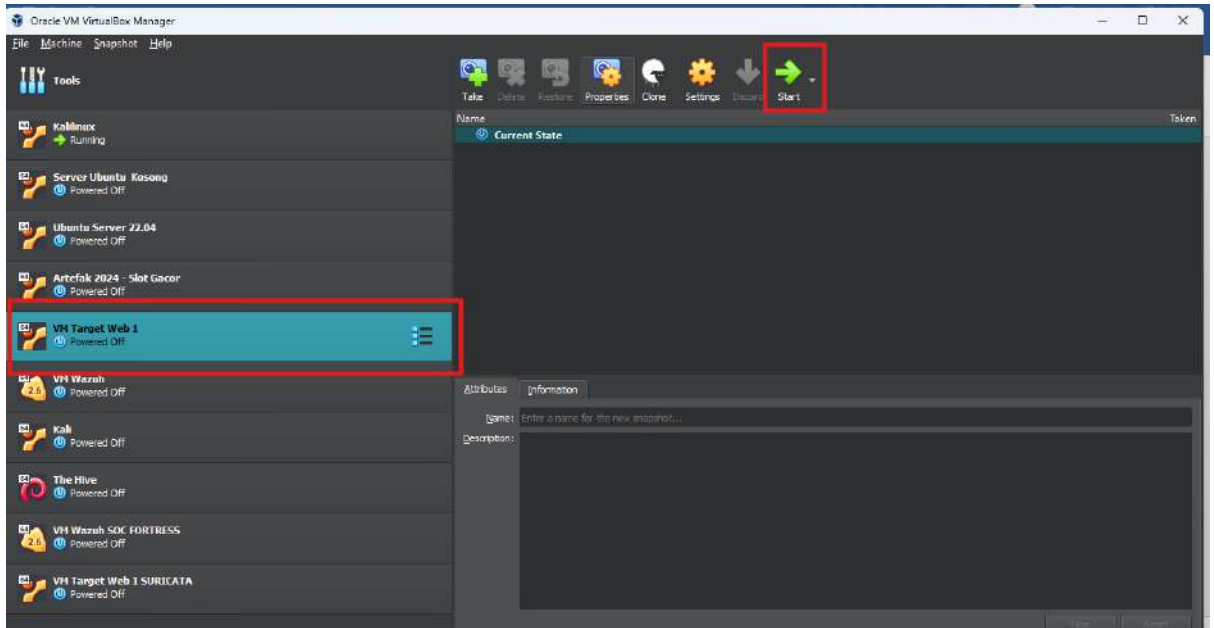
10 Menit

### Catatan Khusus

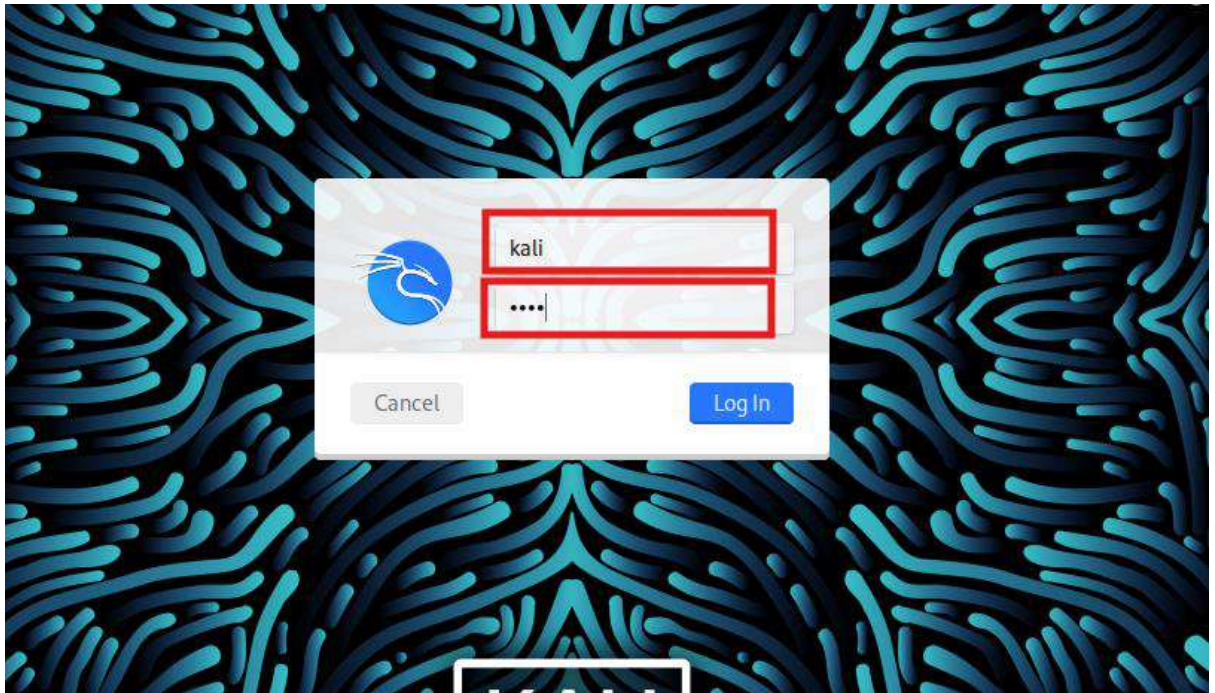
- Siapkan *enviroment* laboratorium virtual sesuai panduan instalasi laboratorium virtual
- Dokumentasikan setiap langkah praktikum karena dapat membantu menjawab pertanyaan pada soal yang diberikan

### Langkah-Langkah

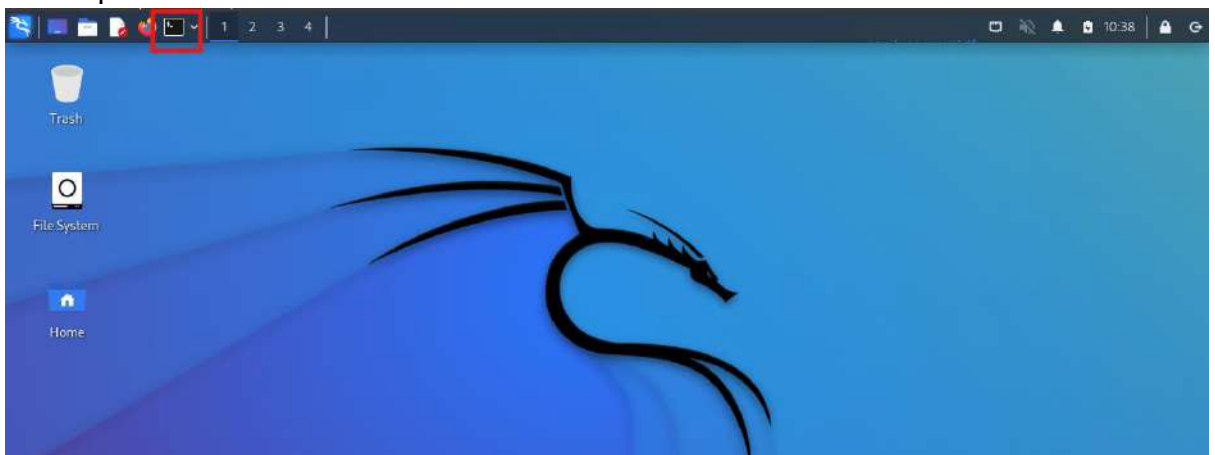
1. Siapkan Virtualbox, nyalakan VM Target Web 1 dan VM Kali dengan menekan virtual machine pada Virtual box lalu menekan start



2. Buka pada VM Kali dan masukan *username* kali dan *password* kali



3. Setelah masuk kedalam tampilan awal dekstop, buka terminal pada kiri atas dekstop



4. Cek IP Kali apakah sudah satu jaringan dengan IP VM Web Target 1 dengan ifconfig ( IP Kali dan IP VM Web Target 1 seharusnya berada pada 10.0.1.0/24 jika dalam enviroment disiapkan dengan benar)

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
└─$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 10.0.1.12 netmask 255.255.255.0 broadcast 10.0.1.255  
    inet6 fe80::a00:27ff:fe17:2c4a prefixlen 64 scopeid 0x20<link>  
    ether 08:00:27:17:2c:4a txqueuelen 1000 (Ethernet)  
    RX packets 55 bytes 3830 (3.7 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 22 bytes 3034 (2.9 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 0 bytes 0 (0.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 0 bytes 0 (0.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

