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

Pengunaan 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 dimiiki 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 perserta didik dalam mengoperasikan NMAP dalam mengidektifikasi kerentanan

Enviroment Laboratorium Virtual

Praktikum ini membutuhkan:

- VM Kali Linux
- VM Target Web 1.

Durasi Praktikum

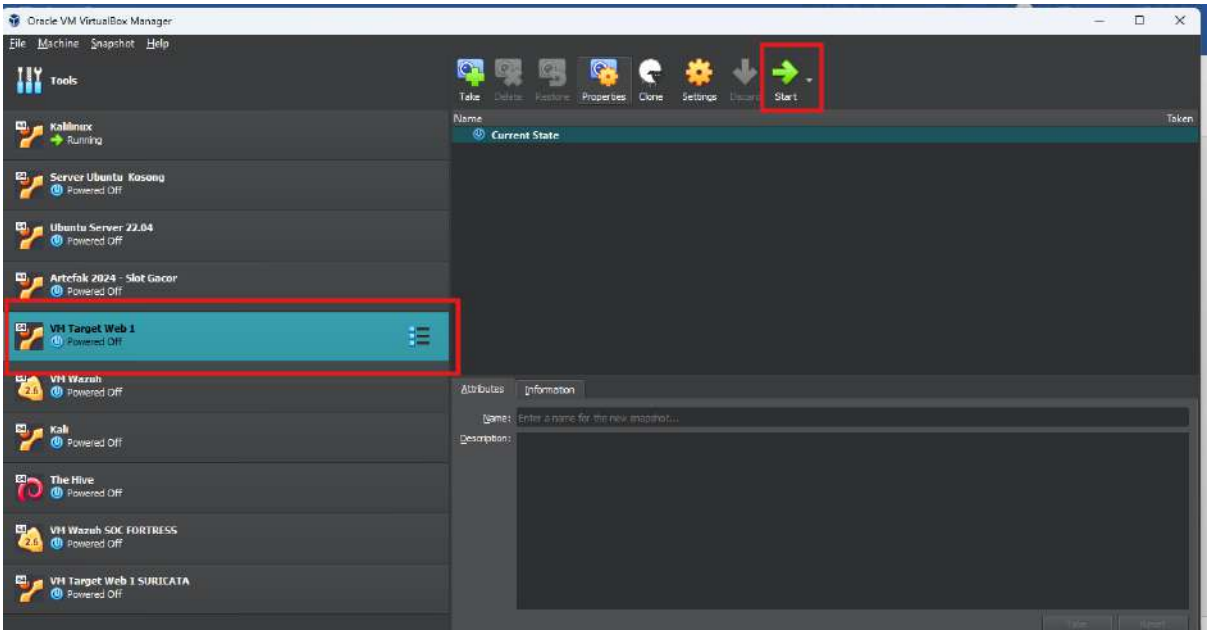
10 Menit

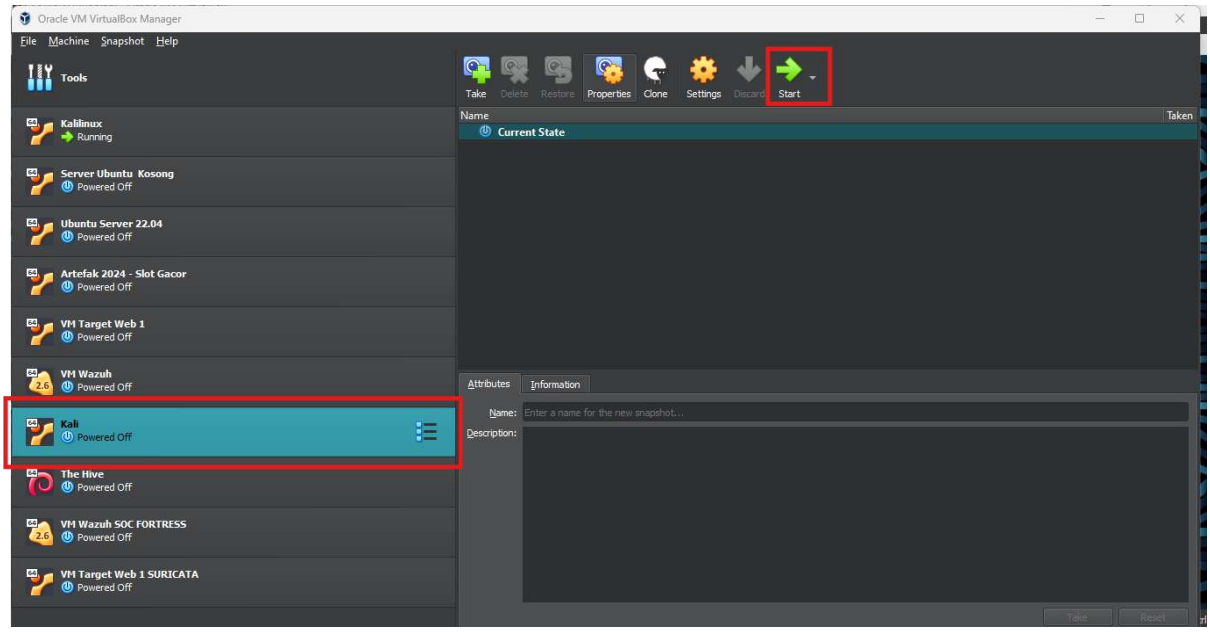
Catatan Khusus

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

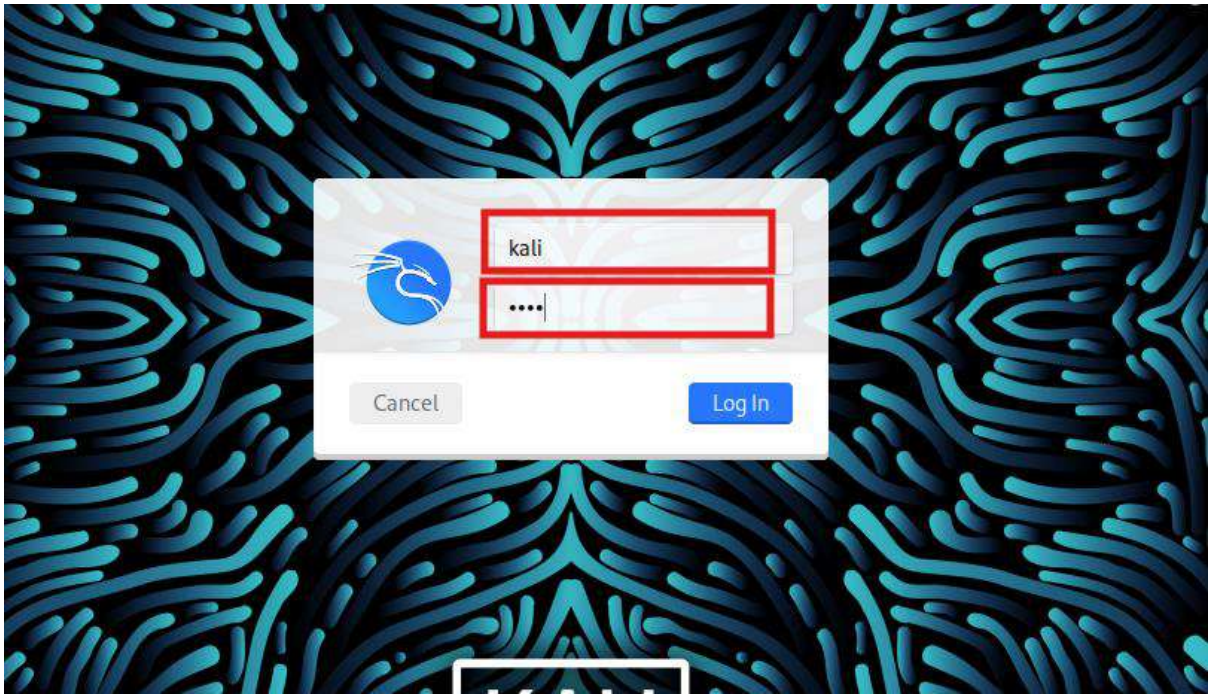
Langkah-Langkah

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

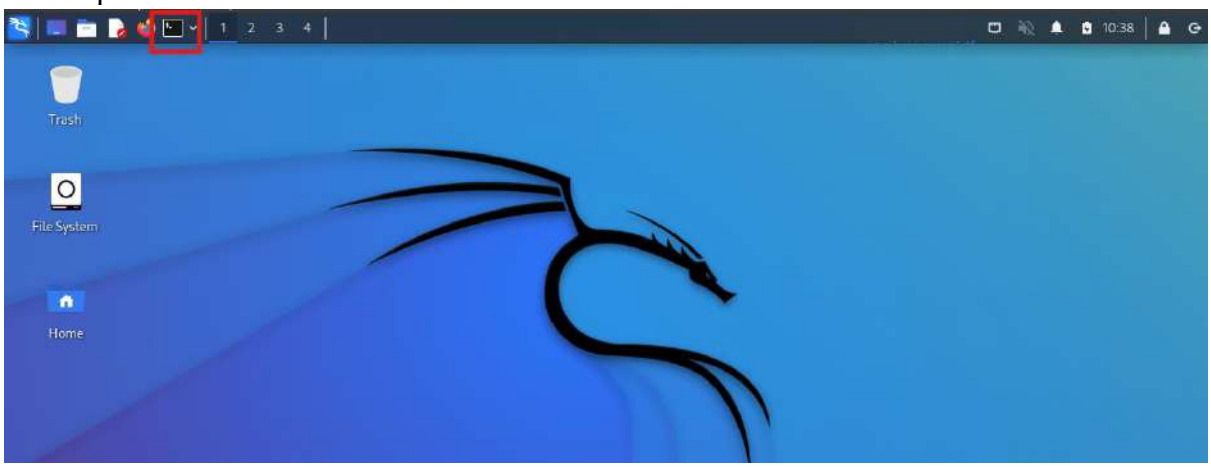




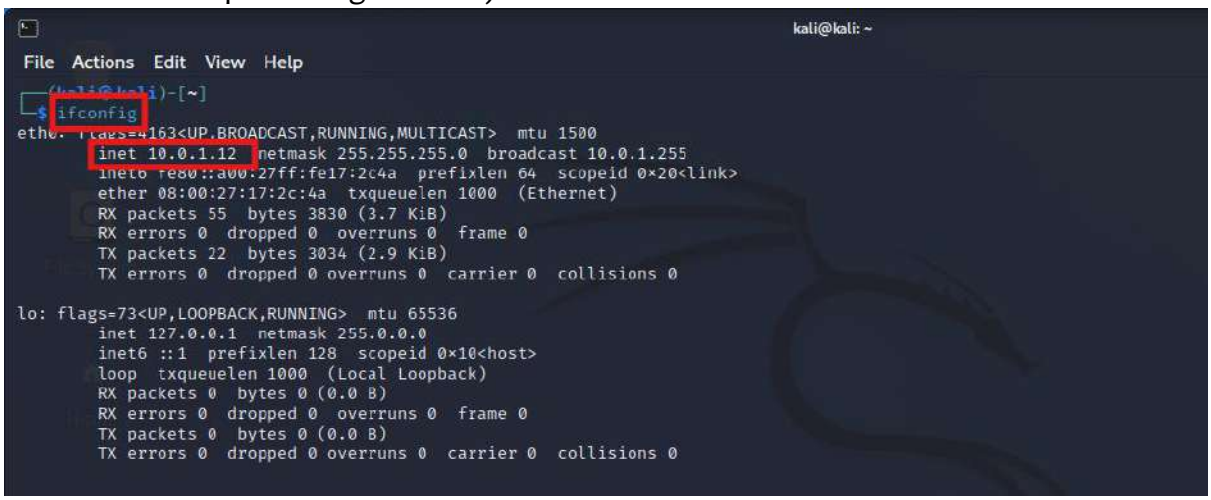
2. Buka pada VM Kali dan masukan *username* `kali` dan *password* `kali`



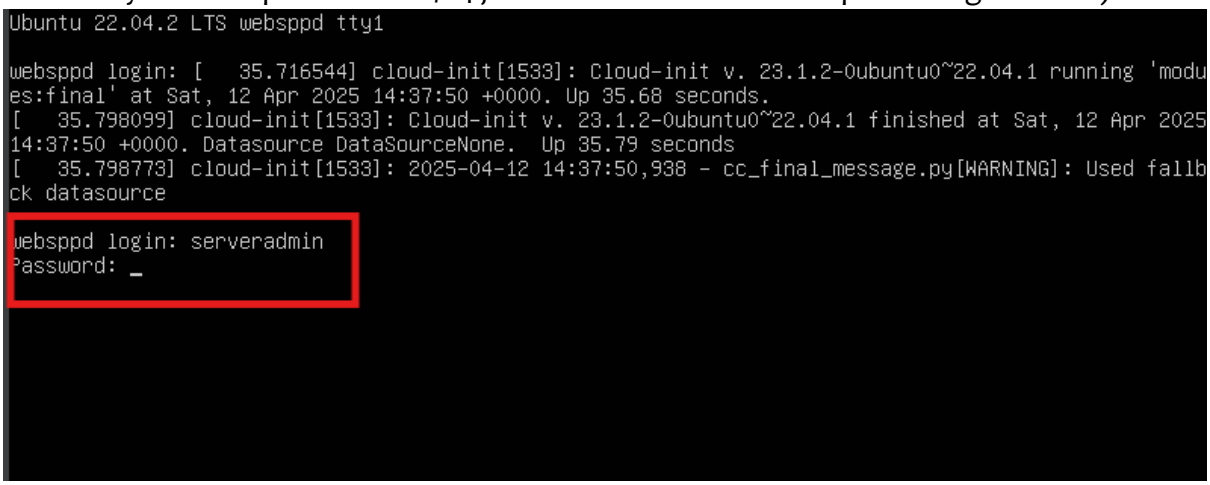
3. Setelah masuk kedalam tampilan awal dekstop, buka terminal pada kiri atas dekstop

