

Nama : Asyrof Hafizh Maulana

Organization Security

2. Install Nessus Professional Scanner (Trial Version) di komputer Linux/Windows anda. Gunakan link berikut untuk mendaftar dan mendownload aplikasi Nessus:

<https://www.tenable.com/products/nessus/nessus-professional/evaluate>

Setelah terpasang dan berjalan dengan baik, gunakan nessus untuk melakukan scanning terhadap :

1. Jaringan Intranet di Rumah/Kost atau Kampus anda

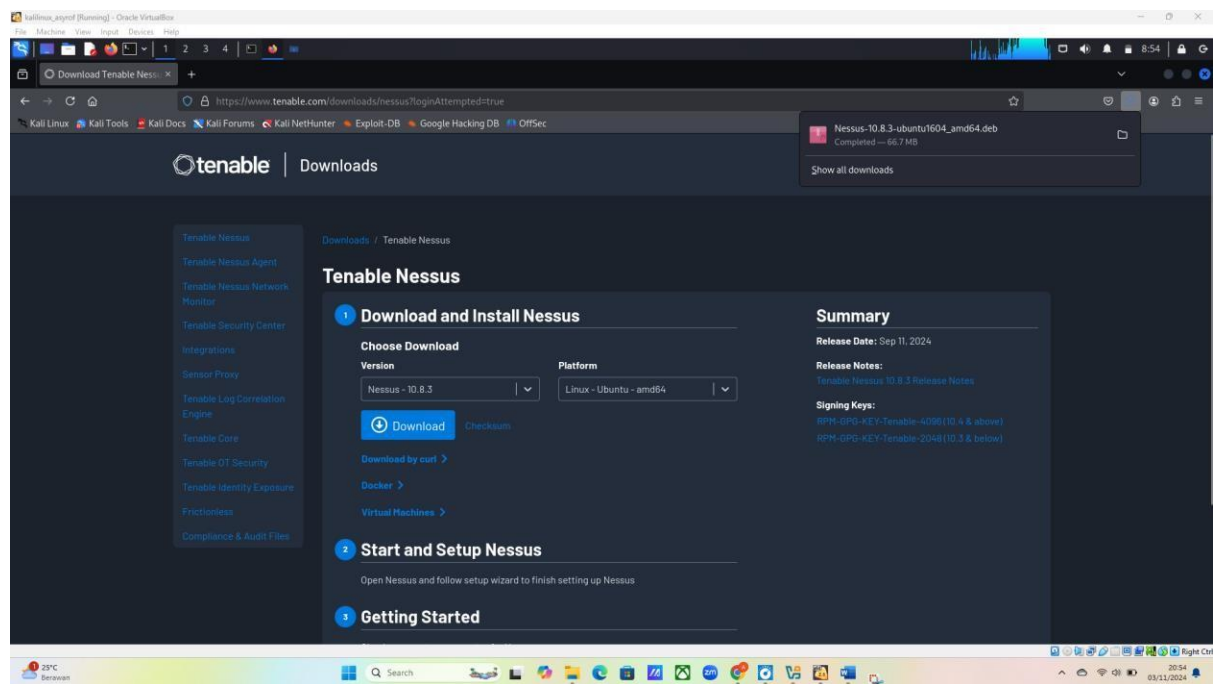
2. Web Server target.rootbrain.com

Jelaskan temuan temuan yang anda dapatkan setelah berhasil melakukan assessment/scanning terhadap target target tersebut. Apakah ada vulnerability yang critical/high yang ditemukan, dan apa saja solusi yang ditawarkan oleh tools tersebut.