5. Beralih ke VM Web Target 1, cek IP apakah sudah pada network yang sama dengan Kali, login terlebih dahulu dengan *username* *serveradmin* dan *password* *ubuntu* lalu jalankan perintah *ifconfig* ( IP Kali dan IP VM Web Target 1 seharusnya berada pada 10.0.1.0/24 jika dalam *enviroment* disiapkan dengan benar)

```
Ubuntu 22.04.2 LTS websppd tty1
websppd login: [ 35.716544] cloud-init[1533]: Cloud-init v. 23.1.2-0ubuntu0~22.04.1 running 'modu
es:final' at Sat, 12 Apr 2025 14:37:50 +0000. Up 35.68 seconds.
[ 35.798099] cloud-init[1533]: Cloud-init v. 23.1.2-0ubuntu0~22.04.1 finished at Sat, 12 Apr 2025
14:37:50 +0000. Datasource DataSourceNone. Up 35.79 seconds
[ 35.798773] cloud-init[1533]: 2025-04-12 14:37:50,938 - cc_final_message.py[WARNING]: Used fallback
datasource

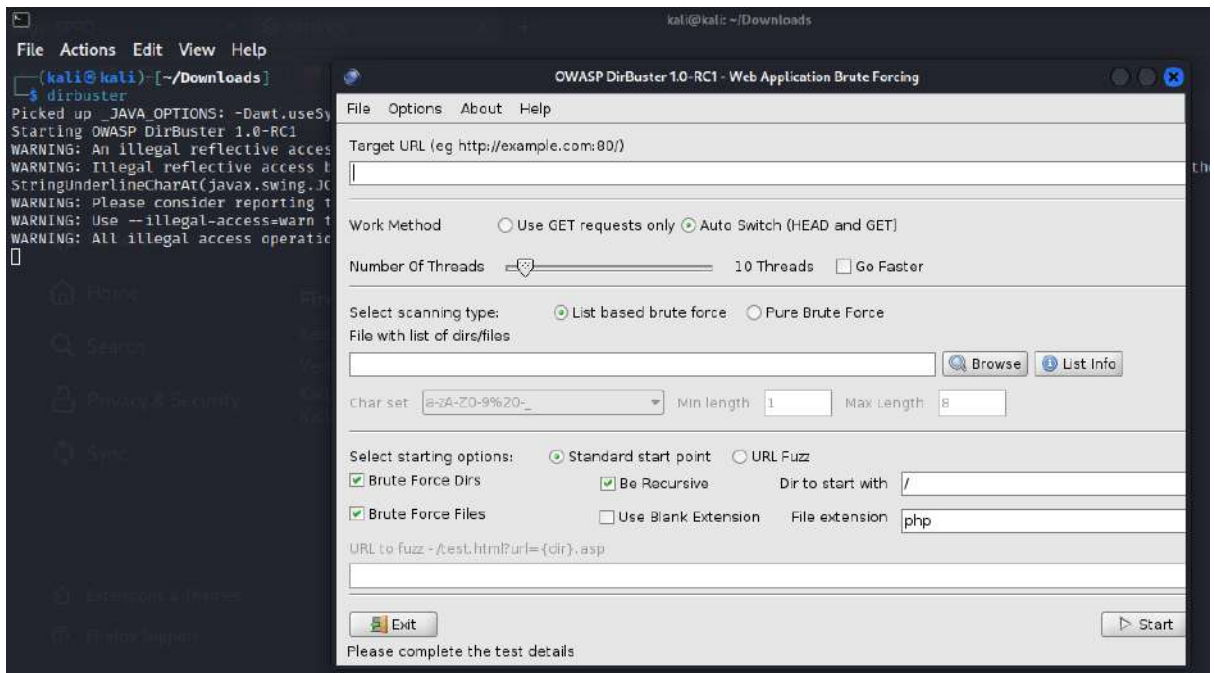
websppd login: serveradmin
Password: _

serveradmin@websppd:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.1.11 netmask 255.255.255.0 broadcast 10.0.1.255
    inet6 fe80::d3:27ff:fead:9c1b prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:ad:9c:1b txqueuelen 1000 (Ethernet)
    RX packets 277 bytes 344725 (344.7 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 366 bytes 29451 (29.4 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

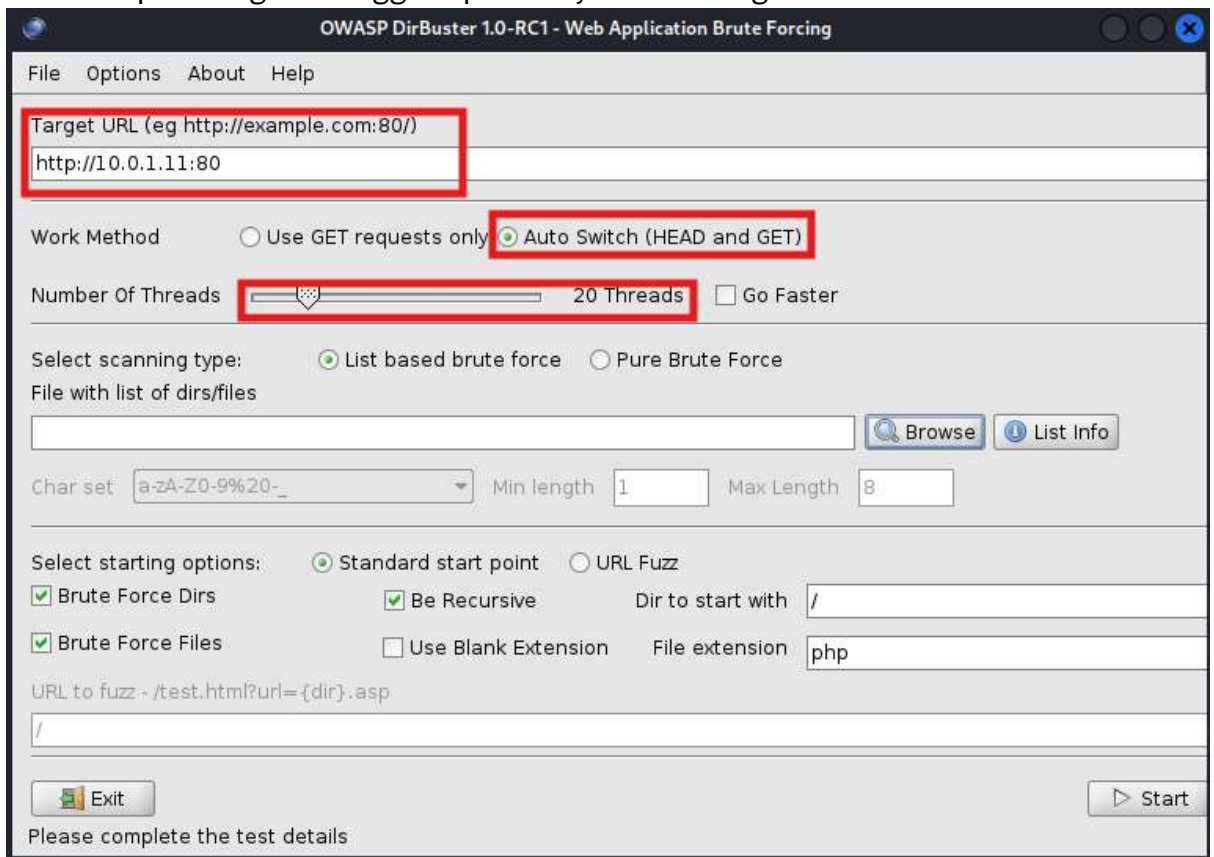
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 152 bytes 12704 (12.7 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 152 bytes 12704 (12.7 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

serveradmin@websppd:~$ _
```

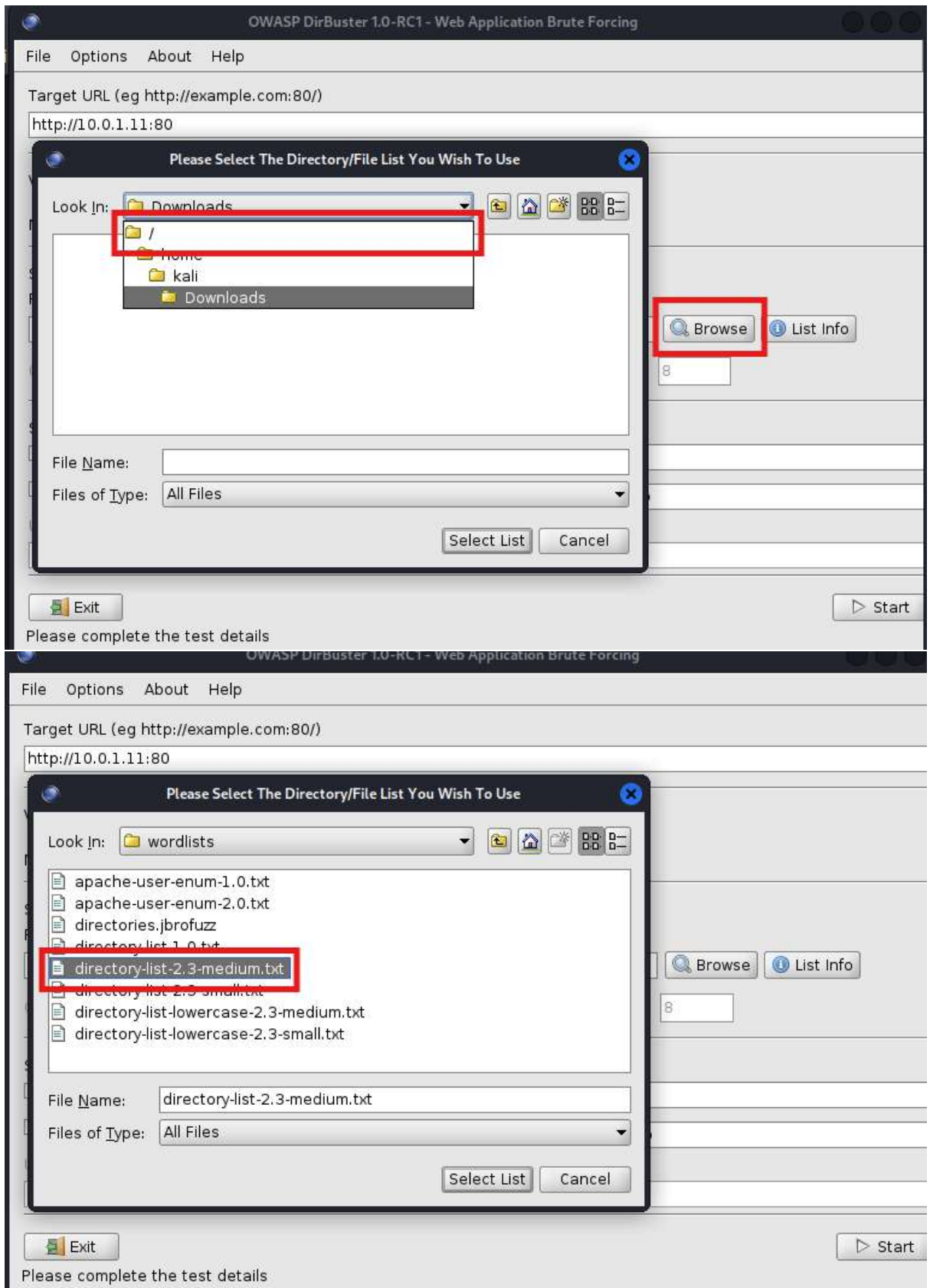
6. Buka terminal Kali dan ketik *dirbuster* untuk memulai menggunakan tools, setelah beberapa saat akan muncul tampilan *dirbuster* pada kali