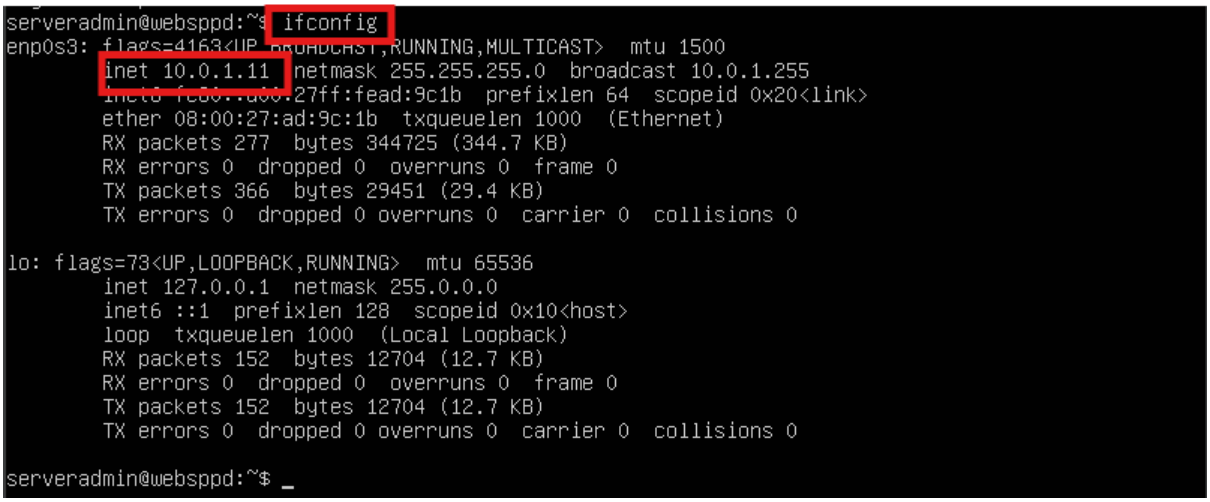


4. Cek IP Kali apakah sudah satu jaringan dengan IP VM Web Target 1 dengan ifconfig (IP Kali dan IP VM Web Target 1 seharusnya berada pada 10.0.1.0/24 jika dalam *enviroment* disiapkan dengan benar)



5. Beralih ke VM Web Target 1, cek IP apakah sudah pada network yang sama dengan Kali, login terlebih dahulu dengan *username* `serverdadmin` 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)

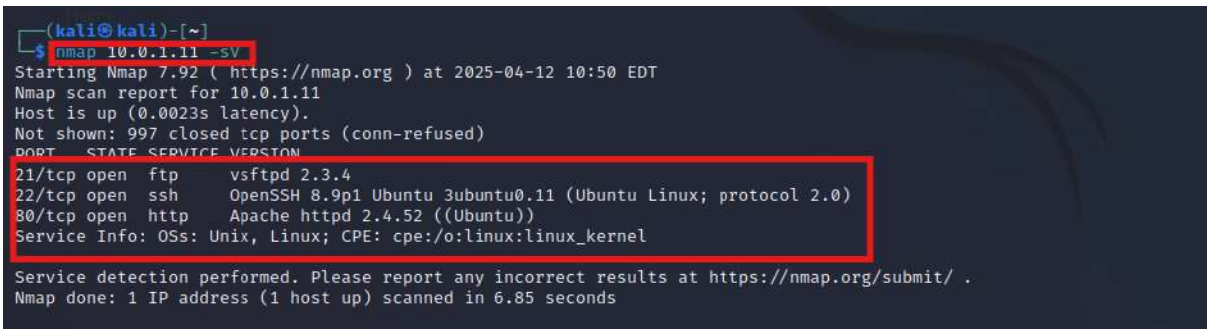




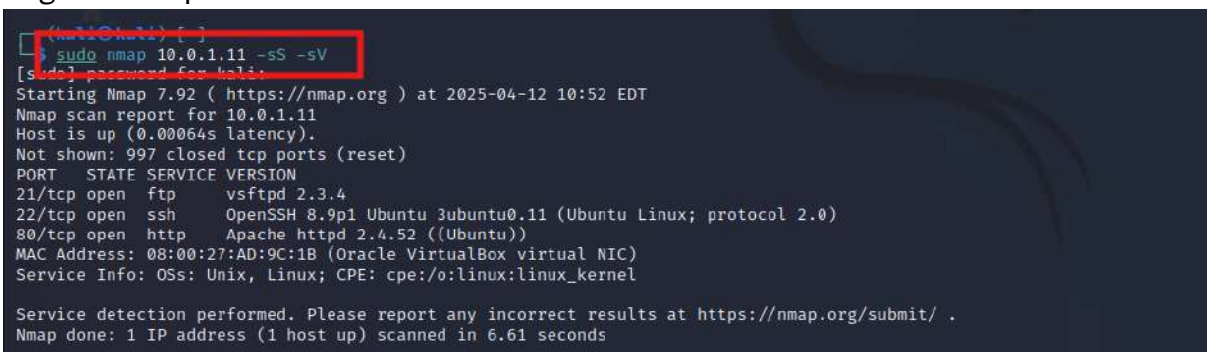
6. Buka kembali Kali dan buka pada terminal, untuk mengetahui perangkat mana saja yang berada dalam jaringan yang sama lakukan NMAP pada network dengan perintah `nmap 10.0.1.0/24`. Tahapan ini dapat digunakan dalam mendeteksi perangkat apa saja yang berada didalam jaringan dan sangat bermanfaat jika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

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

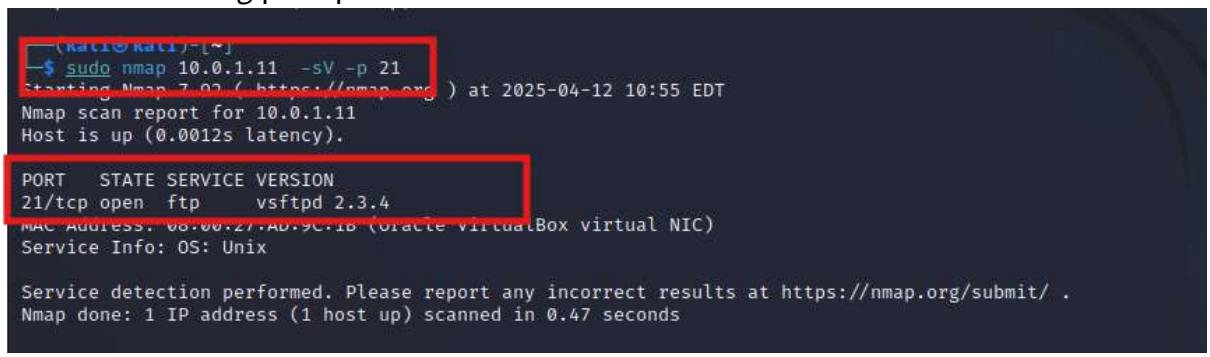
7. Lanjutkan *scanning* dengan langsung merujuk pada IP VM Web Target, tambahkan `-sV` untuk mengetahui versi layanan yang ada dengan perintah `nmap 10.0.1.11 -sV -sS`



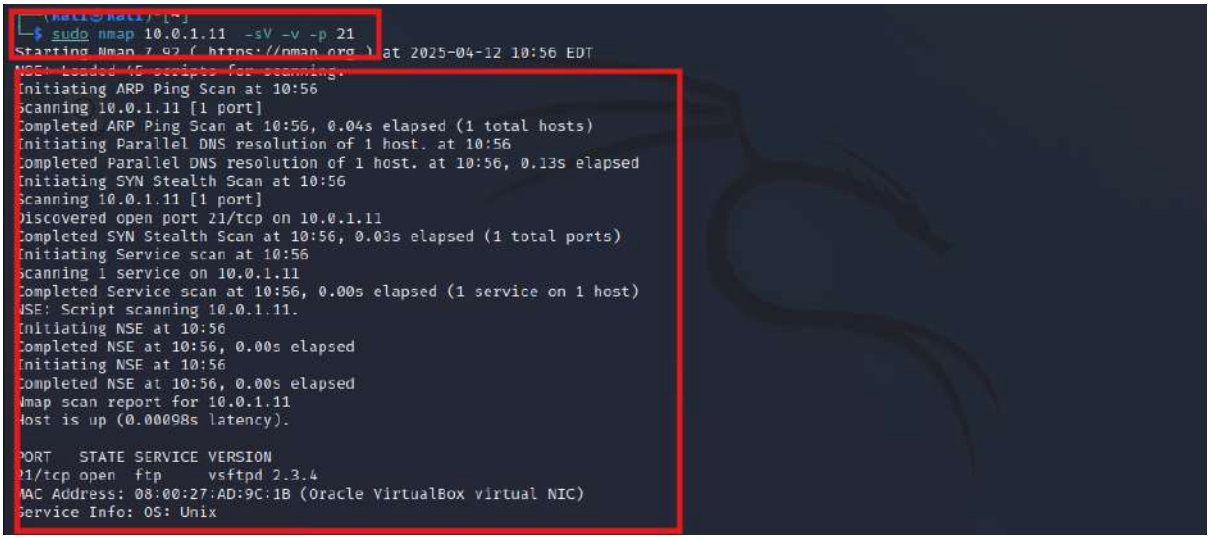
8. Dalam beberapa kasus, melakukan *scanning* akan membuat beban pada target, untuk menghindari hal tersebut dapat ditambahkan `-sS` pada perintah `nmap 10.0.1.11 -sV -sS`. Dengan perintah tersebut, *scanning* akan menjadi lebih ringan dan cepat.



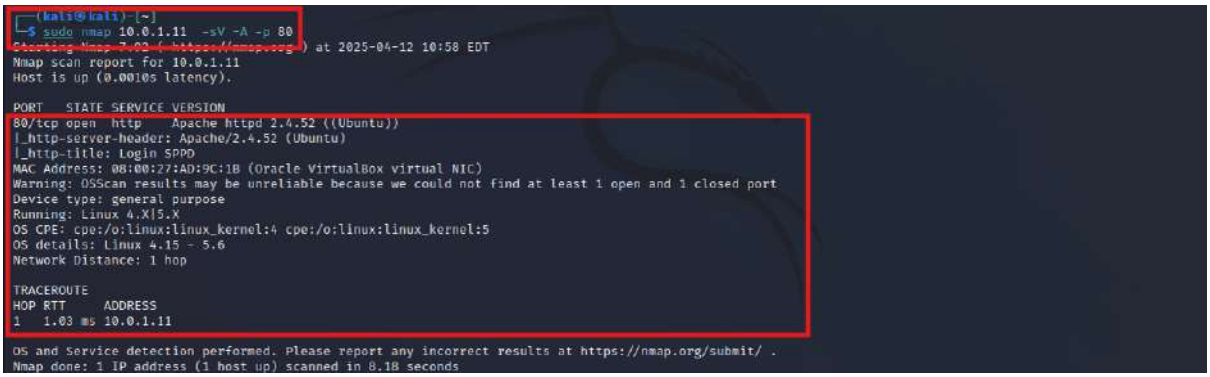
9. Untuk berfokus pada satu IP saja, dapat menambahkan -p pada perintah, `nmap 10.0.1.11 -sV -p <port yang diinginkan>`. Gambar ini contoh dilakukan *scanning* pada port 21



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>`



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>`



Pengunaan 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 dimiiki 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 *enumeration* menggunakan Dirbuster.

Tujuan Praktikum

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

Enviroment Laboratorium Virtual

Praktikum ini membutuhkan:

- VM Kali Linux
- VM Target Web 1.