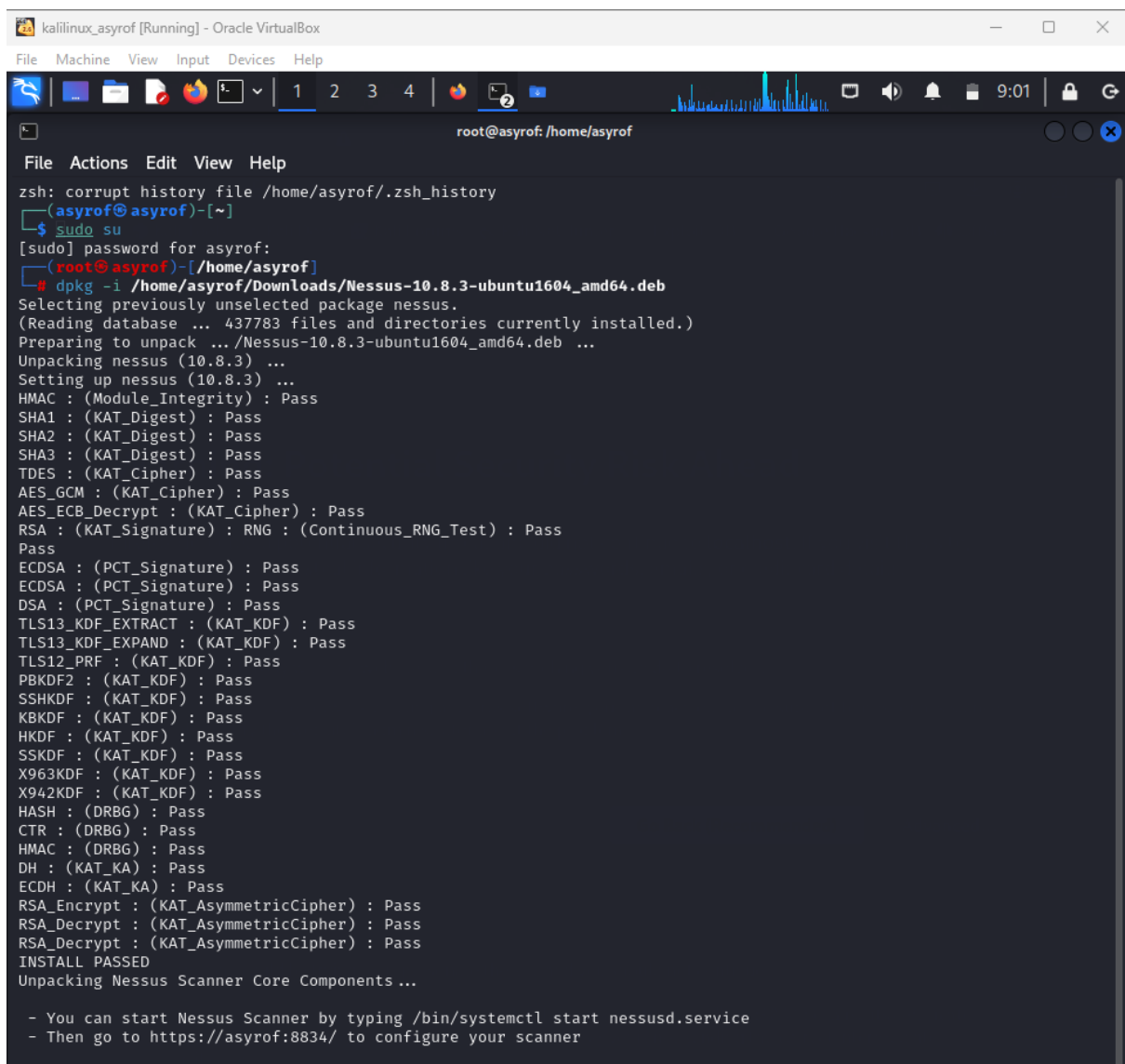
Jawab :

Download Nessus :

<https://www.tenable.com/downloads/nessus?loginAttempted=true>



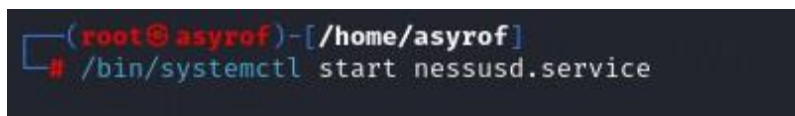
Install Nessus :



```
File Actions Edit View Help
zsh: corrupt history file /home/asyrof/.zsh_history
(asyrof@asyrof)-[~]
$ sudo su
[sudo] password for asyrof:
(root@asyrof)-[/home/asyrof]
# dpkg -i /home/asyrof/Downloads/Nessus-10.8.3-ubuntu1604_amd64.deb
Selecting previously unselected package nessus.
(Reading database ... 437783 files and directories currently installed.)
Preparing to unpack .../Nessus-10.8.3-ubuntu1604_amd64.deb ...
Unpacking nessus (10.8.3) ...
Setting up nessus (10.8.3) ...
HMAC : (Module_Integrity) : Pass
SHA1 : (KAT_Digest) : Pass
SHA2 : (KAT_Digest) : Pass
SHA3 : (KAT_Digest) : Pass
TDES : (KAT_Cipher) : Pass
AES_GCM : (KAT_Cipher) : Pass
AES_ECB_Decrypt : (KAT_Cipher) : Pass
RSA : (KAT_Signature) : RNG : (Continuous_RNG_Test) : Pass
Pass
ECDSA : (PCT_Signature) : Pass
ECDSA : (PCT_Signature) : Pass
DSA : (PCT_Signature) : Pass
TLS13_KDF_EXTRACT : (KAT_KDF) : Pass
TLS13_KDF_EXPAND : (KAT_KDF) : Pass
TLS12_PRF : (KAT_KDF) : Pass
PBKDF2 : (KAT_KDF) : Pass
SSHKDF : (KAT_KDF) : Pass
KBKDF : (KAT_KDF) : Pass
HKDF : (KAT_KDF) : Pass
SSKDF : (KAT_KDF) : Pass
X963KDF : (KAT_KDF) : Pass
X942KDF : (KAT_KDF) : Pass
HASH : (DRBG) : Pass
CTR : (DRBG) : Pass
HMAC : (DRBG) : Pass
DH : (KAT_KA) : Pass
ECDH : (KAT_KA) : Pass
RSA_Encrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
INSTALL PASSED
Unpacking Nessus Scanner Core Components...

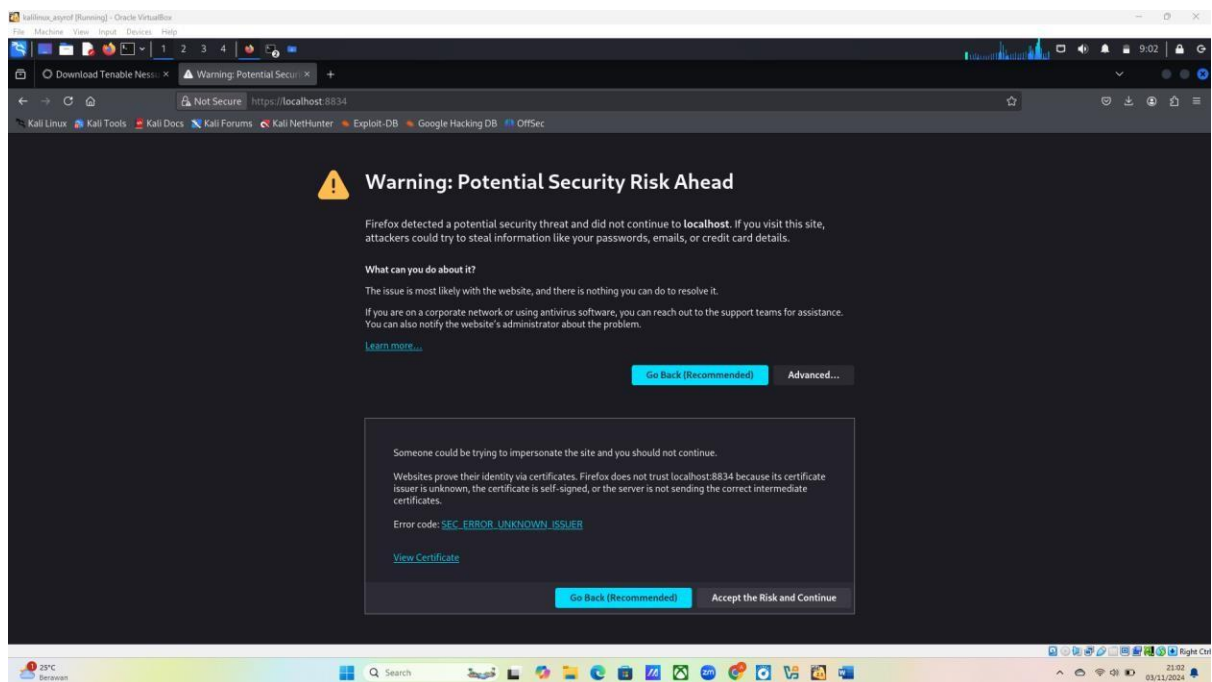
- You can start Nessus Scanner by typing /bin/systemctl start nessusd.service
- Then go to https://asyrof:8834/ to configure your scanner
```