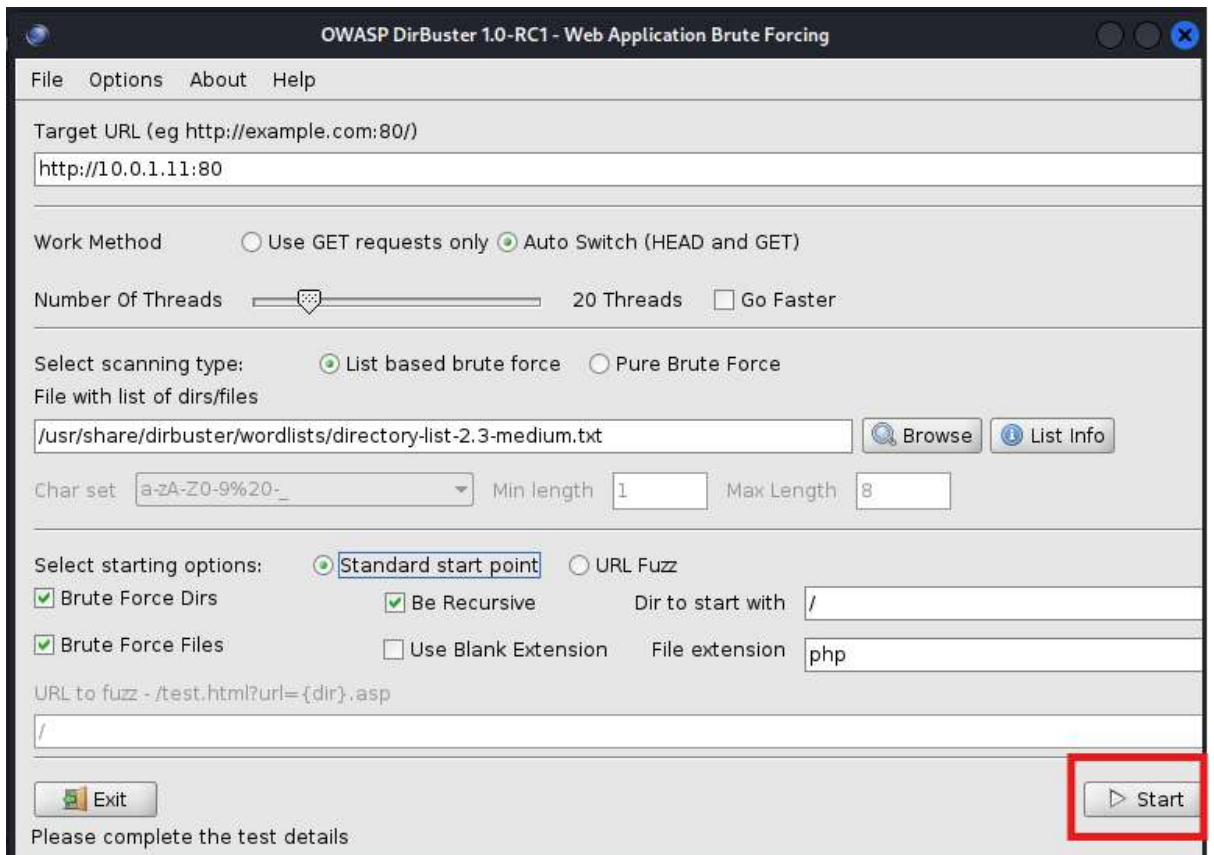
- Masukan IP target yaitu 10.0.1.11 dan port 80. Method yang digunakan pada praktikum kali ini akan menggunakan HEAD dan GET namun pada dirbuster mengakomodir jika hany diganti GET saja. Threads dapat diatur sesuai kemampuan target, semakin banyak threads maka akan menghasilkan banyak paket yang dikirim kepada target sehingga dapat menyebabkan target down.



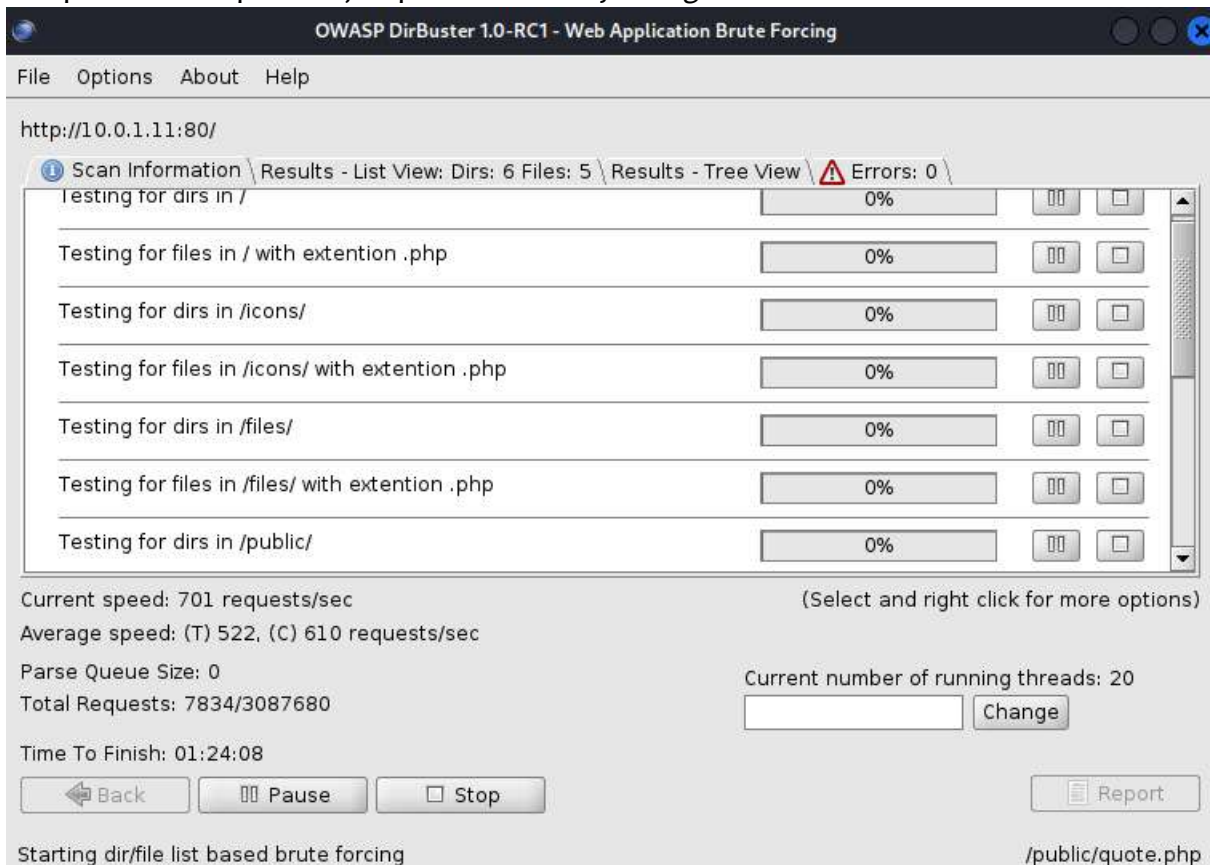
- Masukan worldlist yang akan digunakan, tekan `Browse > / > usr > share > dirbuster > wordlist > directory-list-2.3-medium.txt`