Durasi Praktikum

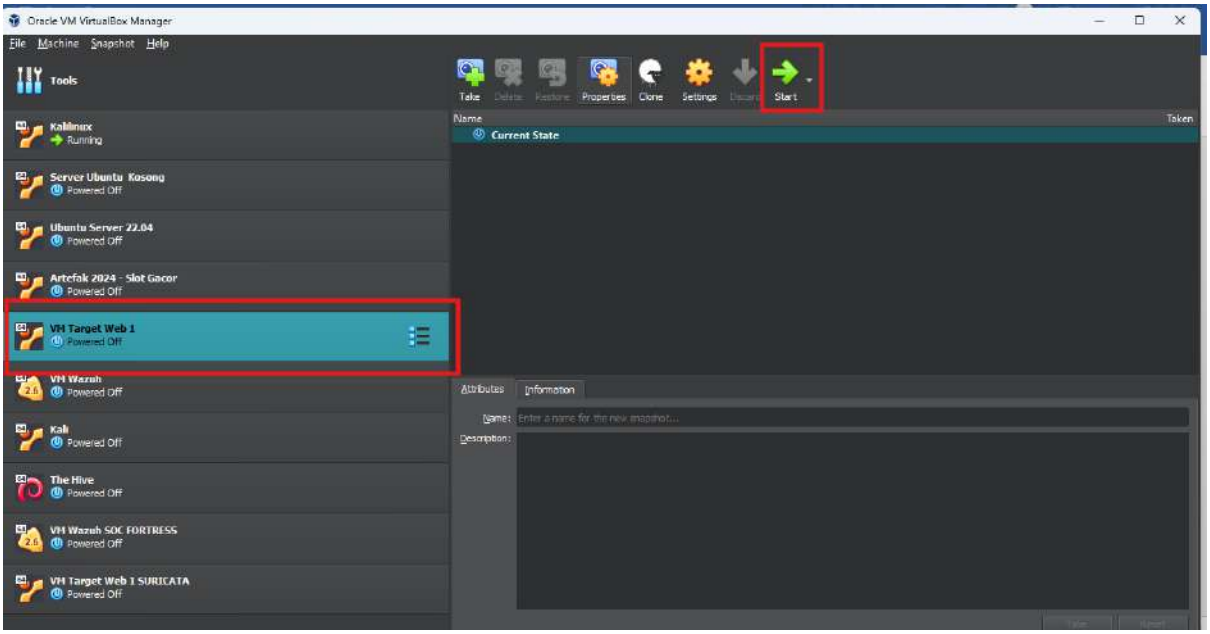
10 Menit

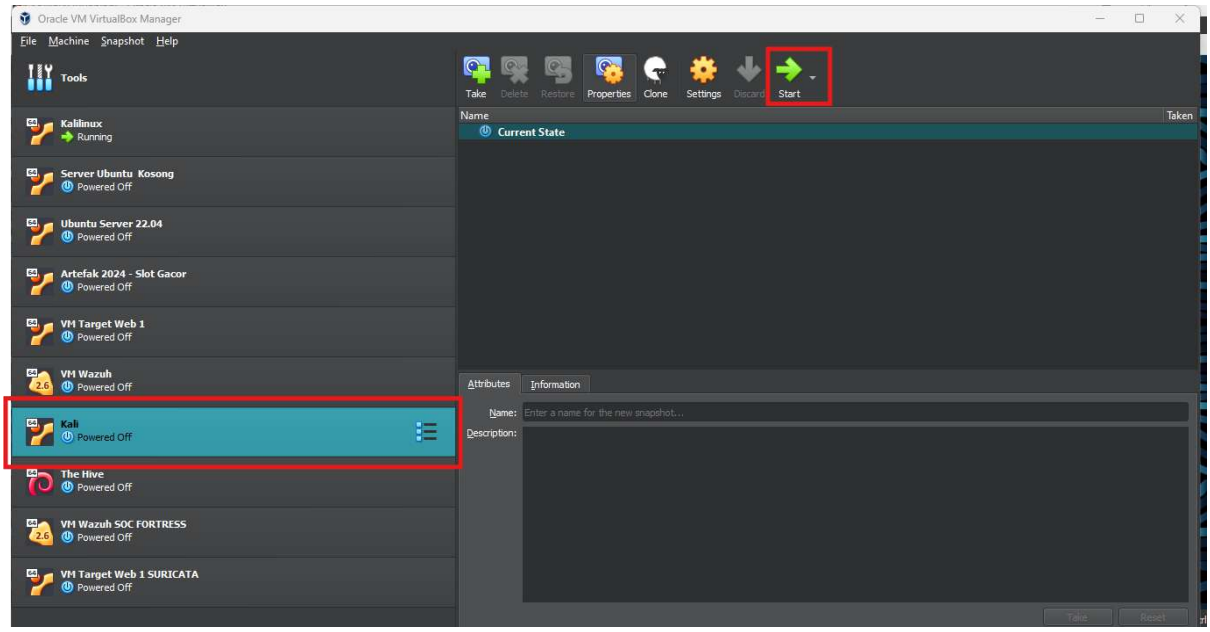
Catatan Khusus

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

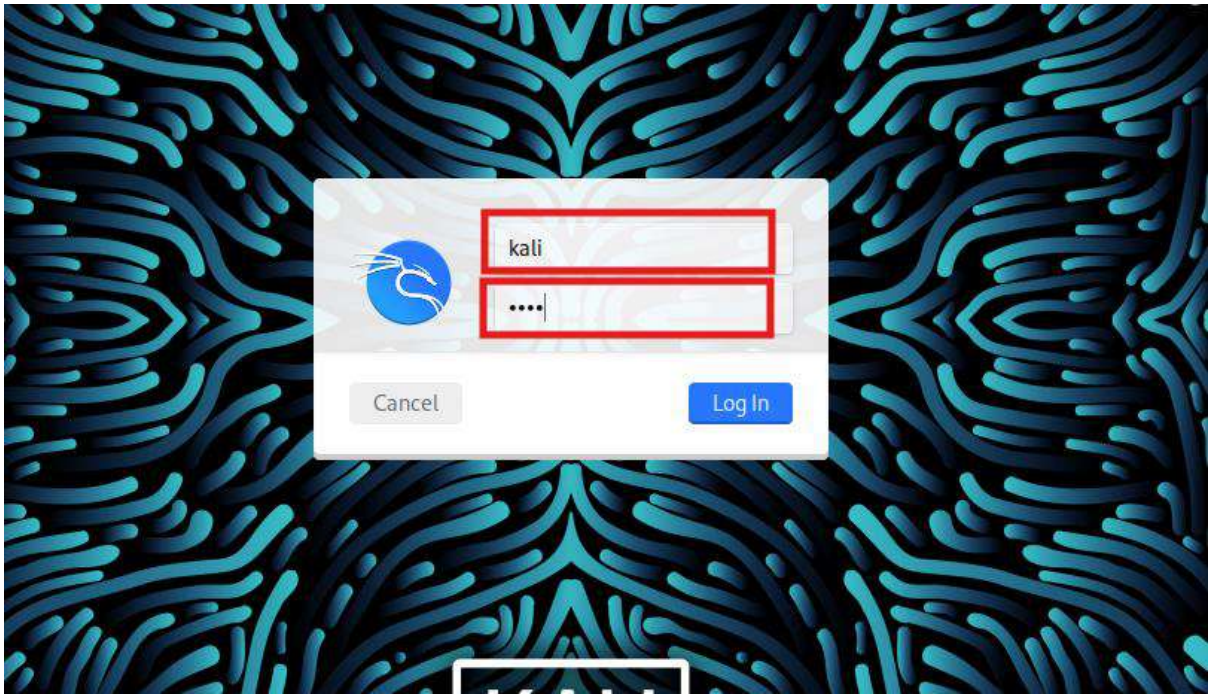
Langkah-Langkah

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

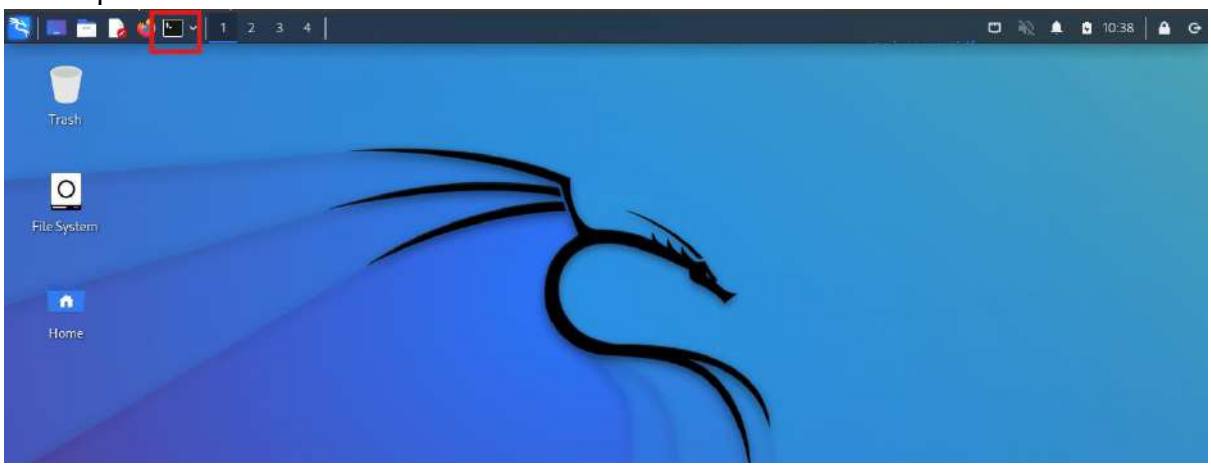




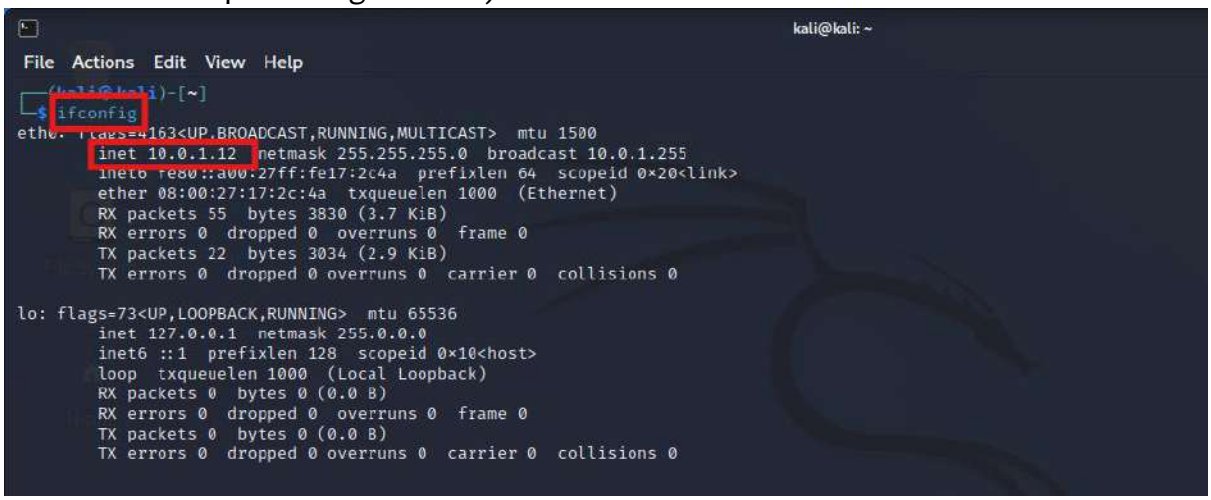
2. Buka pada VM Kali dan masukan *username* `kali` dan *password* `kali`



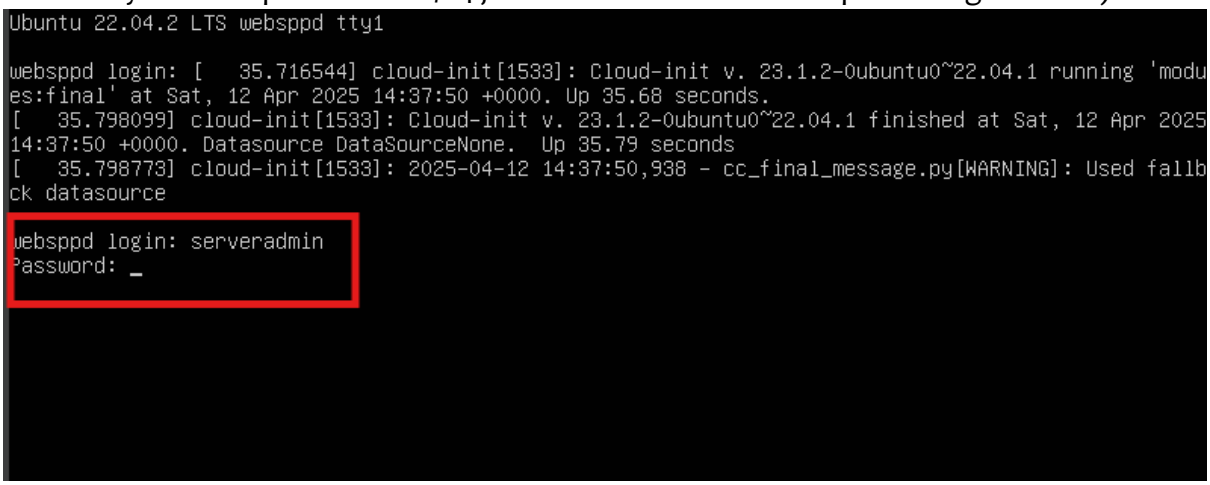
3. Setelah masuk kedalam tampilan awal dekstop, buka terminal pada kiri atas dekstop

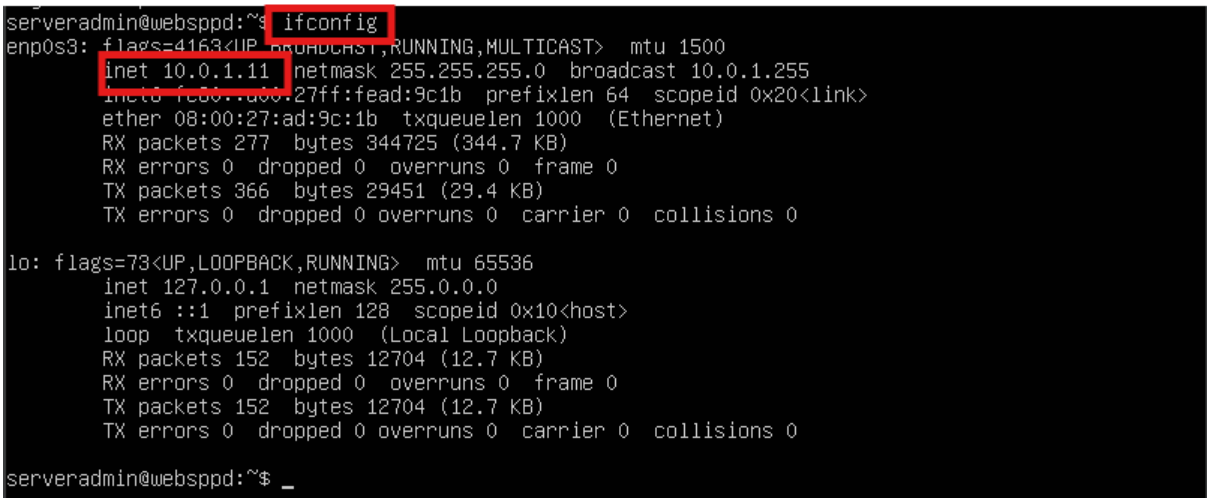


4. Cek IP Kali apakah sudah satu jaringan dengan IP VM Web Target 1 dengan ifconfig (IP Kali dan IP VM Web Target 1 seharusnya berada pada 10.0.1.0/24 jika dalam *enviroment* disiapkan dengan benar)

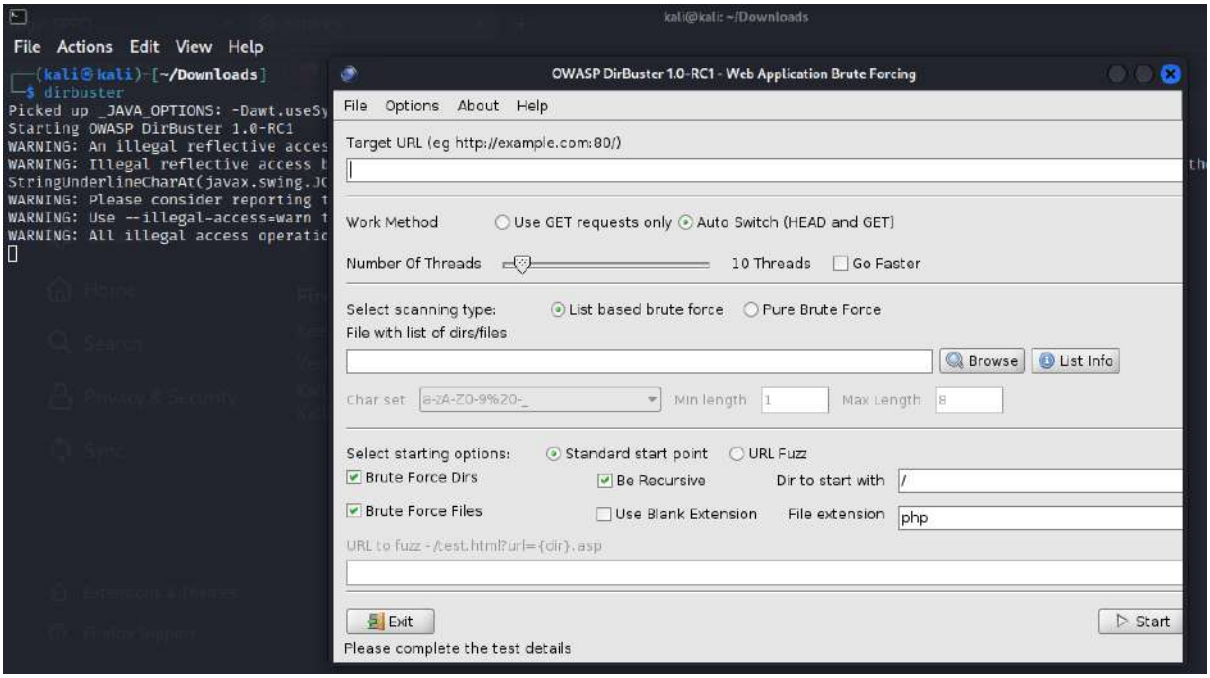


5. Beralih ke VM Web Target 1, cek IP apakah sudah pada network yang sama dengan Kali, login terlebih dahulu dengan *username* `serverdadmin` dan *password* `ubuntu` lalu jalankan perintah `ifconfig` (IP Kali dan IP VM Web Target 1 seharusnya berada pada 10.0.1.0/24 jika dalam *enviroment* disiapkan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