Start Nessus :

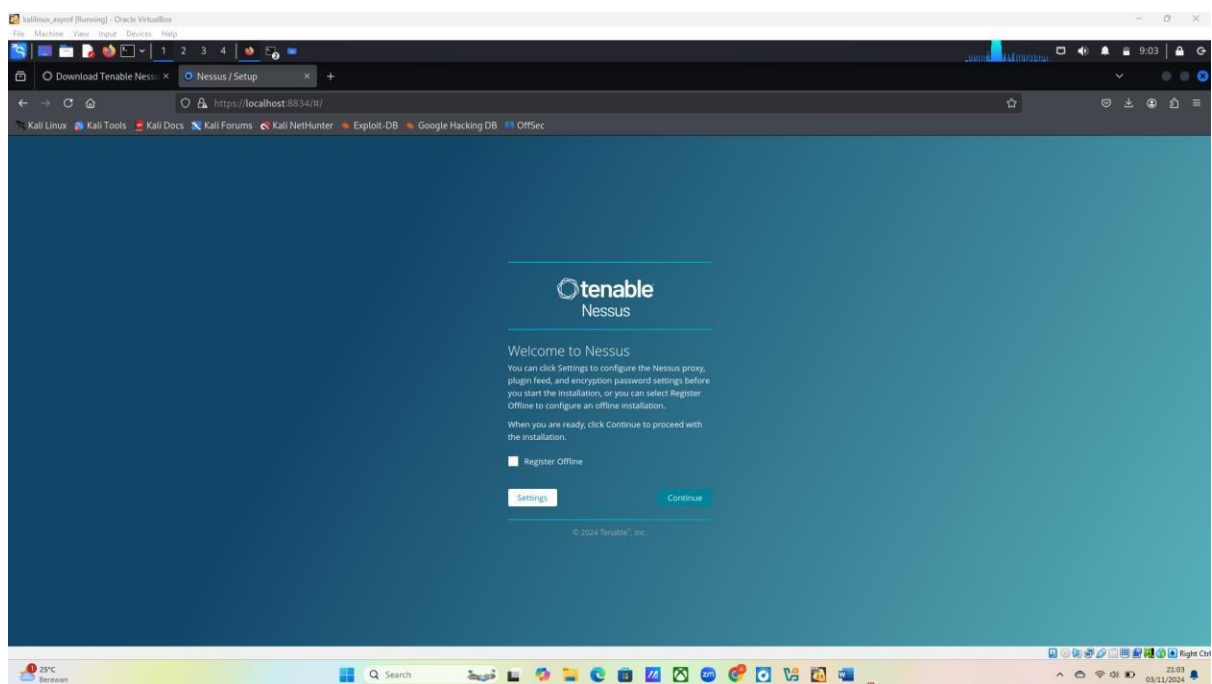


```
(root@asyrof)-[/home/asyrof]
# /bin/systemctl start nessusd.service
```