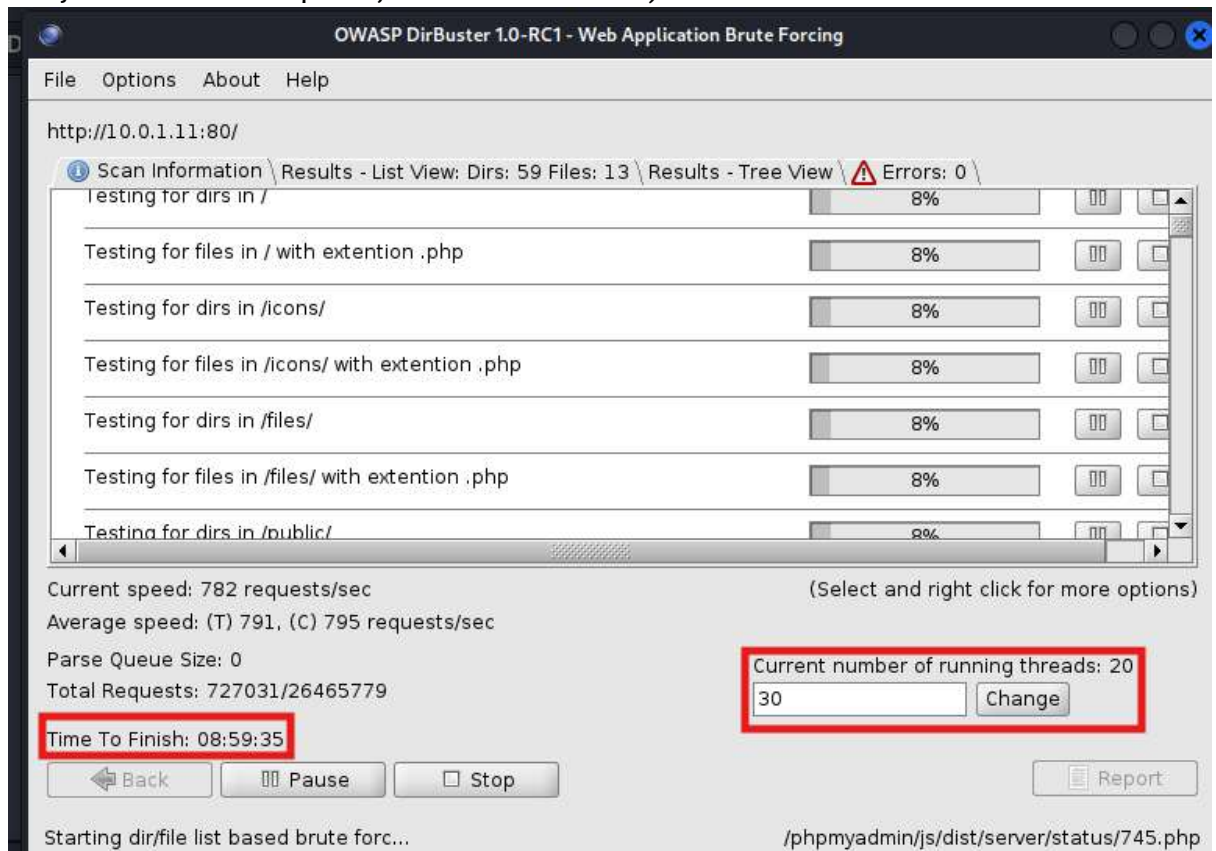
9. Tekan start untuk memulai *directory listing*



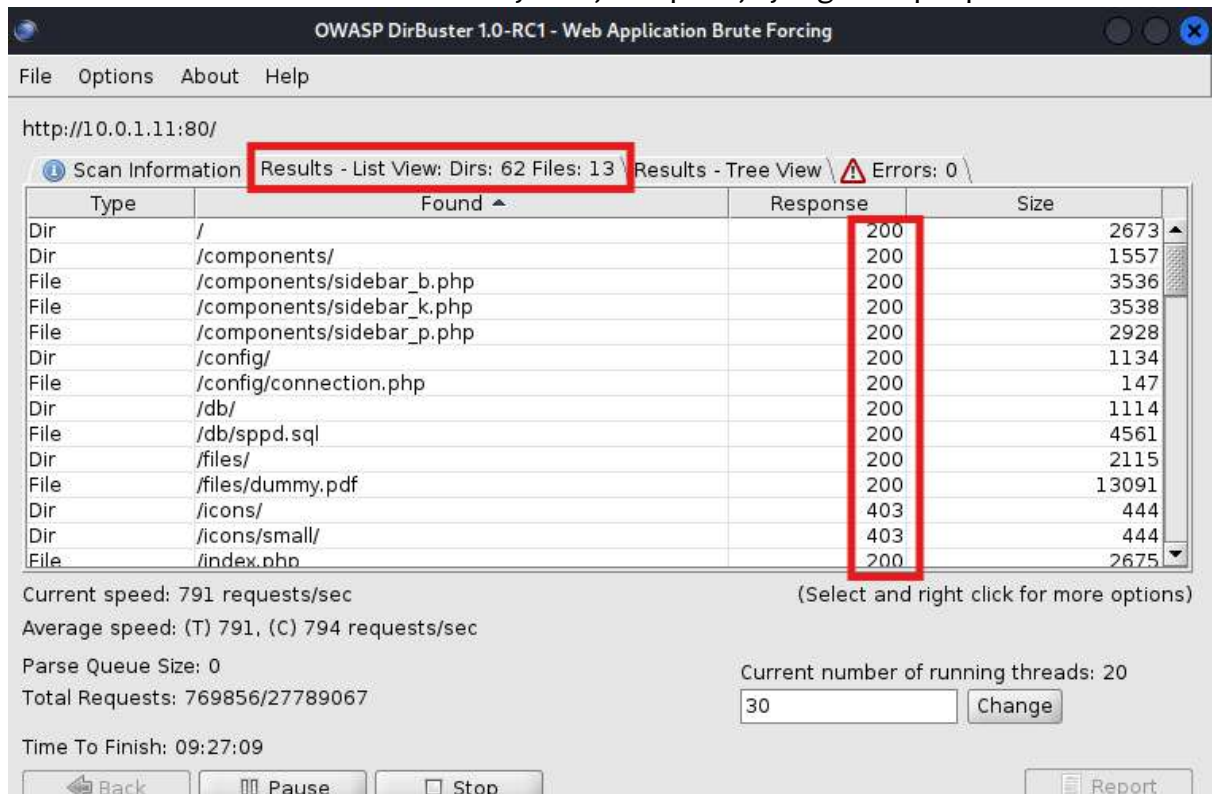
10. Tampilan akan seperti ini jika proses *directory listing* dimulai



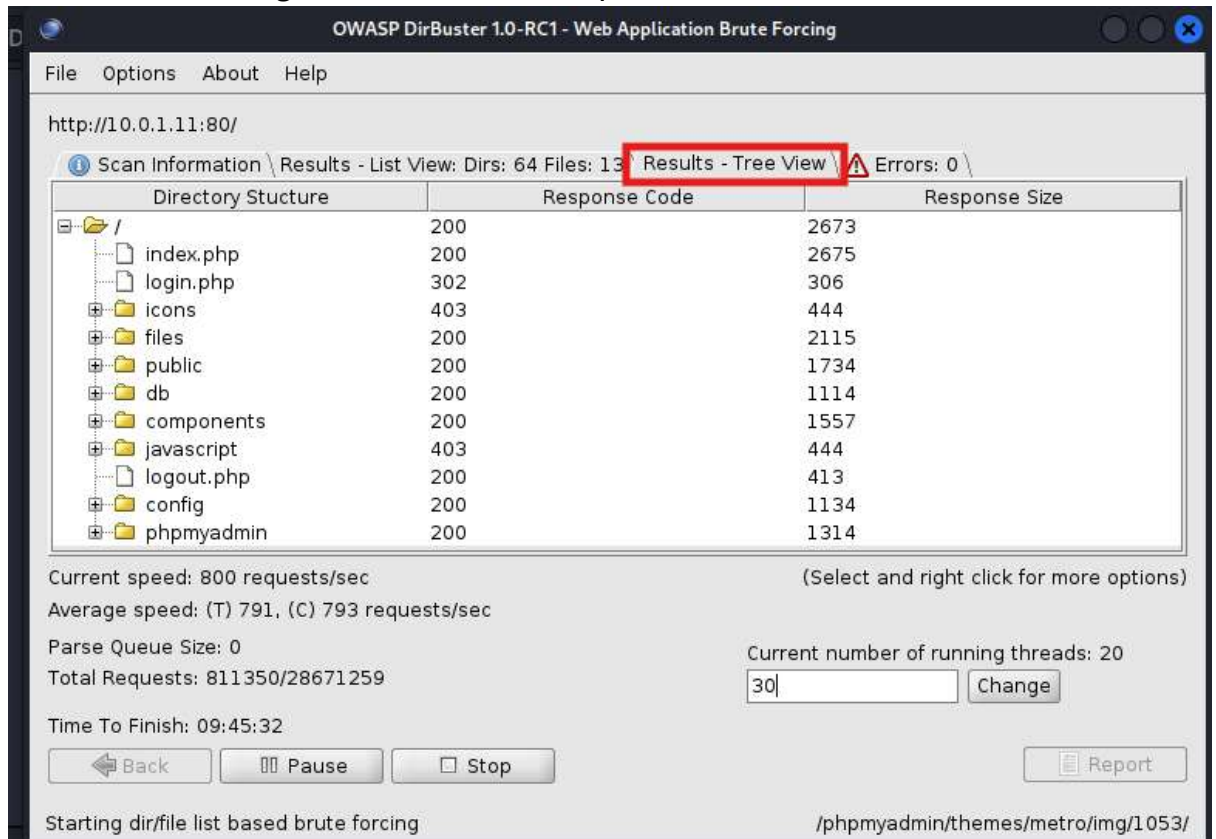
- Anda dapat melihat berapa waktu yang dibutuhkan untuk menyelesaikan pekerjaan pada kiri bawah dan dapat mengatur jumlah thread pada kanan bawah (semakin banyak thread waktu pekerjaan semakin sedikit)