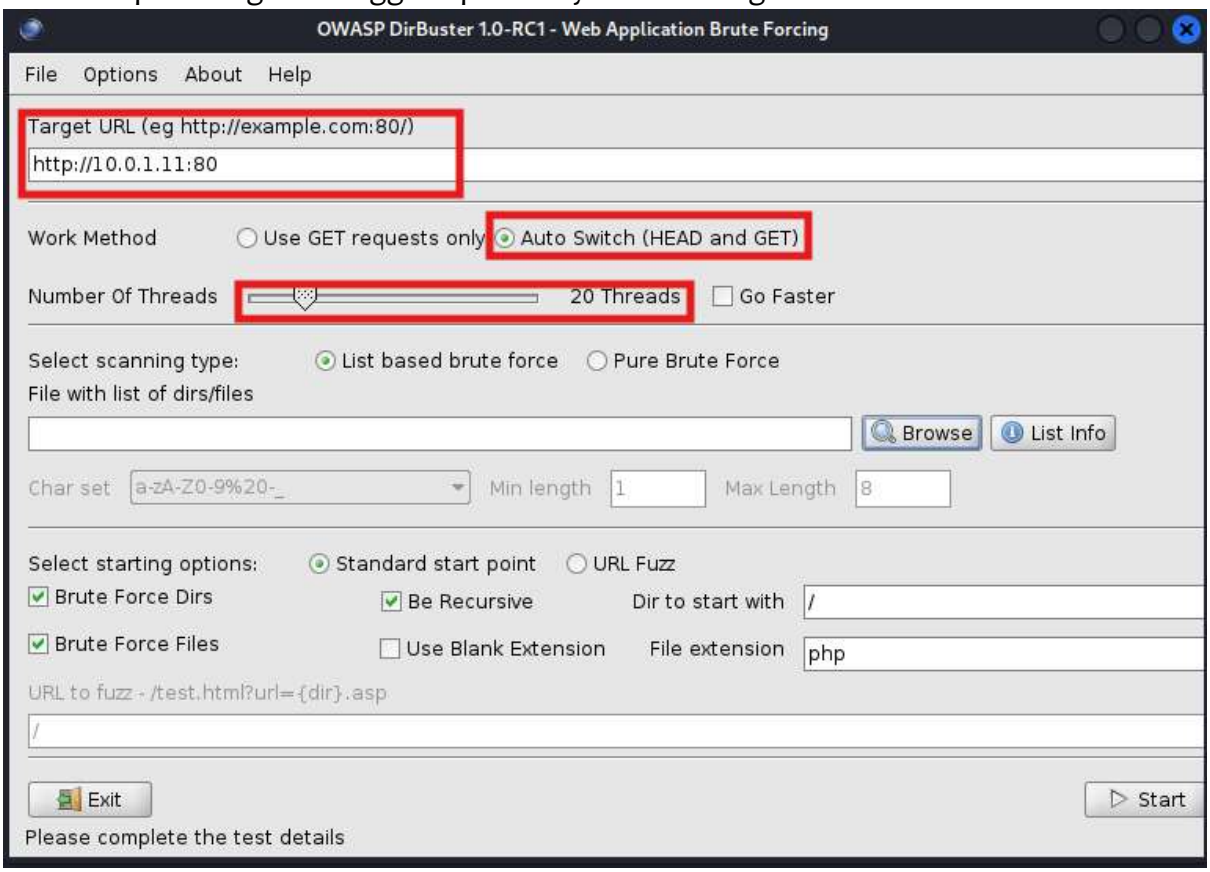




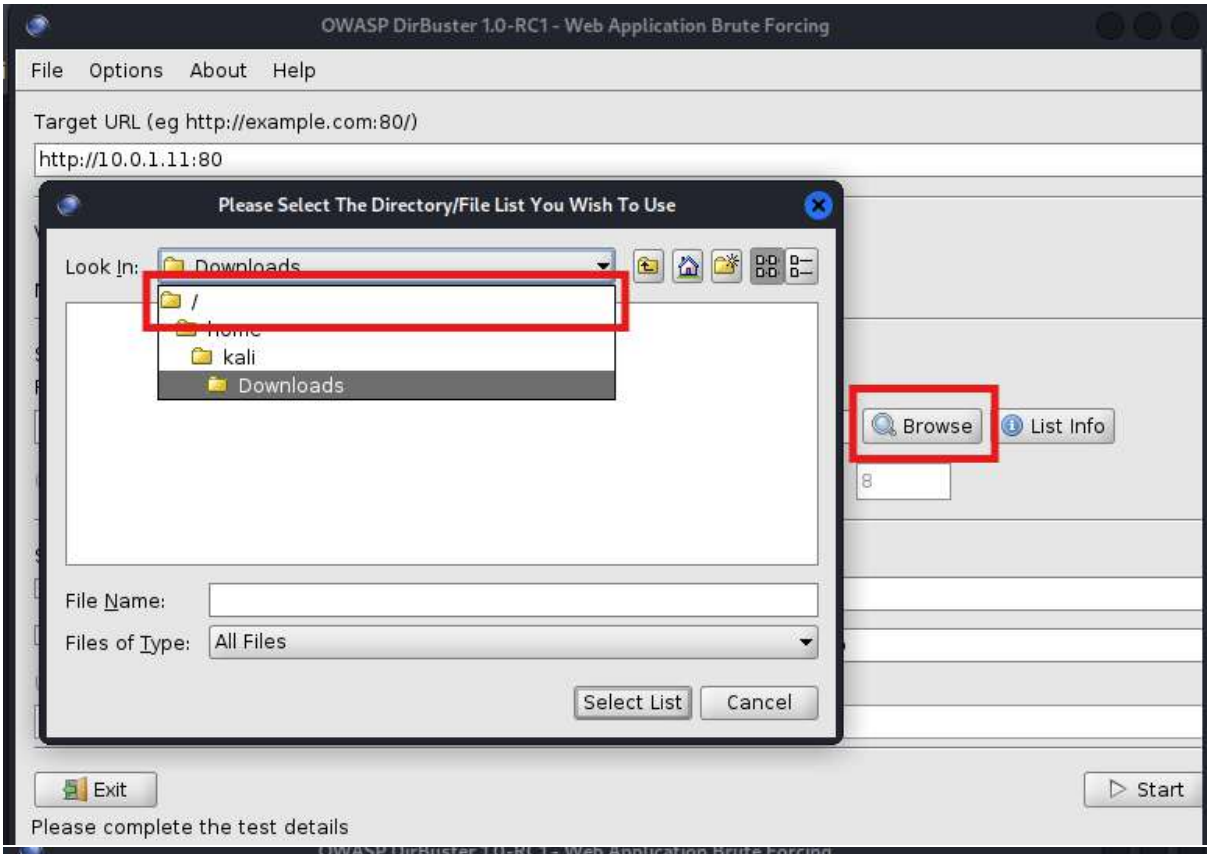
6. Buka termina Kali dan ketik `dirbuster` untuk memulai menggunakan tools, setelah beberapa saat akan muncul tampilan dirbuster pada kali

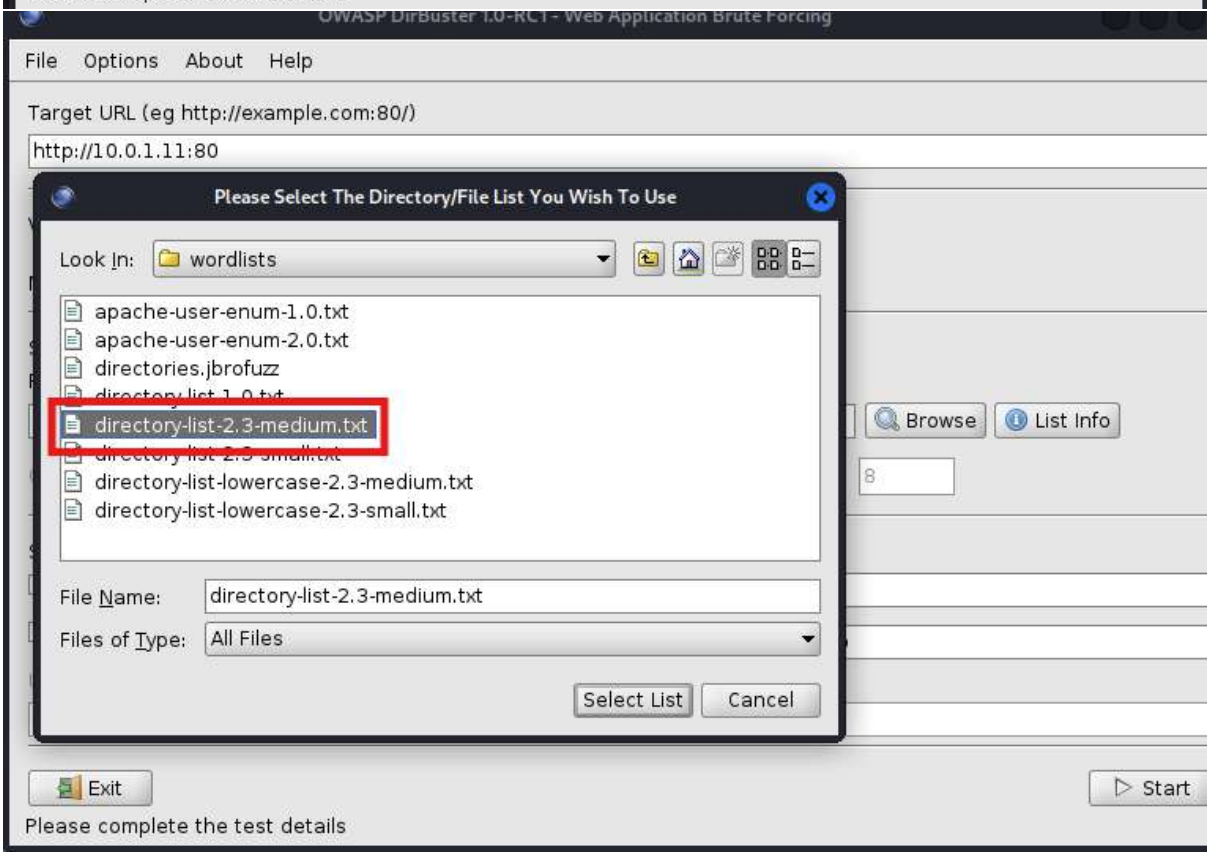


7. Masukan IP target yaitu 10.0.1.11 dan port 80. *Method* yang digunakan pada praktikum kali ini akan menggunakan *HEAD* dan *GET* namun pada dirbuster mengakomodir jika hany diganti *GET* saja. Threads dapat diatur sesuai kemampuan target, semakin banyak threads maka akan menghasilkan banyak paket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

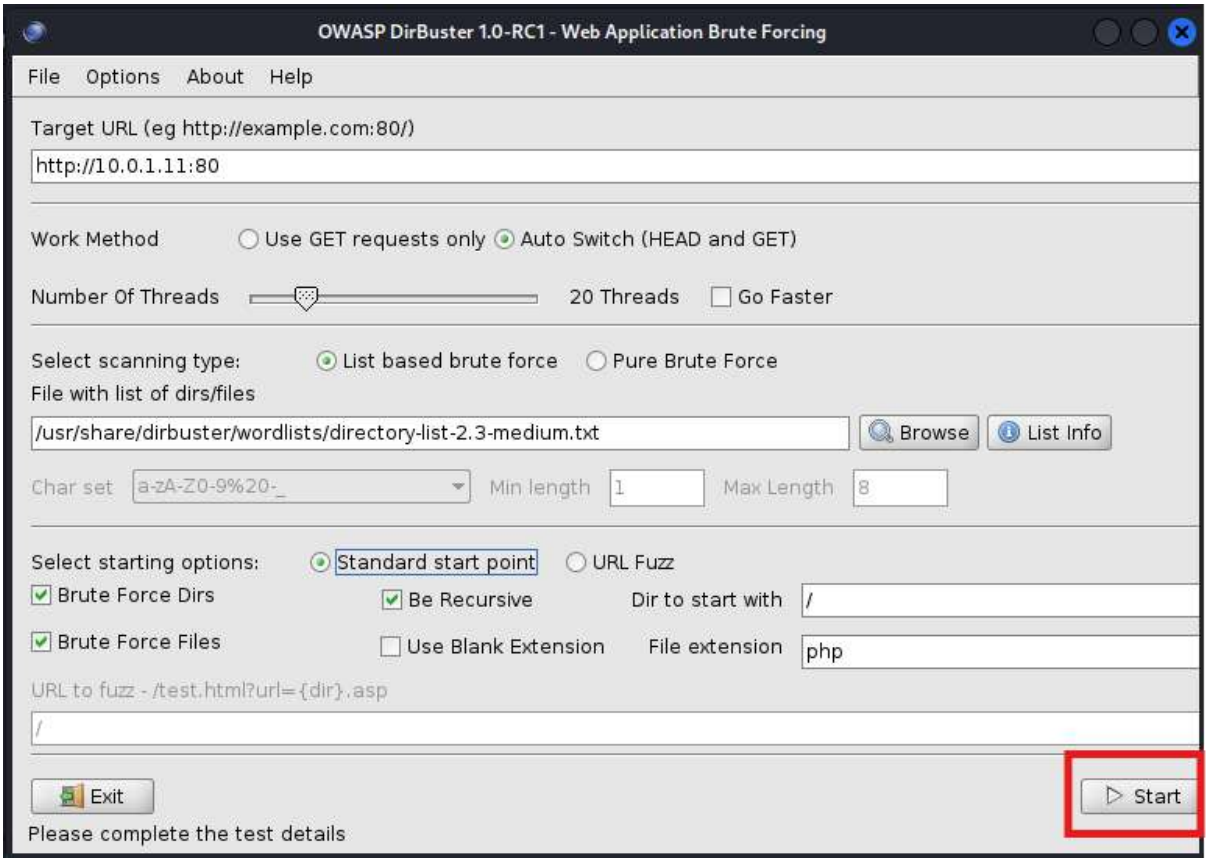


8. Masukan *worldlist* yang akan digunakan, tekan *Browse*I> /> usr> share> dirbuster> wordlist> directory-list-2.3-medium.txt