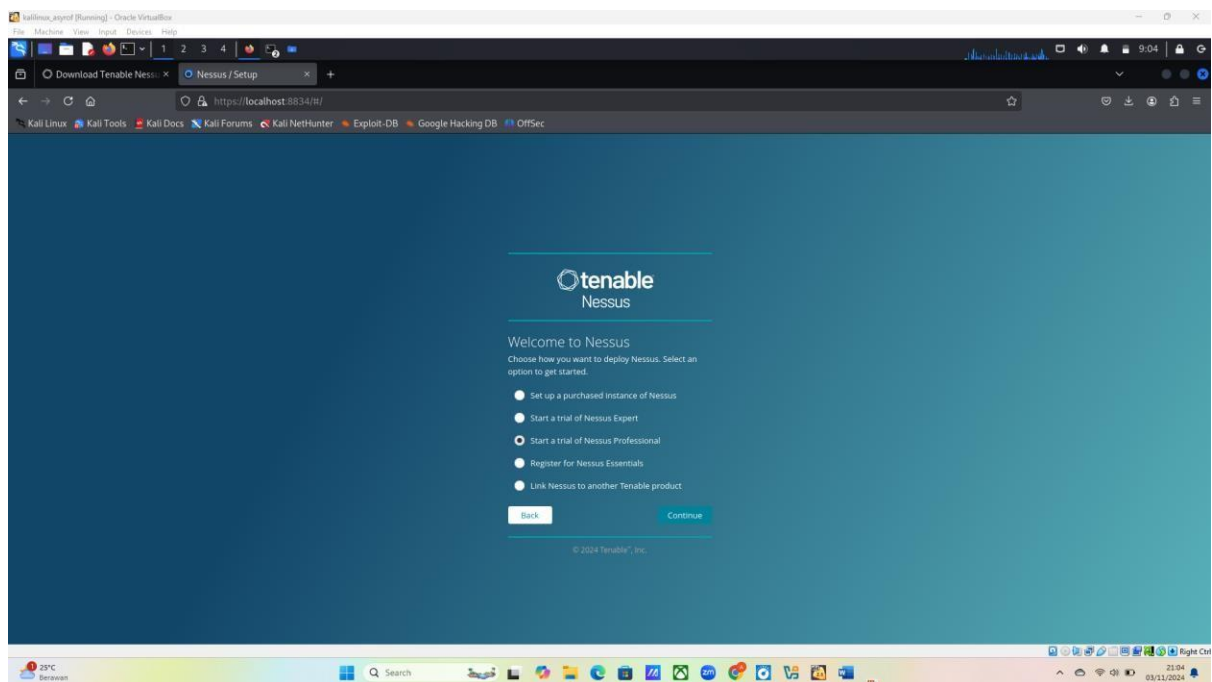
Masuk localhost Nessus <https://localhost:8834/> :



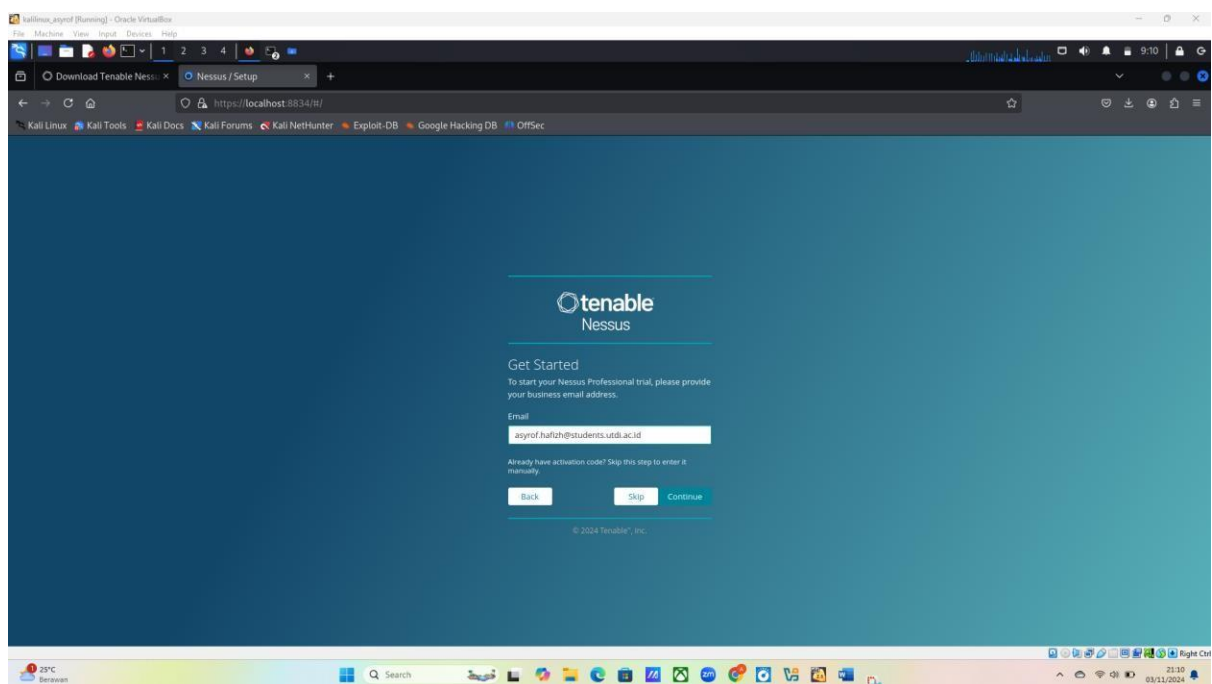
Accept the risk and continue :