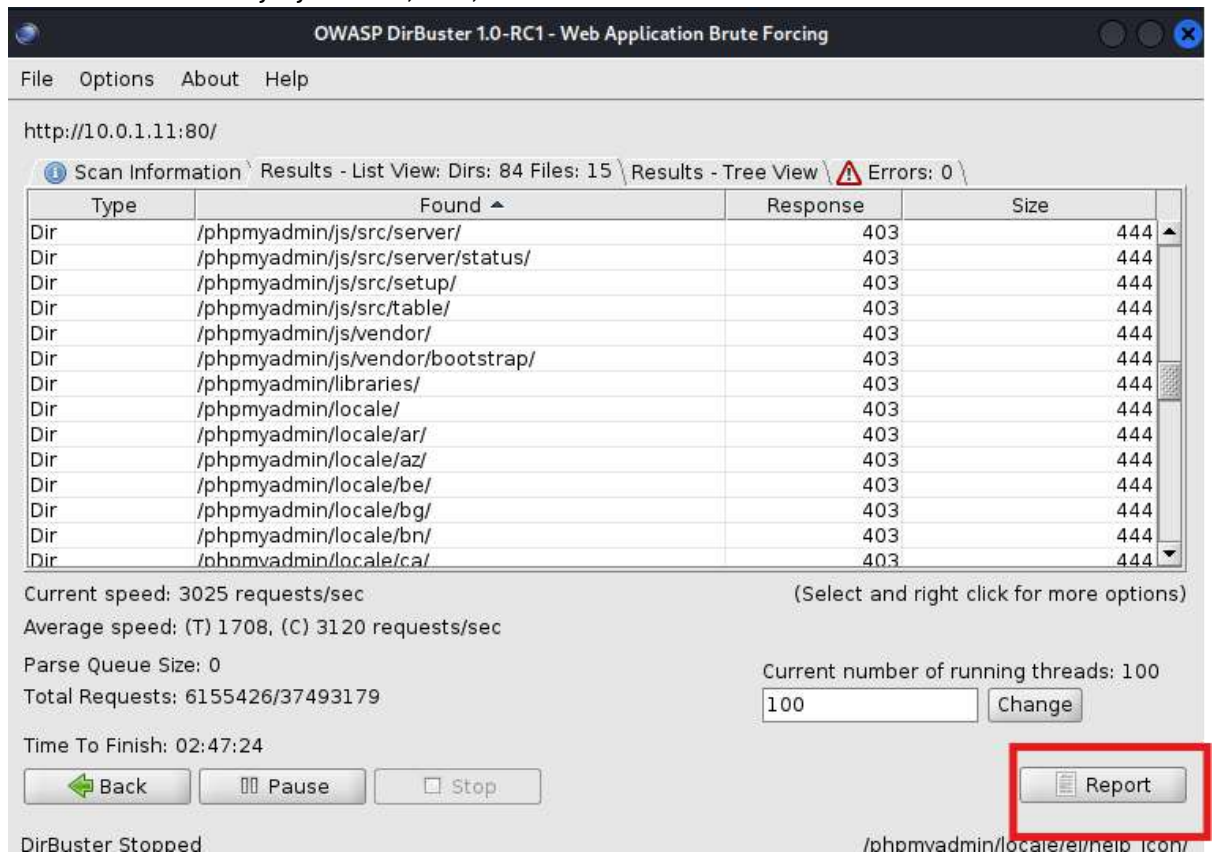
- Buka tab result untuk melihat *directory* dan *files* apa saja yang terdapat pada web



13. Untuk memberikan gambaran lebih anda dapat membuka *tab tree view*



14. Jika pekerjaan sudah selesai, anda dapat melihat laporan yang dapat anda sesuaikan formatnya yaitu txt, xml, dan csv.



15. Kode yang ditemukan dijelaskan pada tabel berikut

Kode	Arti Singkat	Penjelasan
200	OK	Halaman/file berhasil diakses
301	Moved Permanently	URL di-redirect ke tempat lain
302	Found (redirect)	Redirect sementara
403	Forbidden	Kamu tidak diizinkan mengakses (tapi file/folder ada!)
401	Unauthorized	Butuh login dulu (biasanya HTTP Basic Auth)
404	Not Found	File/direktori tidak ditemukan
500	Internal Server Error	Ada error di server
503	Service Unavailable	Server down atau tidak bisa proses

# Penggunaan OWASP ZAP dalam Vurnerabilty Assesment (P.6.1.A)

## Skenario Praktikum

Anda adalah seorang *L1 SOC Analyst* yang bekerja di Pemerintah Daerah Kabupaten Lengkeng. Anda memiliki tugas untuk mengawasi dan memantau seluruh aktivitas jaringan ke dalam infrastruktur TI Pemkab Lengkeng dengan bantuan SIEM. Dalam menjalankan tugas ini, Anda harus memiliki kemampuan untuk mengetahui kerentanan yang dimiliki oleh aset yang anda awasi sehingga menuntut anda untuk mampu mengoperasikan tools *vurnerability assement*.

Pemerintah Daerah Kabupaten Lengkeng memiliki Layanan Web SPPD belum pernah dilakukan *vurnerabilty assesment* dan *penetration testing*. Layanan web tersebut ditempatkan pada VM Target Web 1. Untuk mengetahui *port* apa saja yang menimbulkan kerentanan, anda akan melakukan *vurnerabilty assesment* tahap *scanning*, *enumeration* dan *vurnerabilty analyis* menggunakan Dirbuster.

## Tujuan Praktikum

Praktikum ini bertujuan untuk membantu peserta didik dalam mengoperasikan NMAP dalam mengidektifikasi kerentanan

## Enviroment Laboratorium Virtual

Praktikum ini membutuhkan:

- VM Kali Linux
- VM Target Web 1.

## Durasi Praktikum

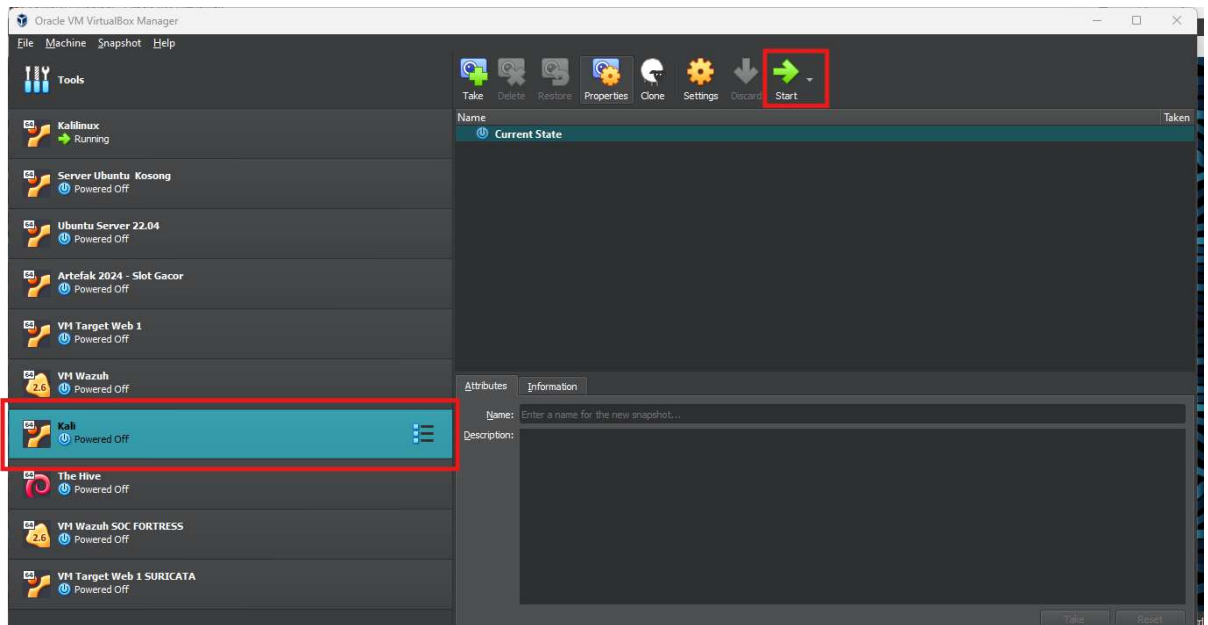
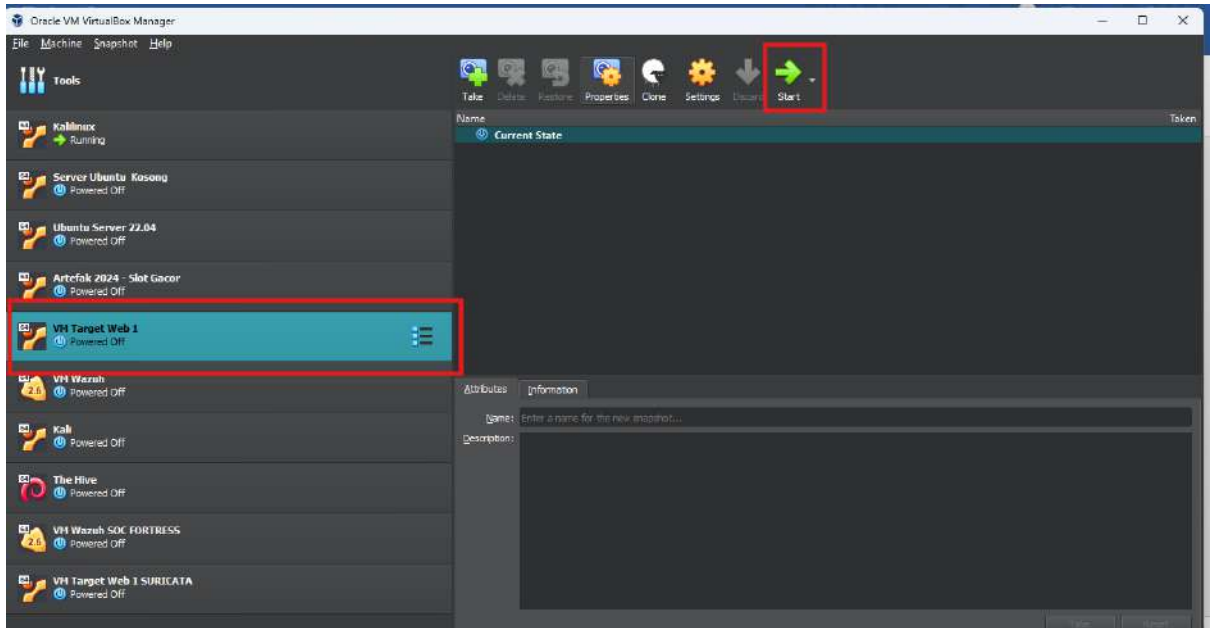
10 Menit