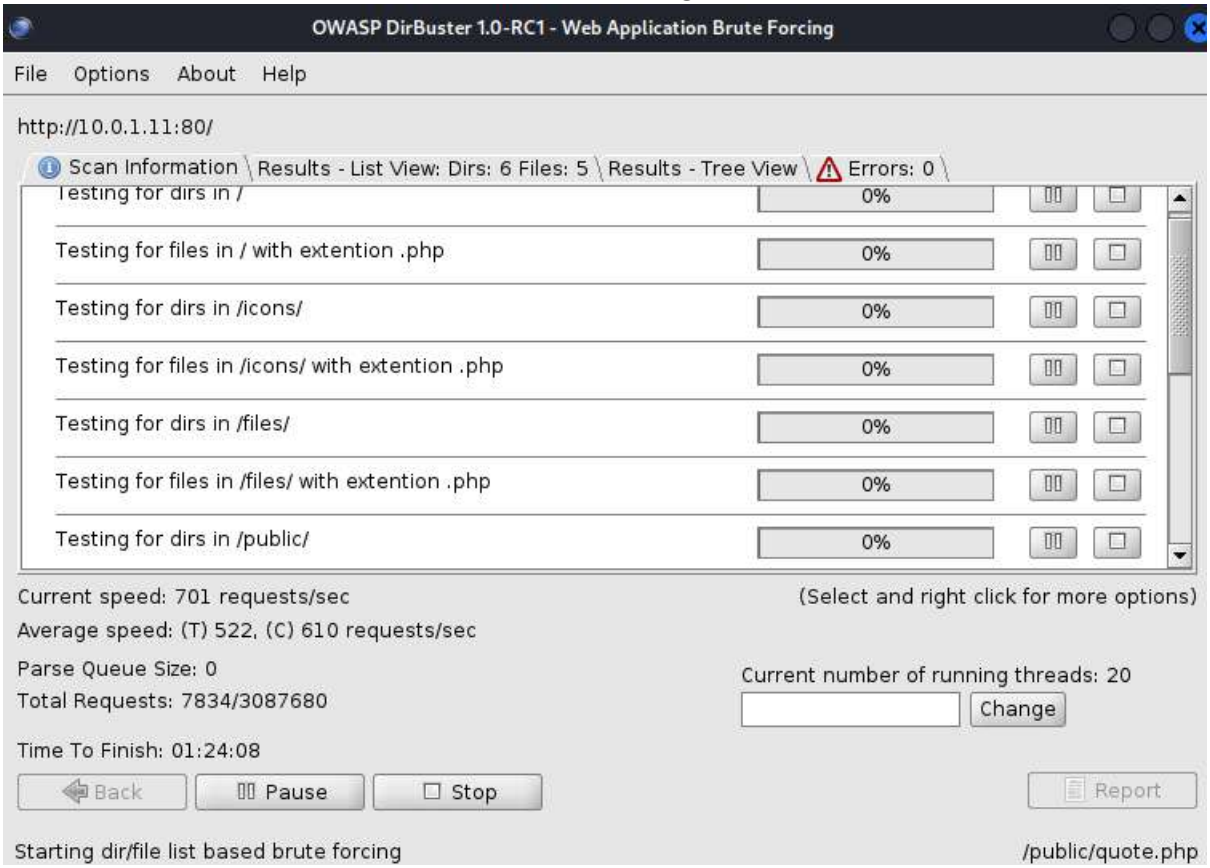




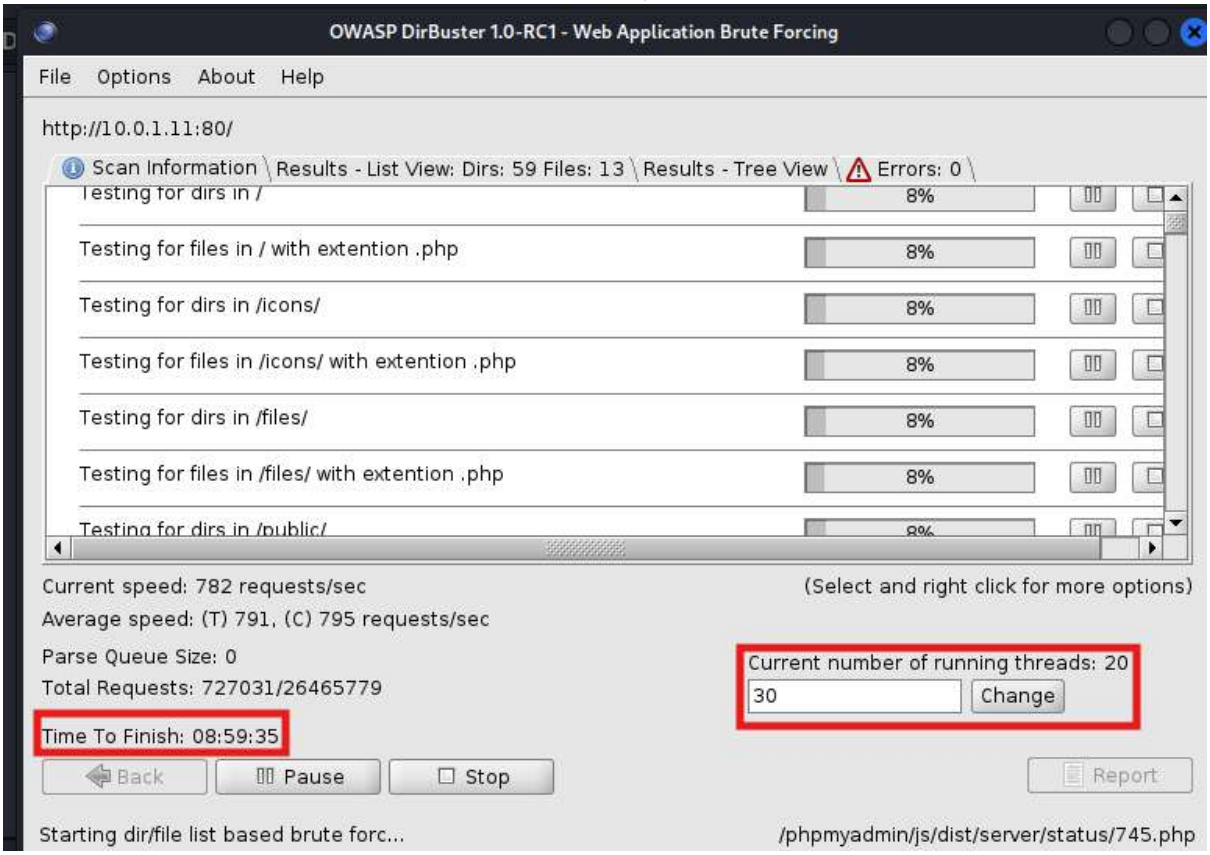
9. Tekan *start* untuk memulai *directory listing*



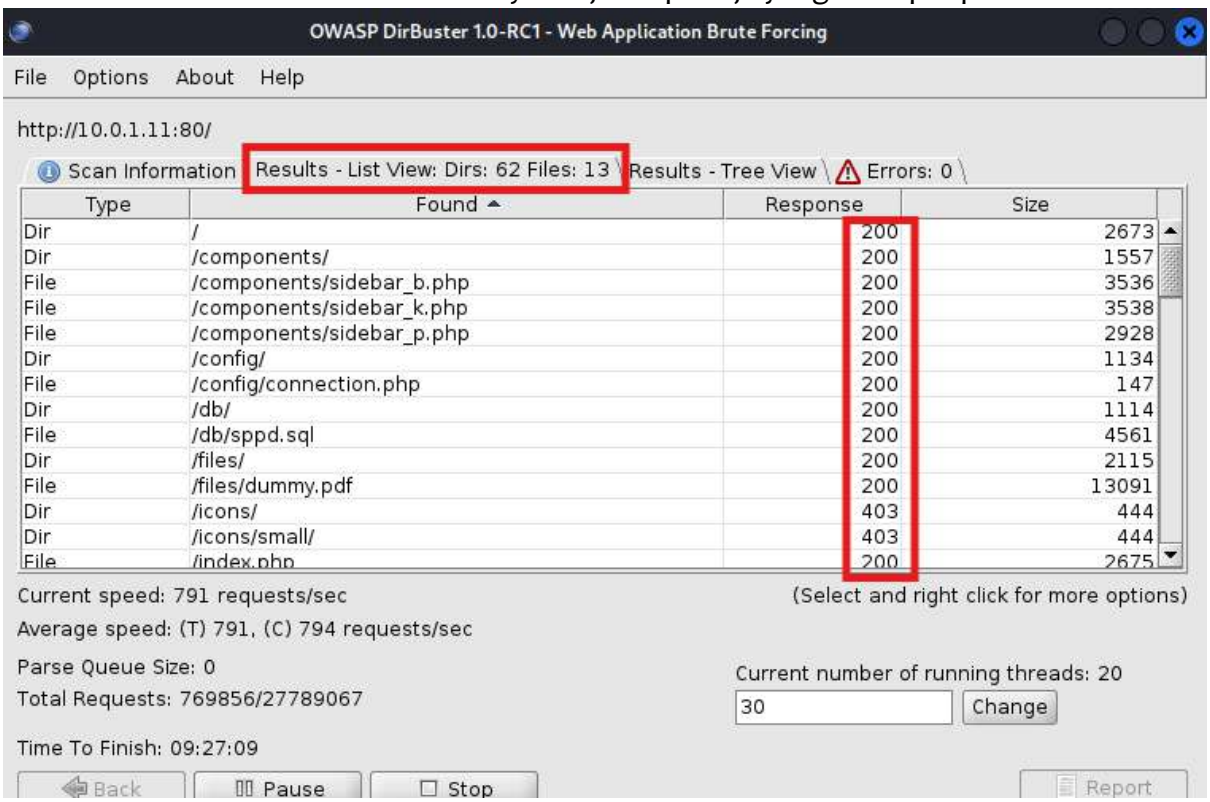
10. Tampilan akan seperti ini jika proses *directory listing* dimulai



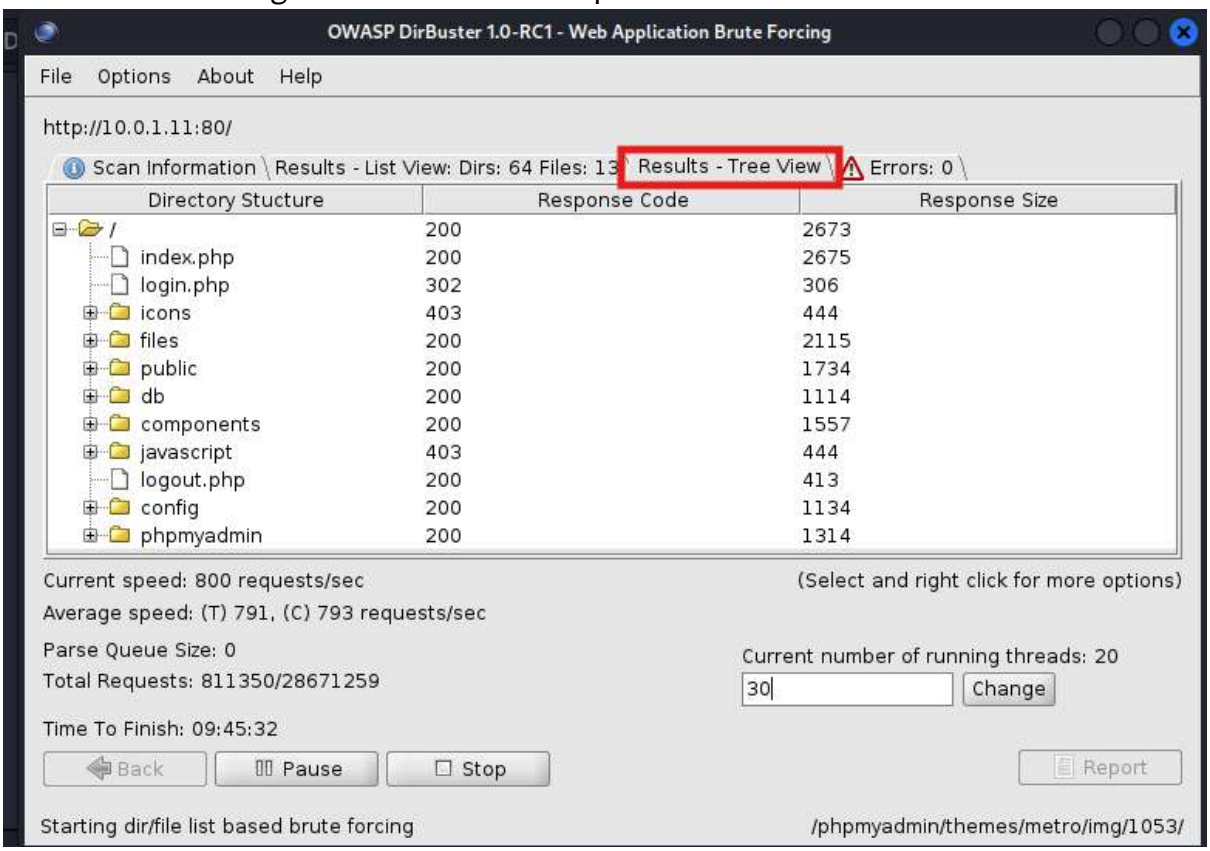
11. Anda dapat melihat berapa waktu yang dibutuhkan untuk menyelesaikan pekerjaan pada kiri bawah dan dapat mengatur jumlah thread pada kanan bawah (semakin banyak thread waktu pekerjaan semakin sedikit)