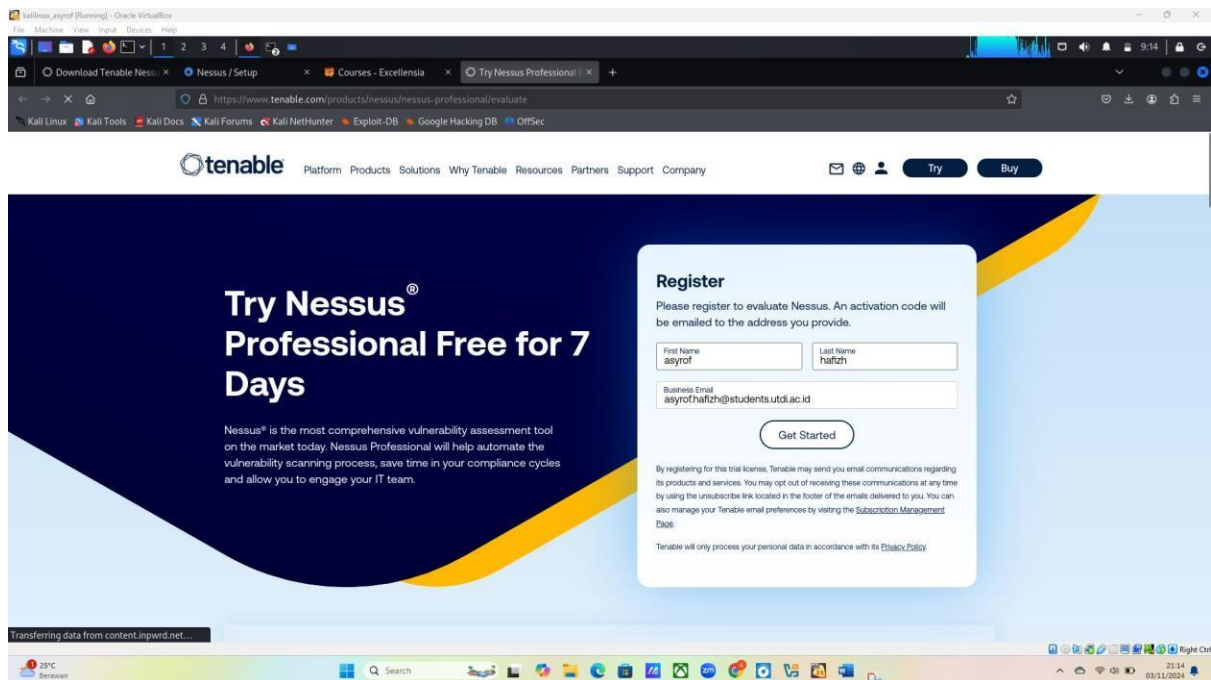
Klik continue dan pilih trial Nessus :



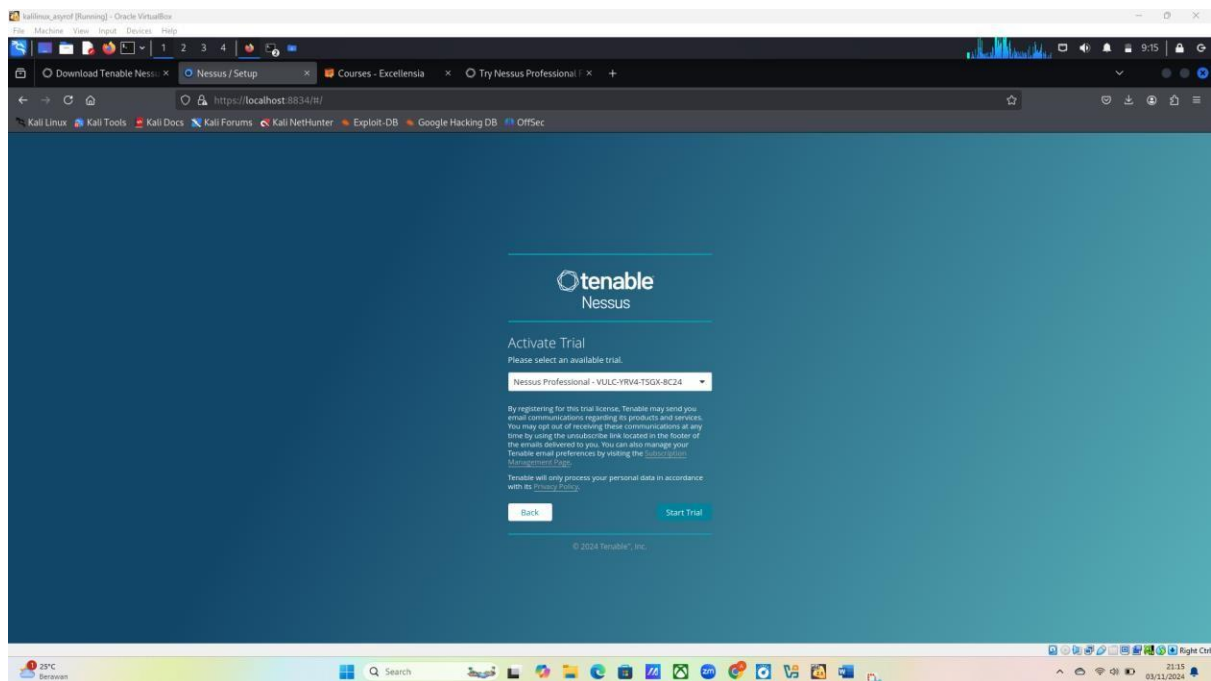
Masukkan email :