## Catatan Khusus

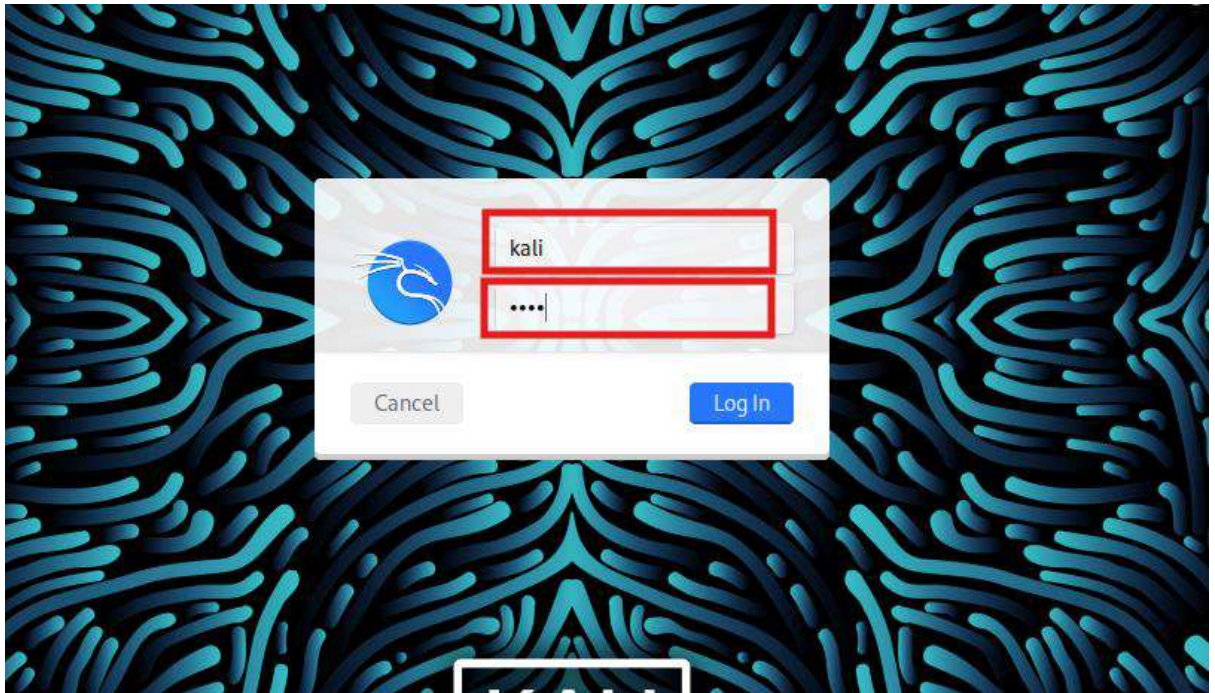
- Siapkan *enviroment* laboratorium virtual sesuai panduan instalasi laboratorium virtual
- Dokumentasikan setiap langkah praktikum karena dapat membantu menjawab pertanyaan pada soal yang diberikan

## Langkah-Langkah

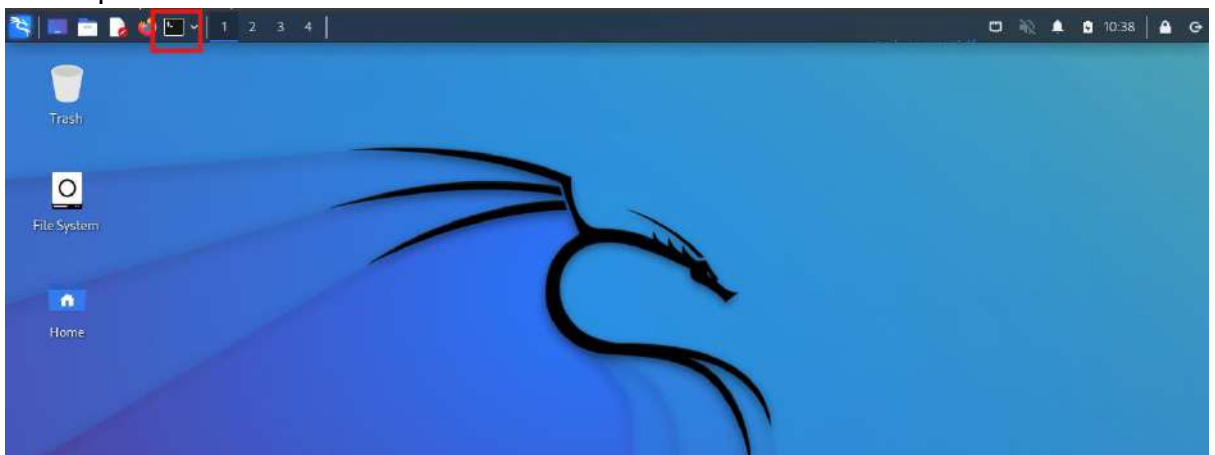
1. Siapkan Virtualbox, nyalakan VM Target Web 1 dab VM Kali dengan menekan virtual machine pada Virtual box lalu menekan start



2. Buka pada VM Kali dan masukan *username* kali dan *password* kali



3. Setelah masuk kedalam tampilan awal dekstop, buka terminal pada kiri atas dekstop



4. Cek IP Kali apakah sudah satu jaringan dengan IP VM Web Target 1 dengan ifconfig ( IP Kali dan IP VM Web Target 1 seharusnya berada pada 10.0.1.0/24 jika dalam enviroment disiapkan dengan benar)

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
└─$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 10.0.1.12 netmask 255.255.255.0 broadcast 10.0.1.255  
    inet6 fe80::a00:27ff:fe17:2c4a prefixlen 64 scopeid 0x20<link>  
    ether 08:00:27:17:2c:4a txqueuelen 1000 (Ethernet)  
    RX packets 55 bytes 3830 (3.7 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 22 bytes 3034 (2.9 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 0 bytes 0 (0.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 0 bytes 0 (0.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