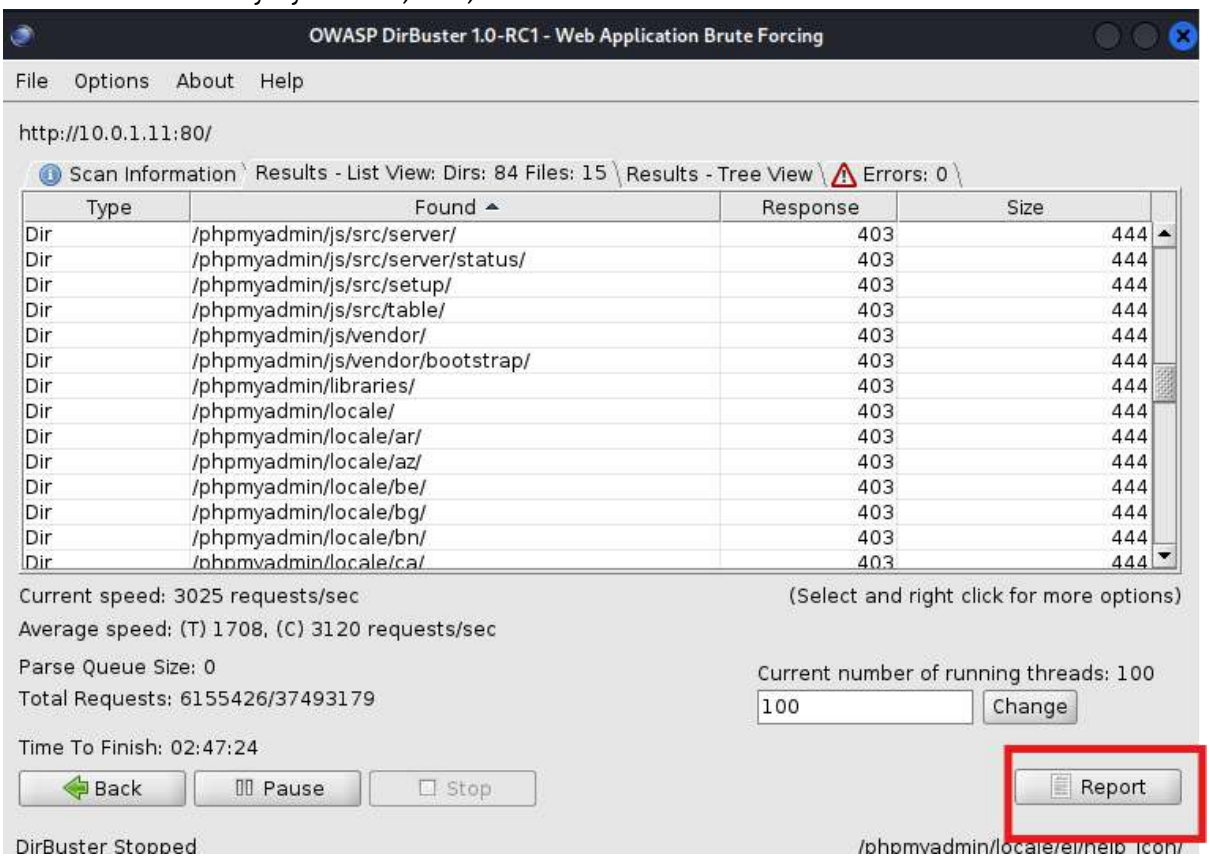
12. Buka tab *result* untuk melihat *directory* dan *files* apa saja yang terdapat pada web



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

Pengunaan 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 dimiiki 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 *scanning*, *enumeration* dan *vurnerabilty analyis* menggunakan Dirbuster.

Tujuan Praktikum

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

Enviroment Laboratorium Virtual

Praktikum ini membutuhkan:

- VM Kali Linux
- VM Target Web 1.

Durasi Praktikum

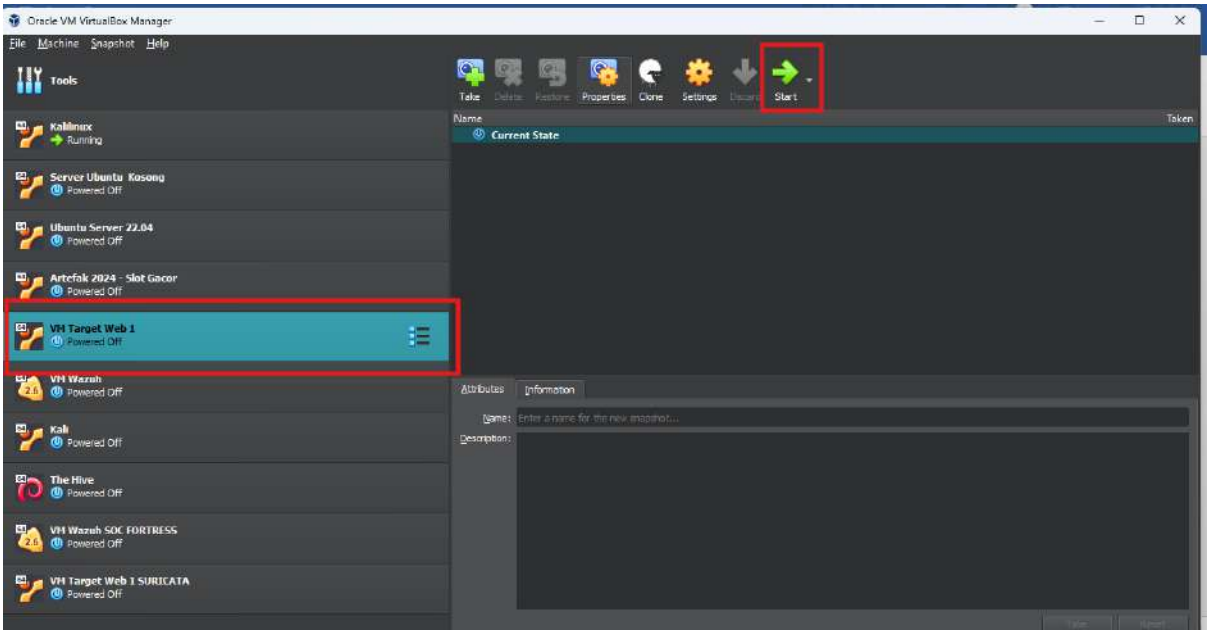
10 Menit

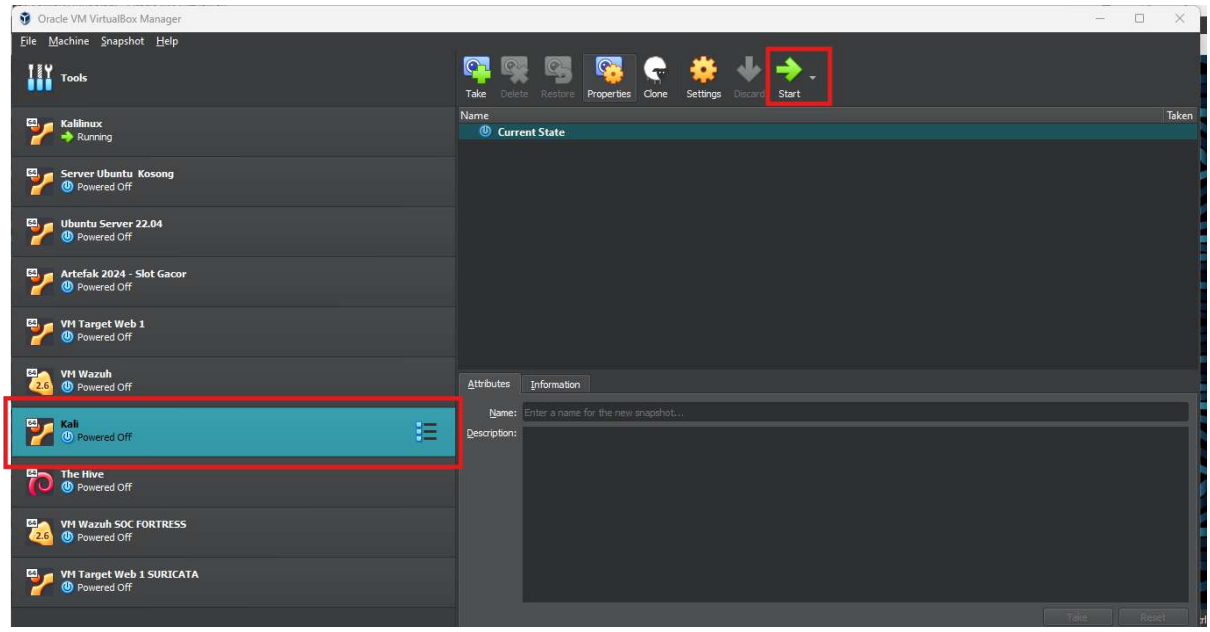
Catatan Khusus

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

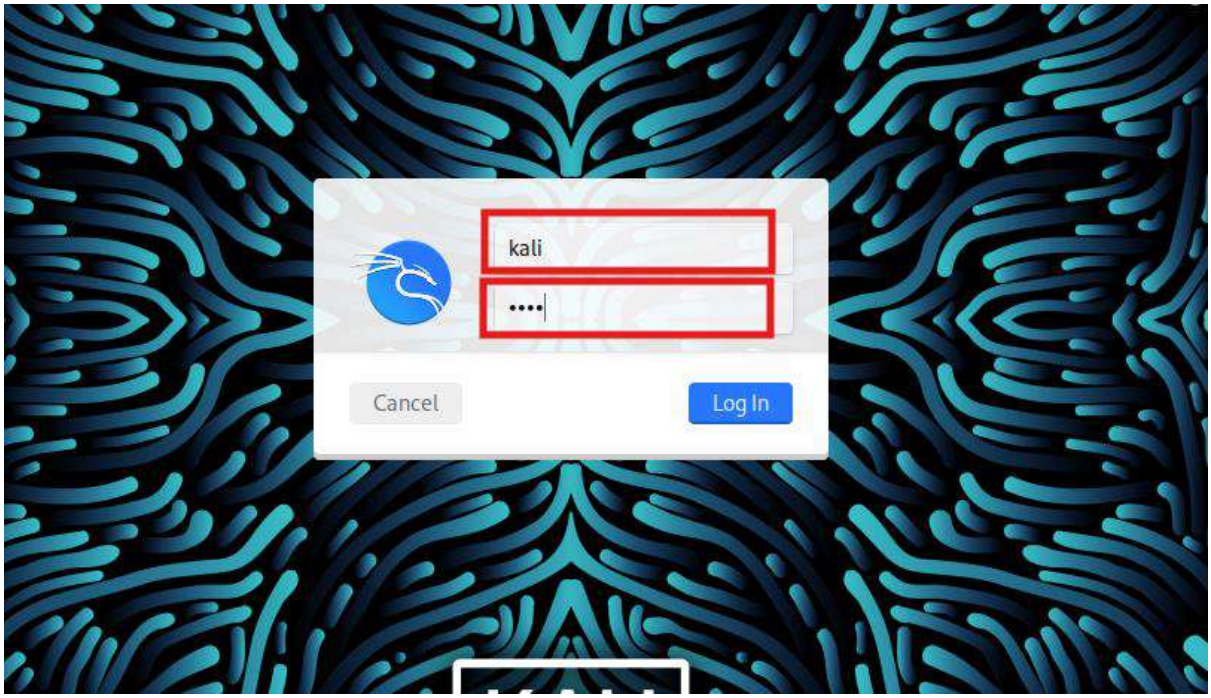
Langkah-Langkah

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

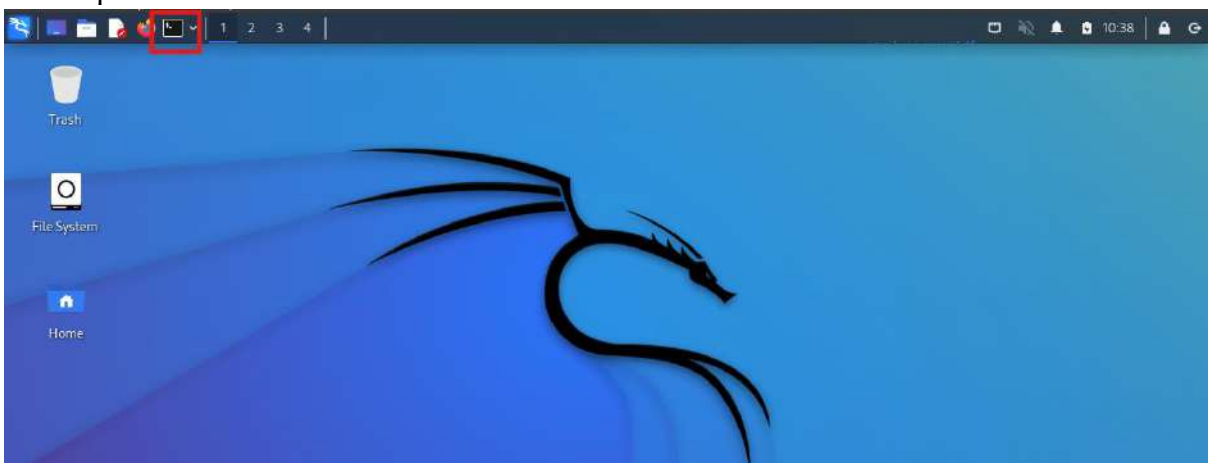




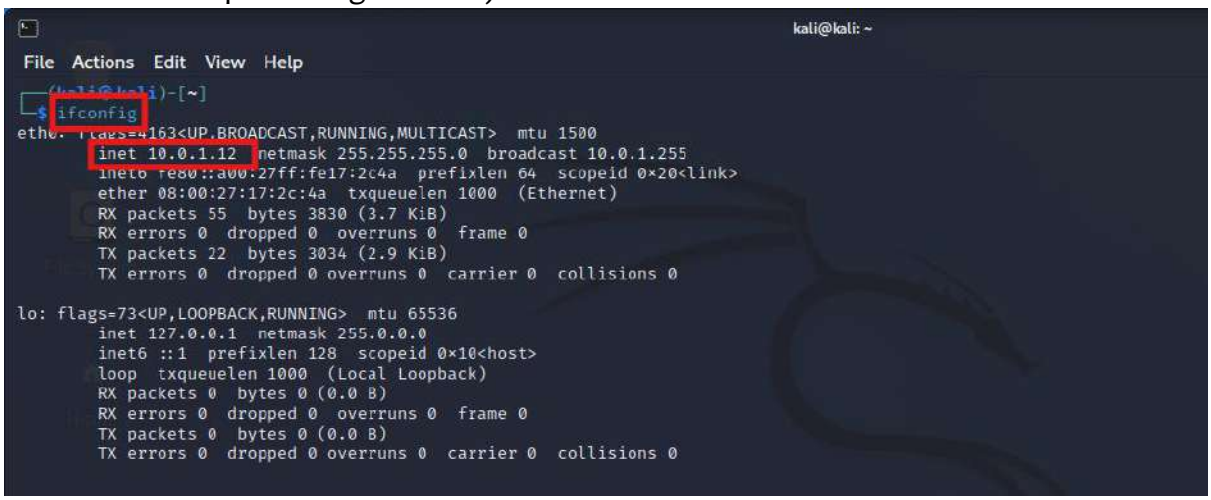
2. Buka pada VM Kali dan masukan *username* `kali` dan *password* `kali`