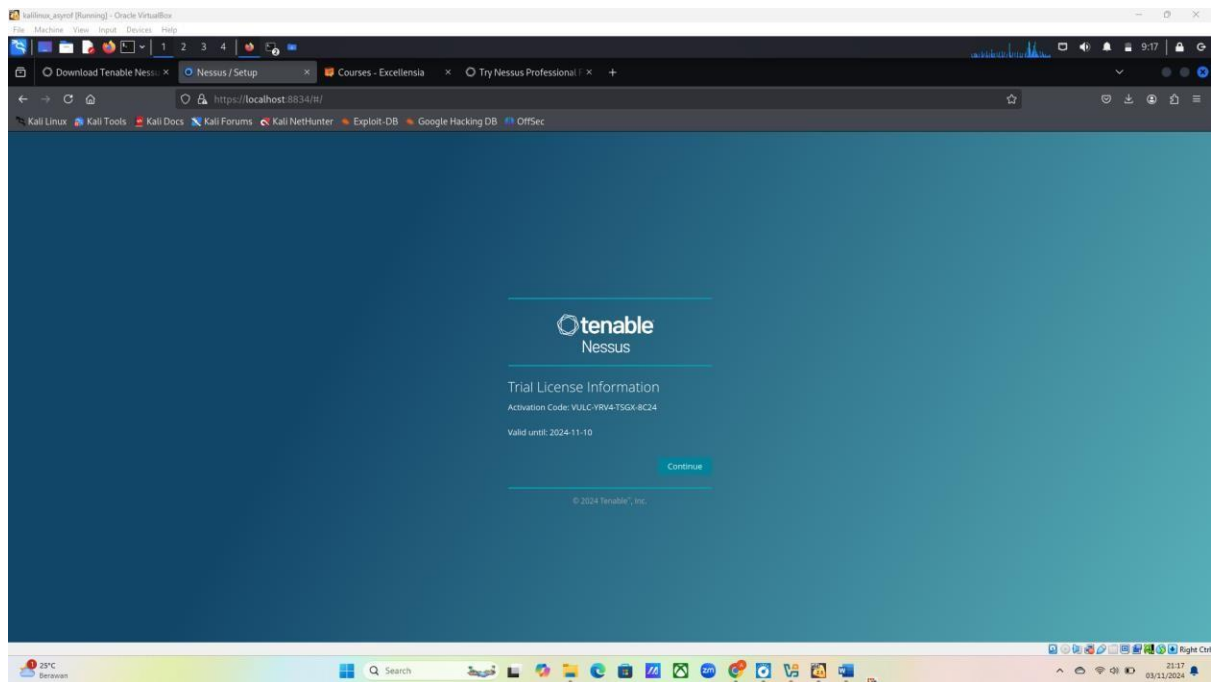
Registrasi akun nessus :



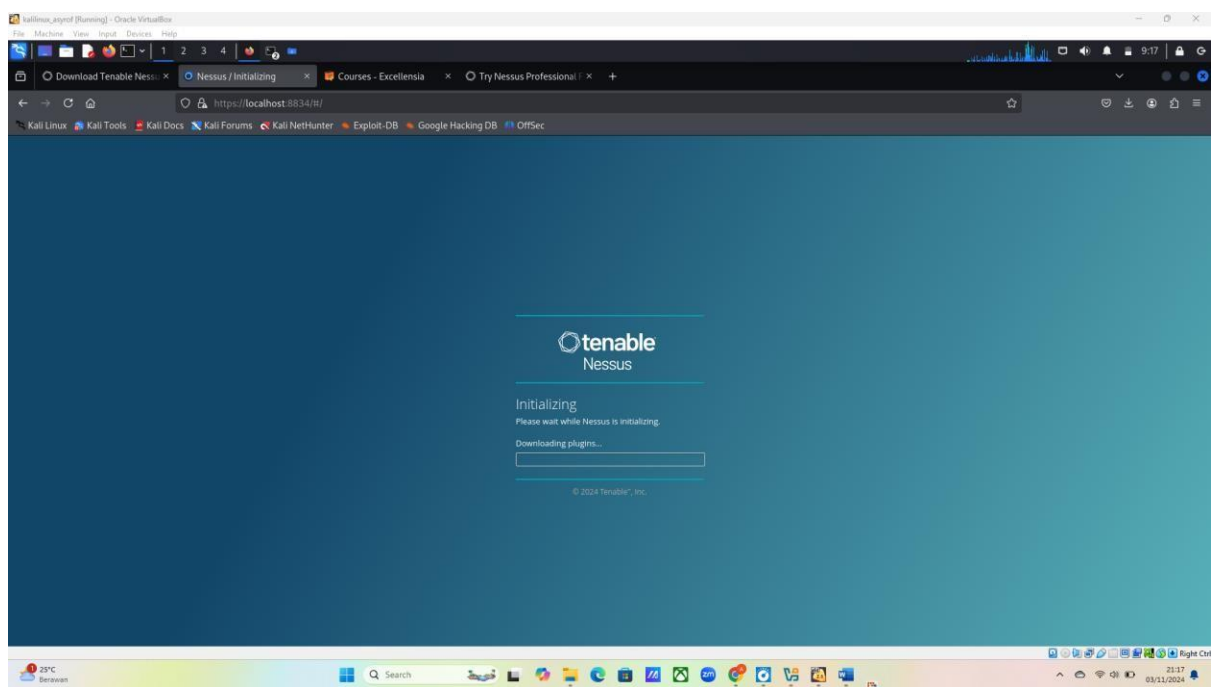
Setelah registrasi dan konfirmasi akun email yang tadi, maka akan ditampilkan serial activate trialnya kemudian start trial:



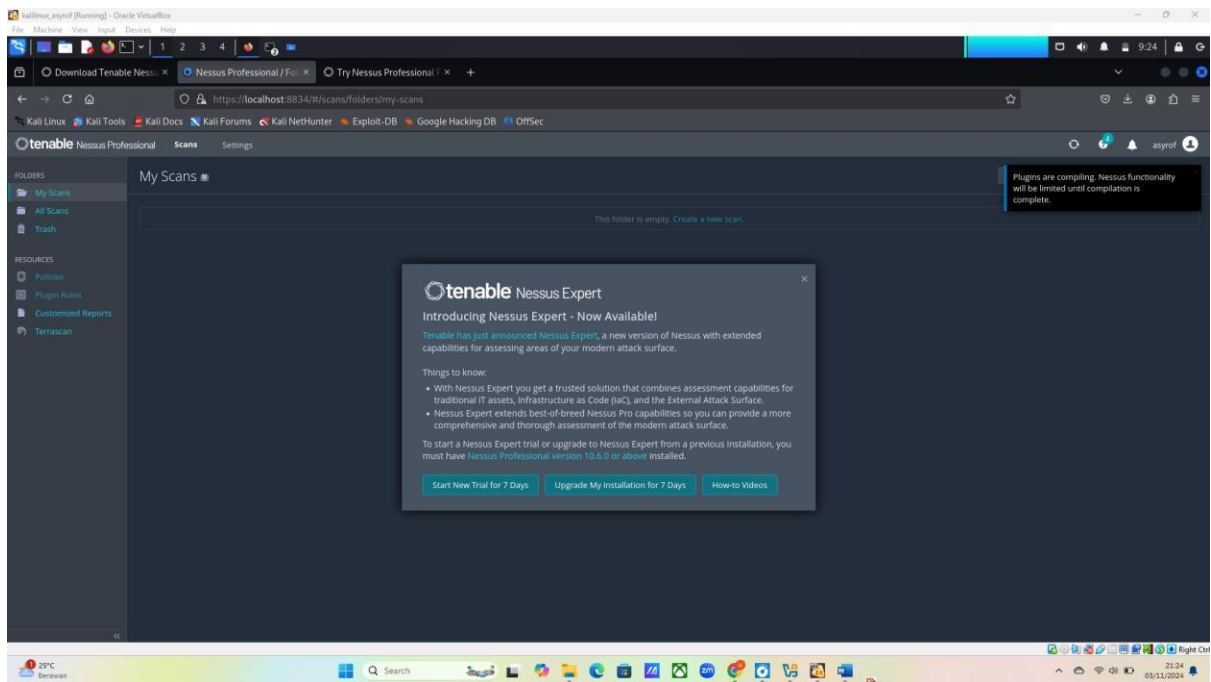
Informasi sampai kapan masa trialnya akan habis :



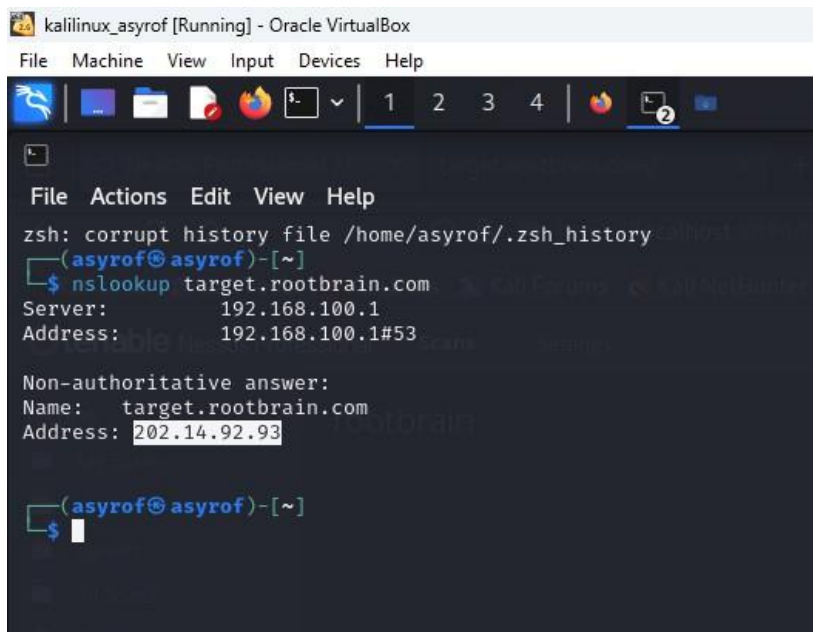
Setelah itu registrasi nama dan password,lalu menunggu instalasi plugin :