5. Beralih ke VM Web Target 1, cek IP apakah sudah pada network yang sama dengan Kali, login terlebih dahulu dengan *username* `serveradmin` dan *password* `ubuntu` lalu jalankan perintah `ifconfig` ( IP Kali dan IP VM Web Target 1 seharusnya berada pada `10.0.1.0/24` jika dalam *enviroment* disiapkan dengan benar)

```
Ubuntu 22.04.2 LTS websppd tty1
websppd login: [ 35.716544] cloud-init[1533]: Cloud-init v. 23.1.2-0ubuntu0~22.04.1 running 'modules:final' at Sat, 12 Apr 2025 14:37:50 +0000. Up 35.68 seconds.
[ 35.798099] cloud-init[1533]: Cloud-init v. 23.1.2-0ubuntu0~22.04.1 finished at Sat, 12 Apr 2025 14:37:50 +0000. Datasource DataSourceNone. Up 35.79 seconds
[ 35.798773] cloud-init[1533]: 2025-04-12 14:37:50,938 - cc_final_message.py[WARNING]: Used fallback datasource

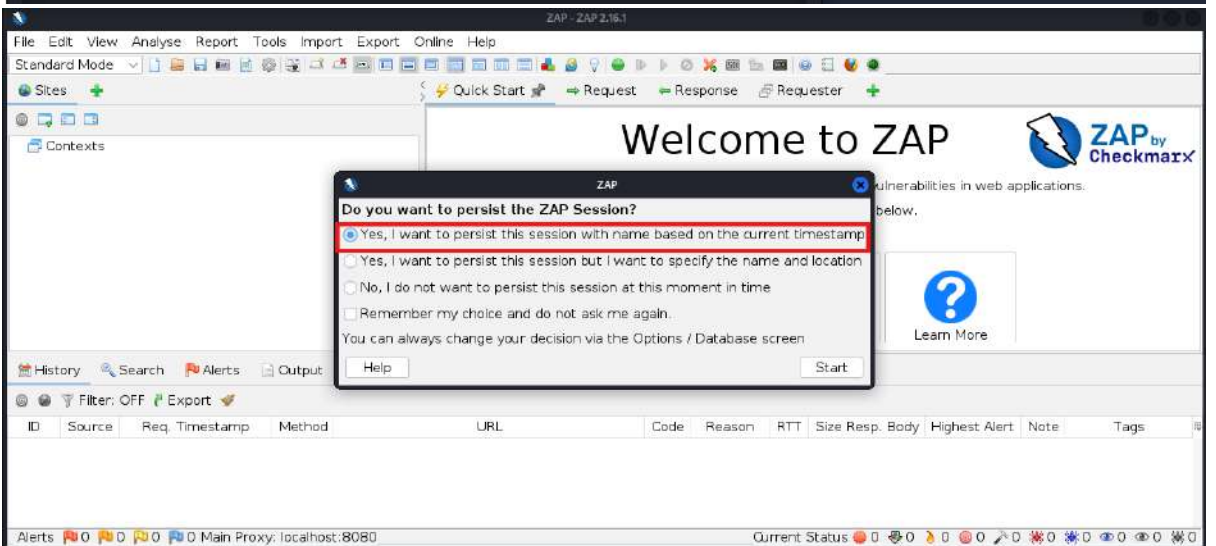
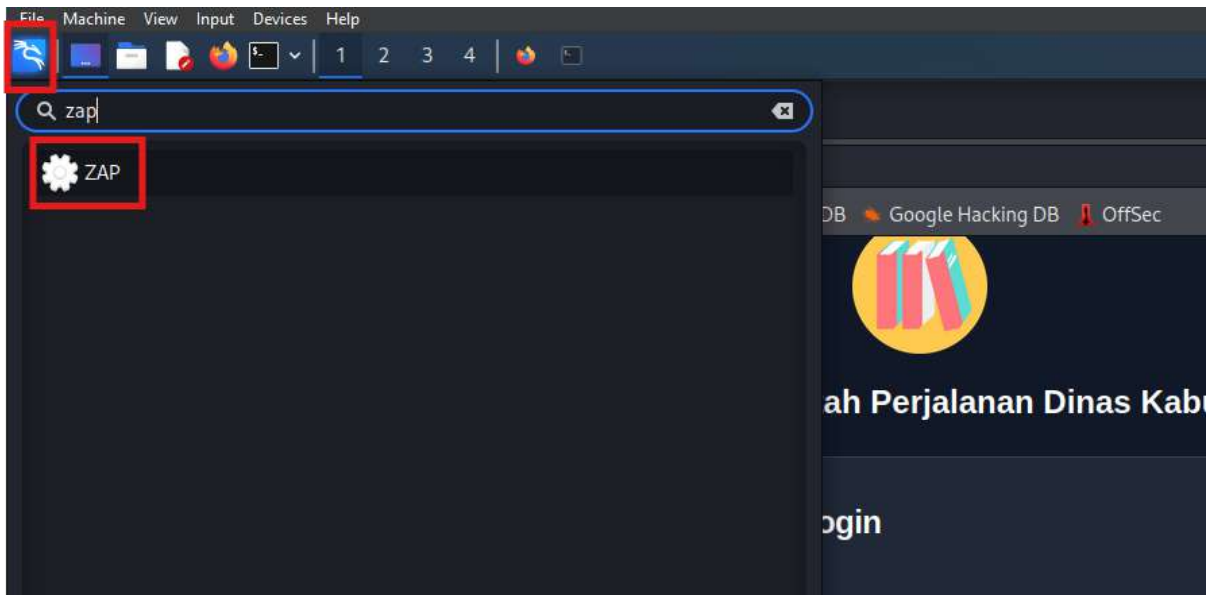
websppd login: serveradmin
Password: _

serveradmin@websppd:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.1.11 netmask 255.255.255.0 broadcast 10.0.1.255
    inet6 fe80::d08:27ff:fead:9c1b prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:ad:9c:1b txqueuelen 1000 (Ethernet)
    RX packets 277 bytes 344725 (344.7 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 366 bytes 29451 (29.4 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

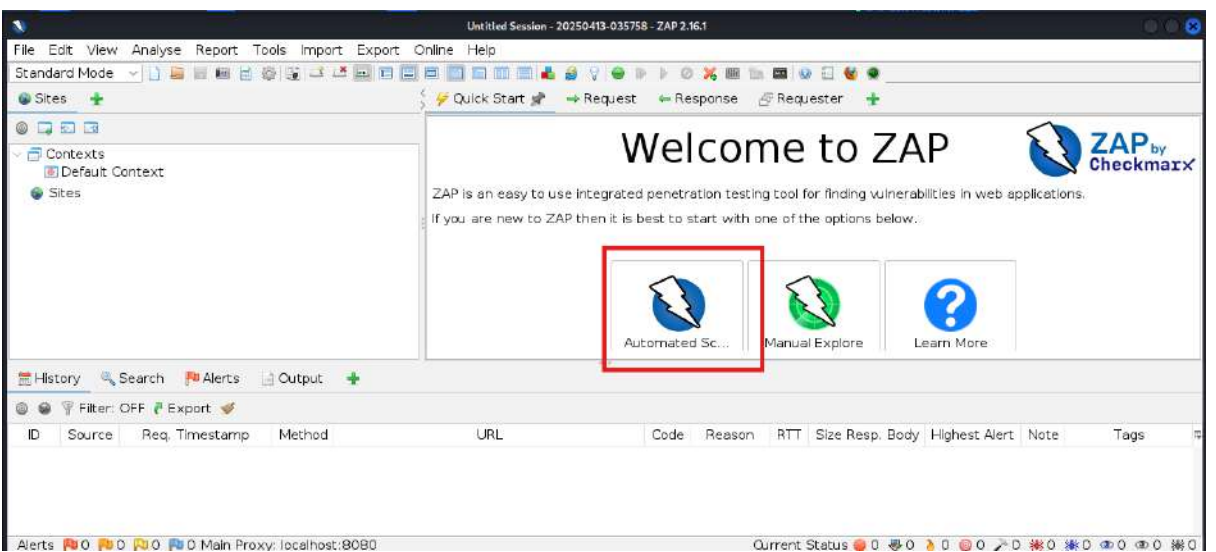
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 152 bytes 12704 (12.7 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 152 bytes 12704 (12.7 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

serveradmin@websppd:~$ _
```

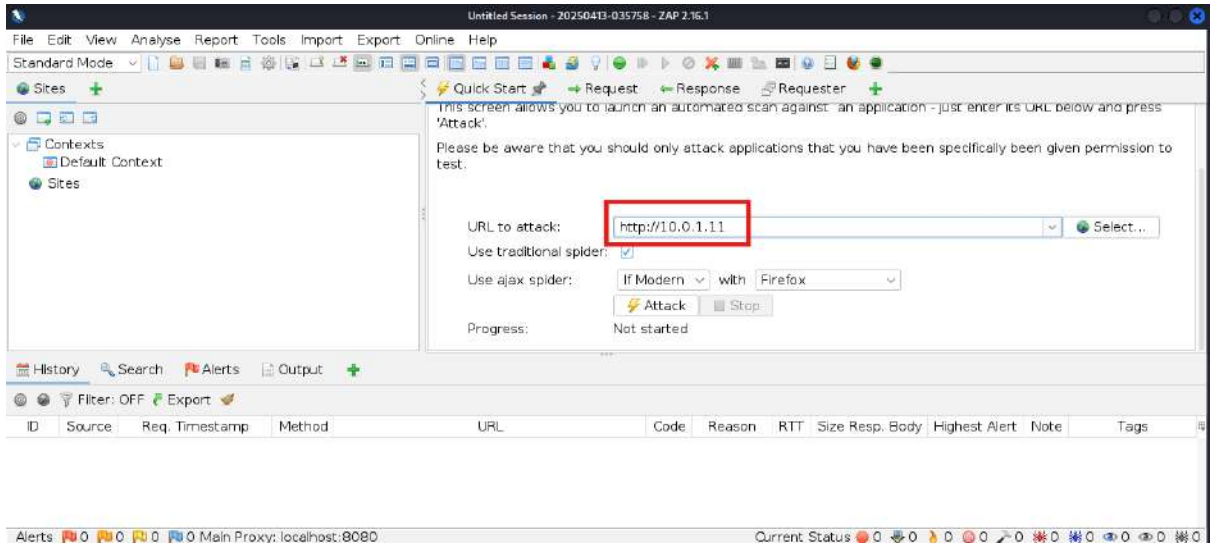
6. Unduh installer OWASP ZAP jika anda menggunakan desktop bukan dari VM Kali laboratorium virtual, lakukan instalasi OWASP ZAP terlebih dahulu. Jika anda menggunakan Kali *search* pada bagian *tools* Kali dan tekan ZAP