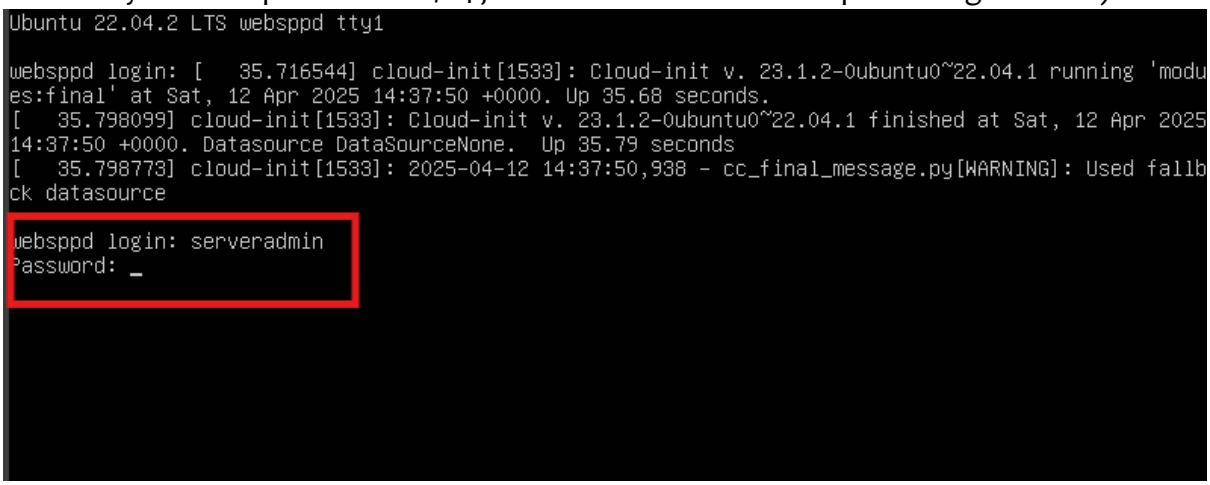
3. Setelah masuk kedalam tampilan awal dekstop, buka terminal pada kiri atas dekstop

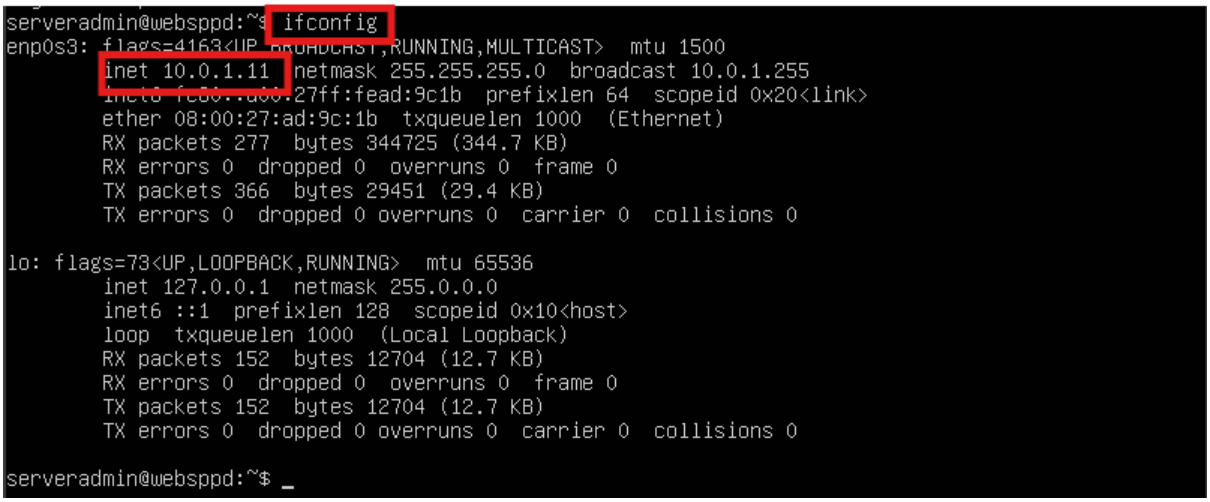


4. Cek IP Kali apakah sudah satu jaringan dengan IP VM Web Target 1 dengan ifconfig (IP Kali dan IP VM Web Target 1 seharusnya berada pada 10.0.1.0/24 jika dalam *enviroment* disiapkan dengan benar)

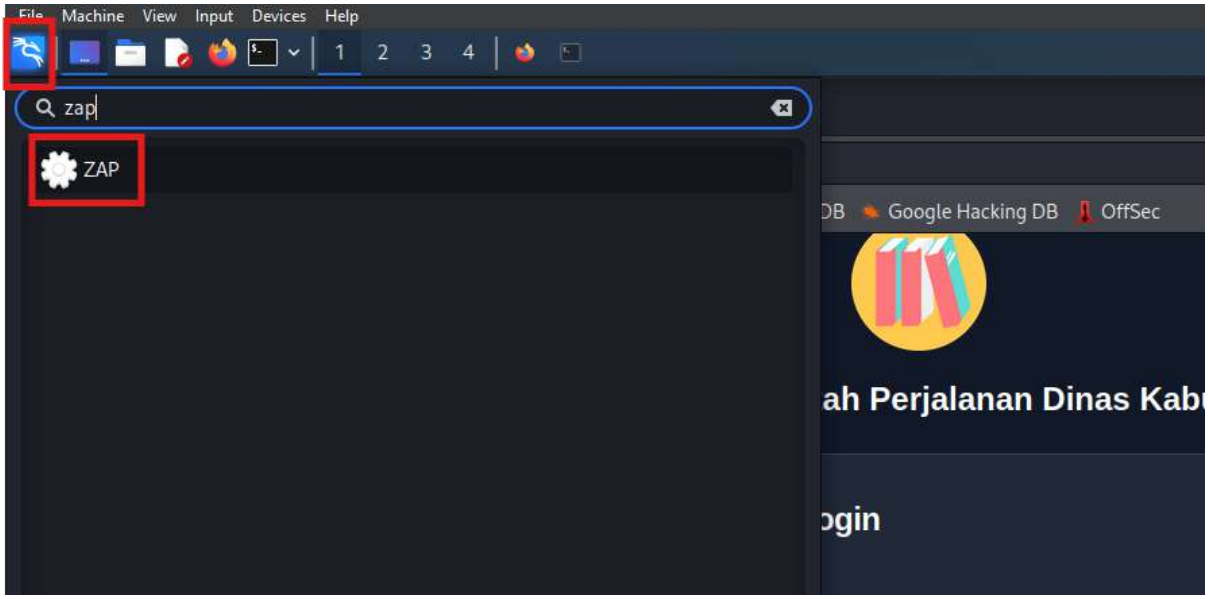


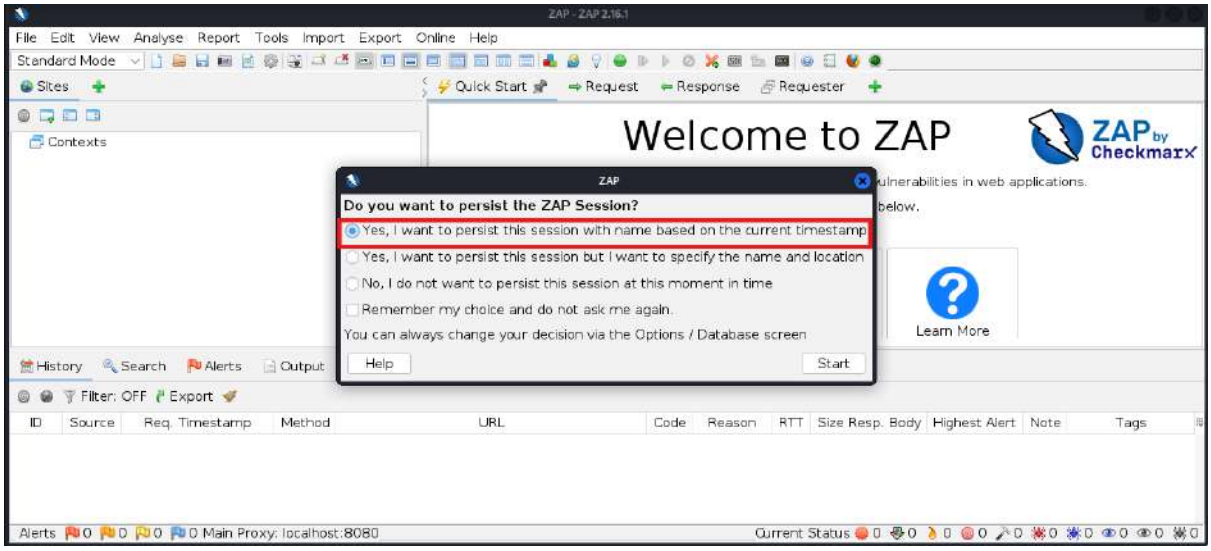
5. Beralih ke VM Web Target 1, cek IP apakah sudah pada network yang sama dengan Kali, login terlebih dahulu dengan *username* `serverdadmin` dan *password* `ubuntu` lalu jalankan perintah `ifconfig` (IP Kali dan IP VM Web Target 1 seharusnya berada pada 10.0.1.0/24 jika dalam *enviroment* disiapkan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



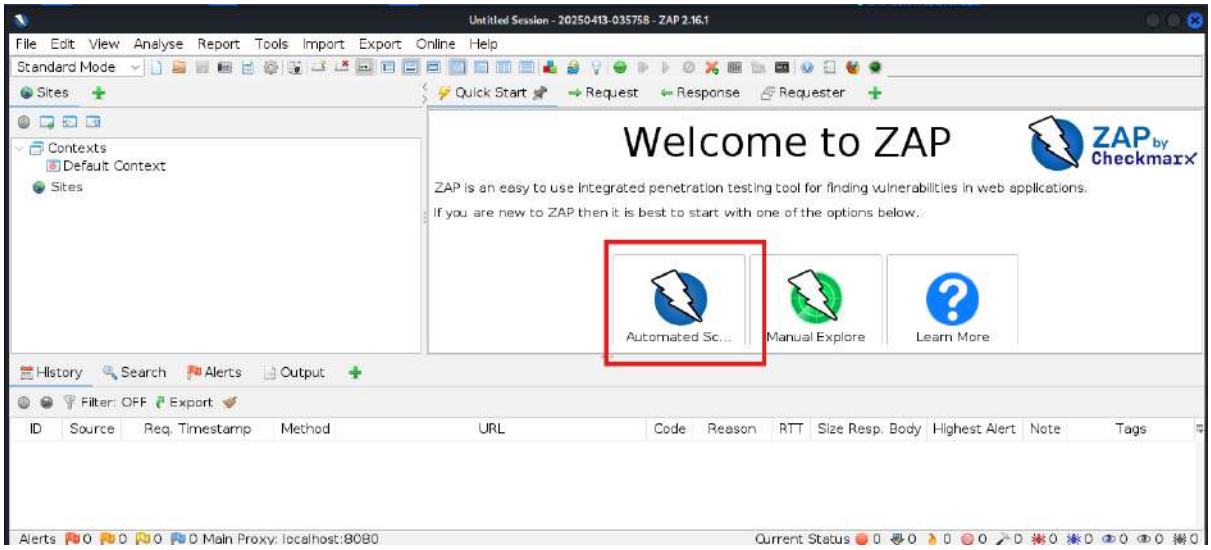


6. Unduh installer OWASP ZAP jika anda menggunakan desktop bukan dari VM Kali laboratorium virtual, lakukan installasi OWASP ZAP terlebih dahulu. Jika anda menggunakan Kali *search* pada bagian *tools* Kali dan tekan ZAP

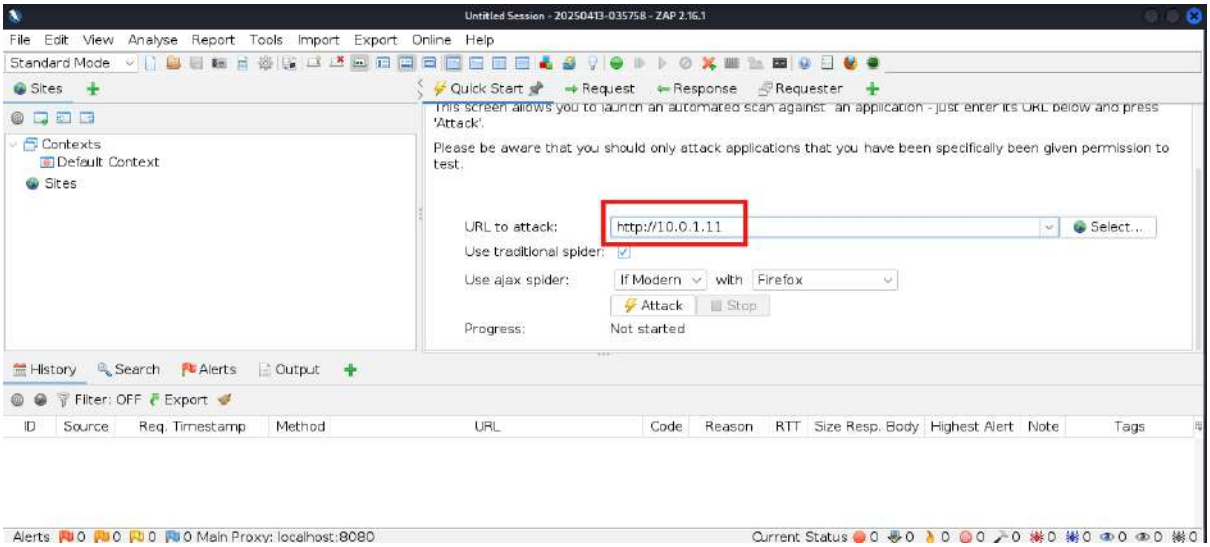


7. 