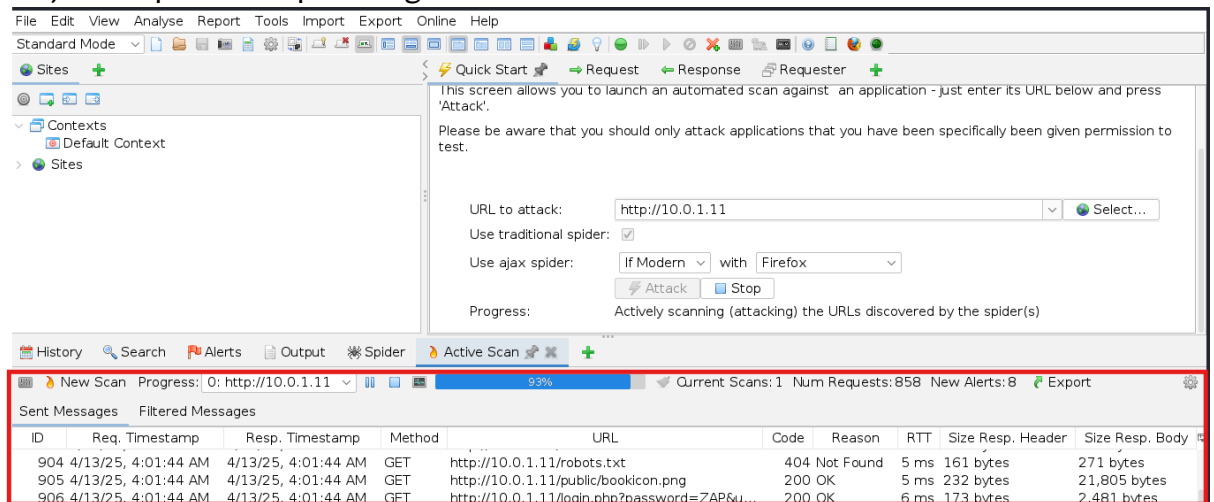
- 7.
8. Pilih *automated scan*



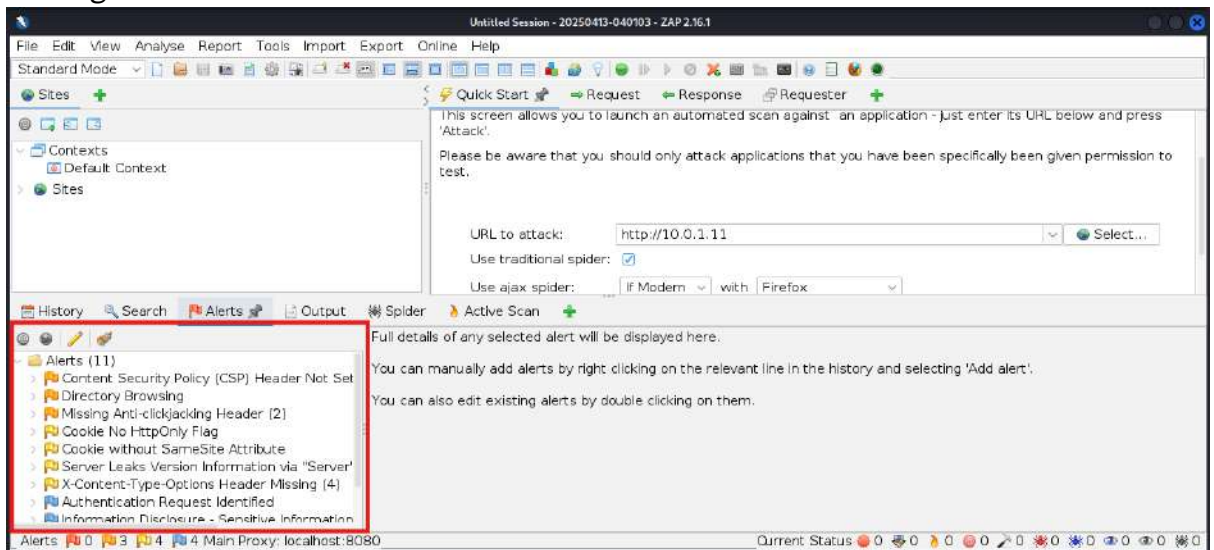
9. Masukkan IP VM Web Server Target 1, lalu klik *attack*



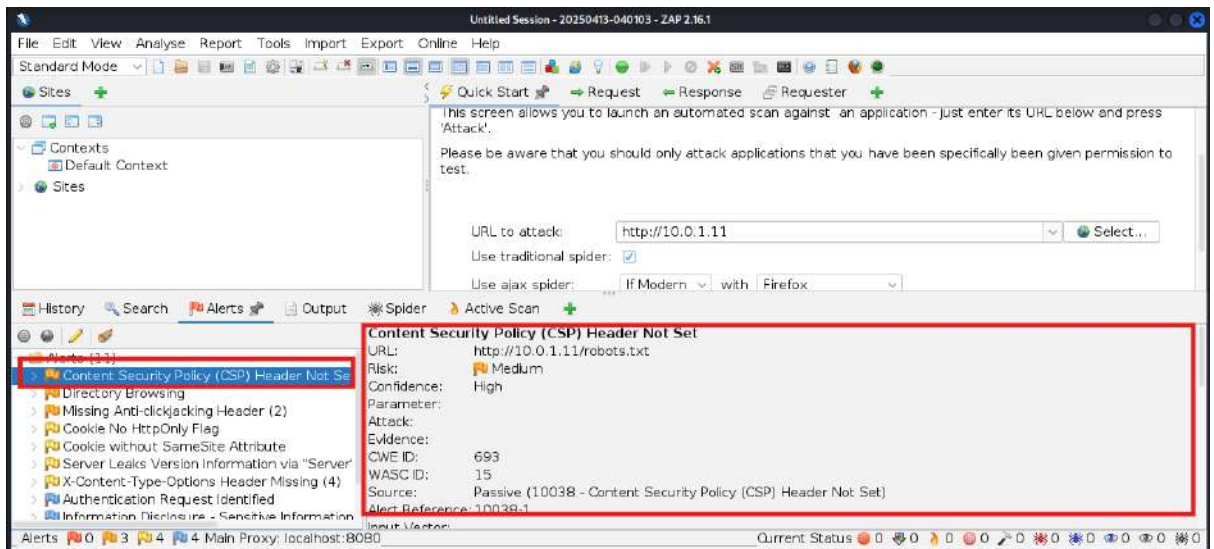
10. Tampilan ketika *attack* sudah dijalankan seperti gambar dibawah ini, proses yang berjalan dapat dilihat pada bagian bawah



11. Kerentanan yang dideteksi terdapat pada bagian kiri bawah, yang akan dikategorikan berdasarkan warna



12. Tekan pada salah satu kerentanan untuk melihat detail kerentanan



13. Dokumentasikan setiap temuan yang ada.

## Membedakan Bagian Aset yang Merupakan Kerentanan dan bukan Kerentanan (P.6.1.B)

### Skenario Praktikum

Anda adalah seorang *L1 SOC Analyst* yang bekerja di Pemerintah Daerah Kabupaten Lengkeng. Anda memiliki tugas untuk mengawasi dan memantau seluruh aktivitas jaringan ke dalam infrastruktur TI Pemkab Lengkeng dengan bantuan SIEM. Dalam menjalankan tugas ini, Anda harus memiliki kemampuan untuk mengetahui kerentanan yang dimiliki oleh aset yang anda awasi sehingga menuntut anda untuk mampu mengoperasikan *tools vulnerability assesment*.

Pemerintah Daerah Kabupaten Lengkeng memiliki Layanan Web SPPD belum pernah dilakukan *vulnerability assesment* dan *penetration testing*. Saat anda melaksanakan tahapan *vulnerability assesment*, anda menemukan beberapa bagian pada aset anda yang ternyata menimbulkan kerentanan

### Tujuan Praktikum

Praktikum ini bertujuan untuk membantu peserta didik dalam mengenali kerentanan pada aset

### Environment Laboratorium Virtual

Praktikum ini membutuhkan:

- Browser terhubung keinternet

### Durasi Praktikum

10 Menit

### Catatan Khusus

- Siapkan *environment* laboratorium virtual sesuai panduan instalasi laboratorium virtual
- Dokumentasikan setiap langkah praktikum karena dapat membantu menjawab pertanyaan pada soal yang diberikan

### Langkah-Langkah

1. Siapkan dokumentasi praktikum penggunaan NMAP pada awal modul ini, pada praktikum ini akan melanjutkan temuan hasil NMAP.
2. Akses pada [CVE.mitre.com](https://cve.mitre.com). Tekan Search CVE List.

The mission of the CVE® Program is to identify, define, and catalog publicly disclosed cybersecurity vulnerabilities.

- Masukan bagian dari aset yang hendak anda selidiki, misalkan vsftpd yang ada dalam server anda, lalu tekan submit

- Pilih yang sesuai dengan versi yang anda miliki.

Name	Description
<a href="#">CVE-2021-30047</a>	VSFTPD 3.0.3 allows attackers to cause a denial of service due to limited number of connections allowed.
<a href="#">CVE-2017-8218</a>	vsftpd on TP-Link C2 and C20i devices through firmware 0.9.1 4.2 v0032.0 Build 160706 Rel.37961n has a backdoor admin account with the 1234 password, a backdoor guest account with the guest password, and a backdoor test account with the test password.
<a href="#">CVE-2015-1419</a>	Unspecified vulnerability in vsftpd 3.0.2 and earlier allows remote attackers to bypass access restrictions via unknown vectors, related to deny_file parsing.
<a href="#">CVE-2012-2127</a>	fs/proc/root.c in the procs implementation in the Linux kernel before 3.2 does not properly interact with CLONE_NEWPID clone system calls, which allows remote attackers to cause a denial of service (reference leak and memory consumption) by making many connections to a daemon that uses PID namespaces to isolate clients, as demonstrated by vsftpd.
<a href="#">CVE-2011-2523</a>	vsftpd 2.3.4 downloaded between 20110630 and 20110703 contains a backdoor which opens a shell on port 6200/tcp.
<a href="#">CVE-2011-2189</a>	net/core/nec_namespace.c in the Linux kernel 2.6.32 and earlier does not properly handle a high rate of creation and cleanup of network namespaces, which makes it easier for remote attackers to cause a denial of service (memory consumption) via requests to a daemon that requires a separate namespace per connection, as demonstrated by vsftpd.
<a href="#">CVE-2011-0762</a>	The vsf_filename_passes_filter function in ls.c in vsftpd before 2.3.3 allows remote authenticated users to cause a denial of service (CPU consumption and process slot exhaustion) via crafted glob expressions in STAT commands in multiple FTP sessions, a different vulnerability than CVE-2010-2632.
<a href="#">CVE-2009-5029</a>	Integer overflow in the __tzfile_read function in glibc before 2.15 allows context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted timezone (TZ) file, as demonstrated using vsftpd.
<a href="#">CVE-2009-4457</a>	Multiple unspecified vulnerabilities in the Vsftpd Webmin module before 1.3b for the Vsftpd server have unknown impact and attack vectors related to "Some security issues."
<a href="#">CVE-2008-2375</a>	Memory leak in a certain Red Hat deployment of vsftpd before 2.0.5 on Red Hat Enterprise Linux (RHEL) 3 and 4, when PAM is used, allows remote attackers to cause a denial of service (memory consumption) via a large number of invalid authentication attempts within the same session, a different vulnerability than CVE-2007-5962.
<a href="#">CVE-2007-5962</a>	Memory leak in a certain Red Hat patch, applied to vsftpd 2.0.5 on Red Hat Enterprise Linux (RHEL) 5 and Fedora 6 through 8, and on Foresight Linux and rPath appliances, allows remote attackers to cause a denial of service (memory consumption) via a large number of CWD commands, as demonstrated by an

5. Tekan nomor CVE pada sebelah kiri untuk mendapatkan informasi lebih detail terkait