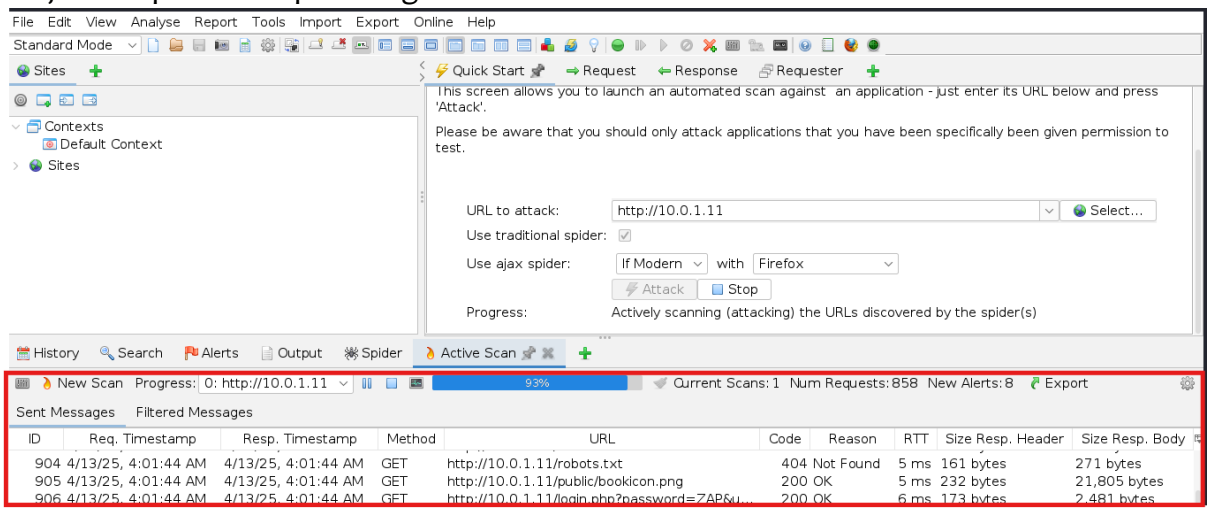
8. Pilih *automated scan*



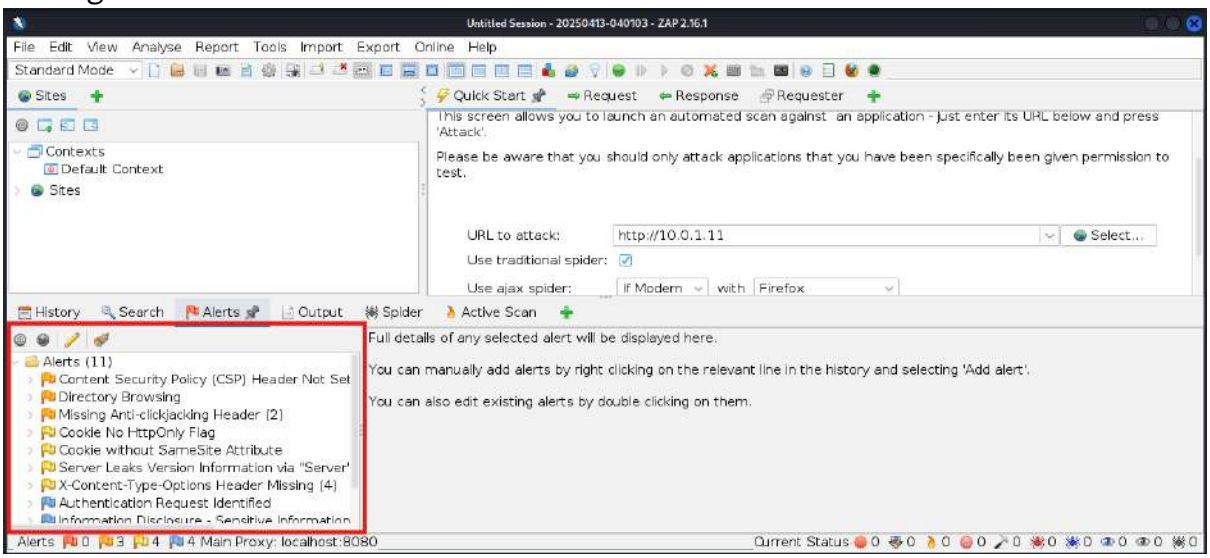
9. Masukan IP VM Web Server Target 1, lalu klik *attack*



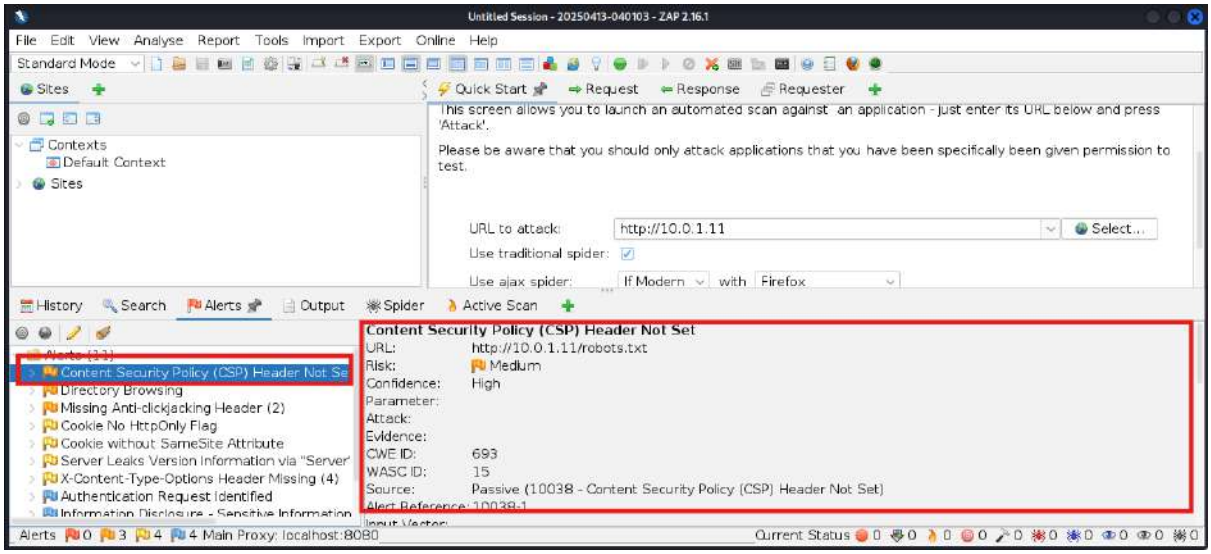
10. Tampilan ketika *attack* sudah dijalankan seperti gambar dibawah ini, proses yang berjalan dapat dilihat pada bagian bawah



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 dimiiki 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*. Saat anda melaksanakan tahapan vurnerability assesment, anda menemukan beberapa bagian pada aset anda yang ternyata menimbulkan kerentanan

Tujuan Praktikum

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

Enviroment Laboratorium Virtual

Praktikum ini membutuhkan:

- Browser terhubung keinternet

Durasi Praktikum

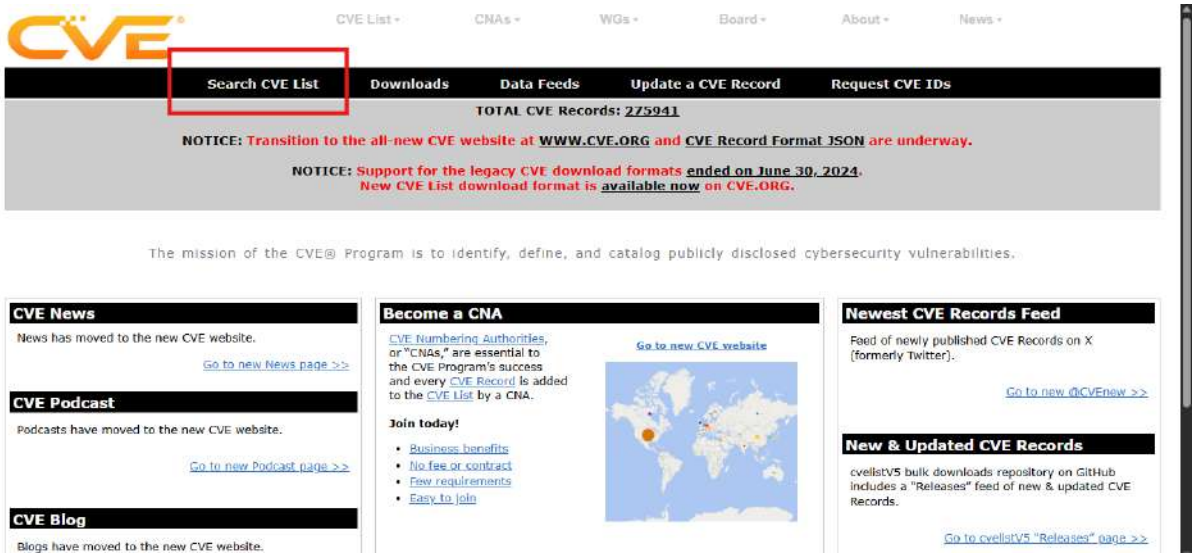
10 Menit

Catatan Khusus

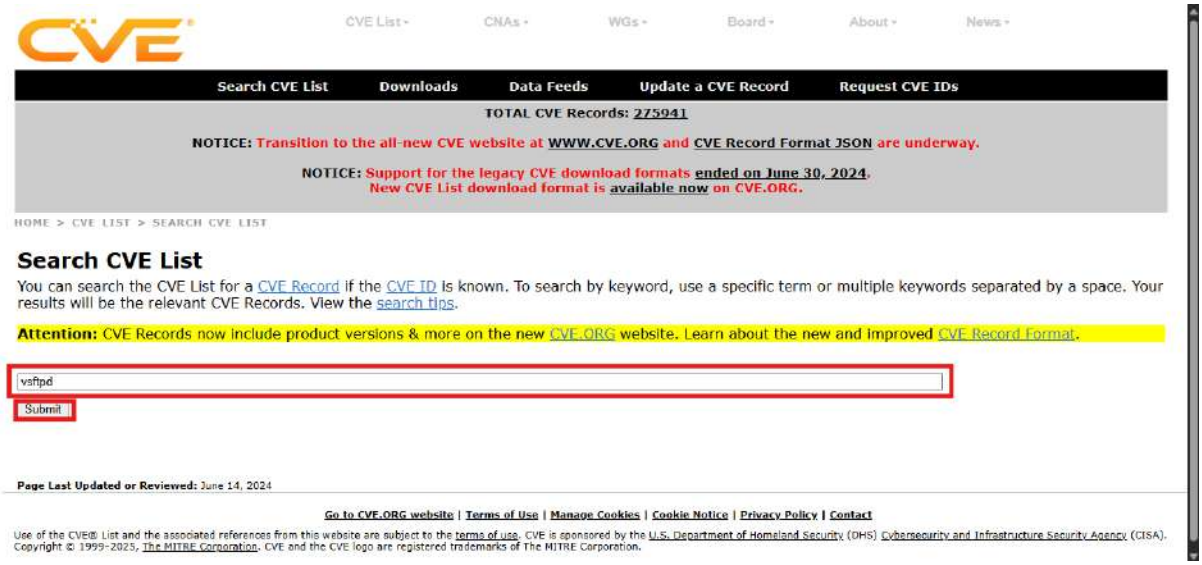
- Siapkan *enviroment* laboratorium virtual sesuai panduan installasi laboratorium virtual
- Dokumentasikan setiap langkah praktikum karena dapat membantu menjawab pertanyaan pada soal yang diberikan

Langkah-Langkah

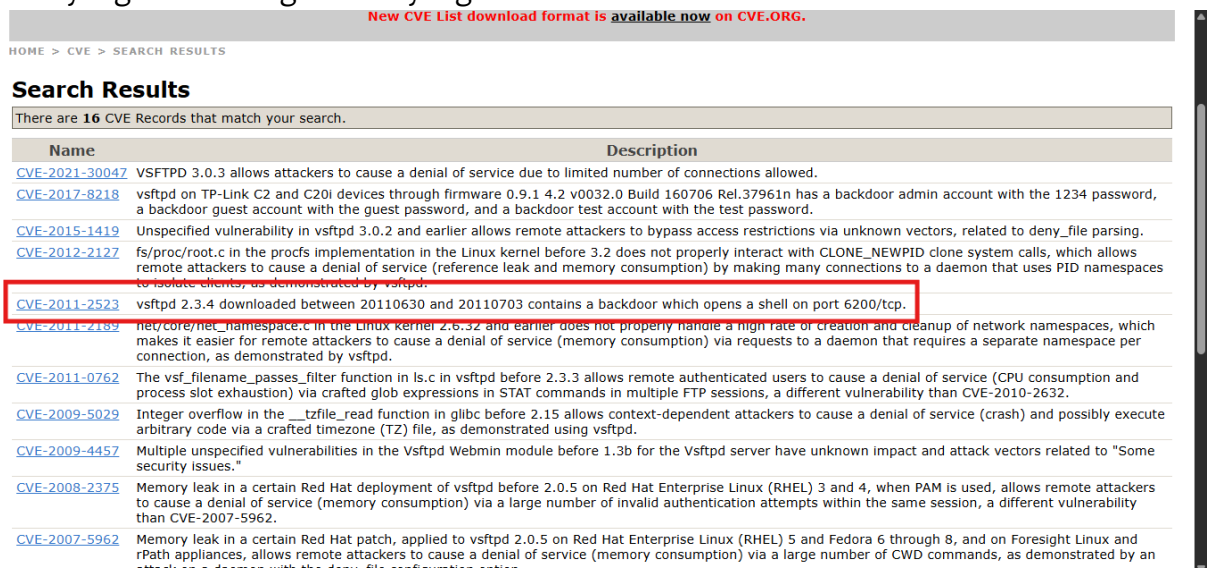
1. Siapkan dokumentasi praktikum penggunaan NMAP pada awal modul ini, pada praktikum ini akan melanjutkan temuan hasil NMAP.
2. Akses pada CVE.mitre.com. Tekan Search CVE List.



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



4. Pilih yang sesuai dengan versi yang anda miliki.



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