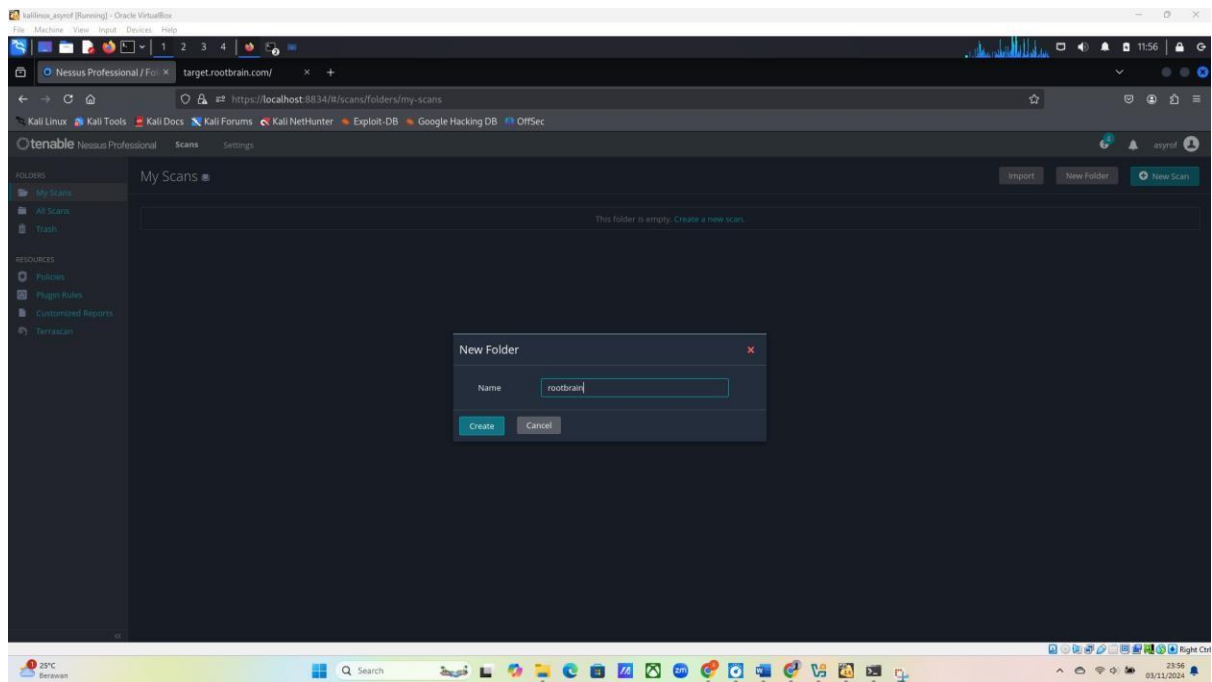
Tampilan halaman utama Nessus :



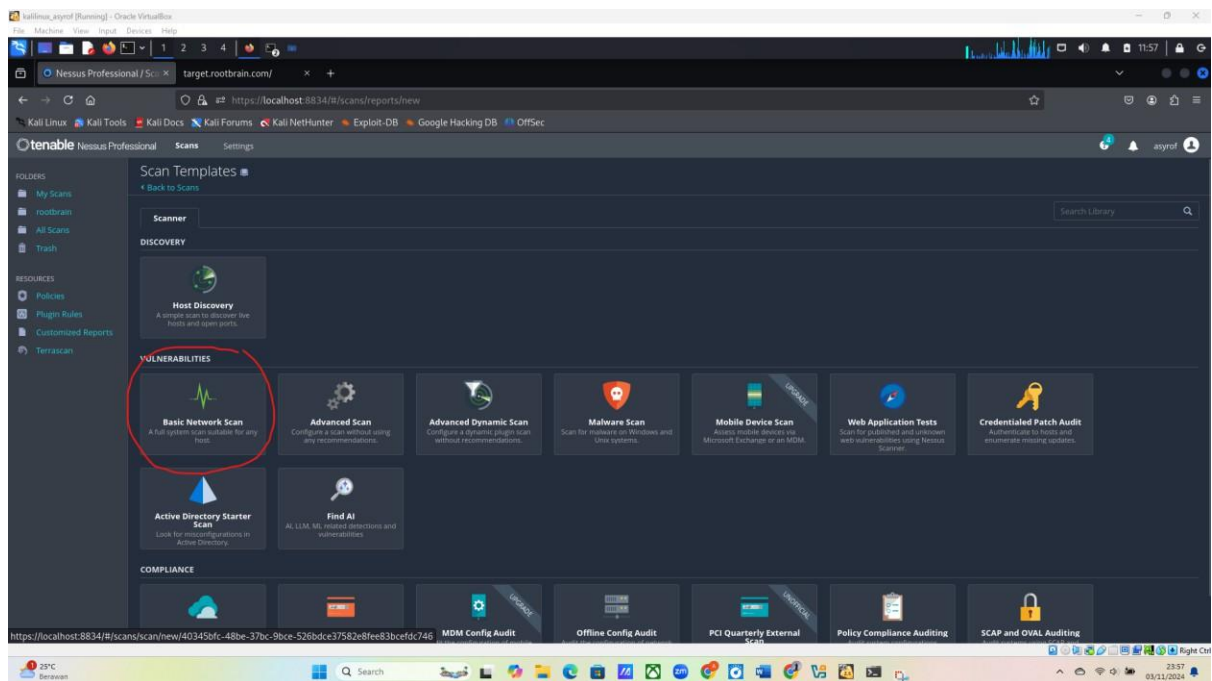
Pertama saya akan scan target.rootbrain.com,cek ip target.rootbrain.com :



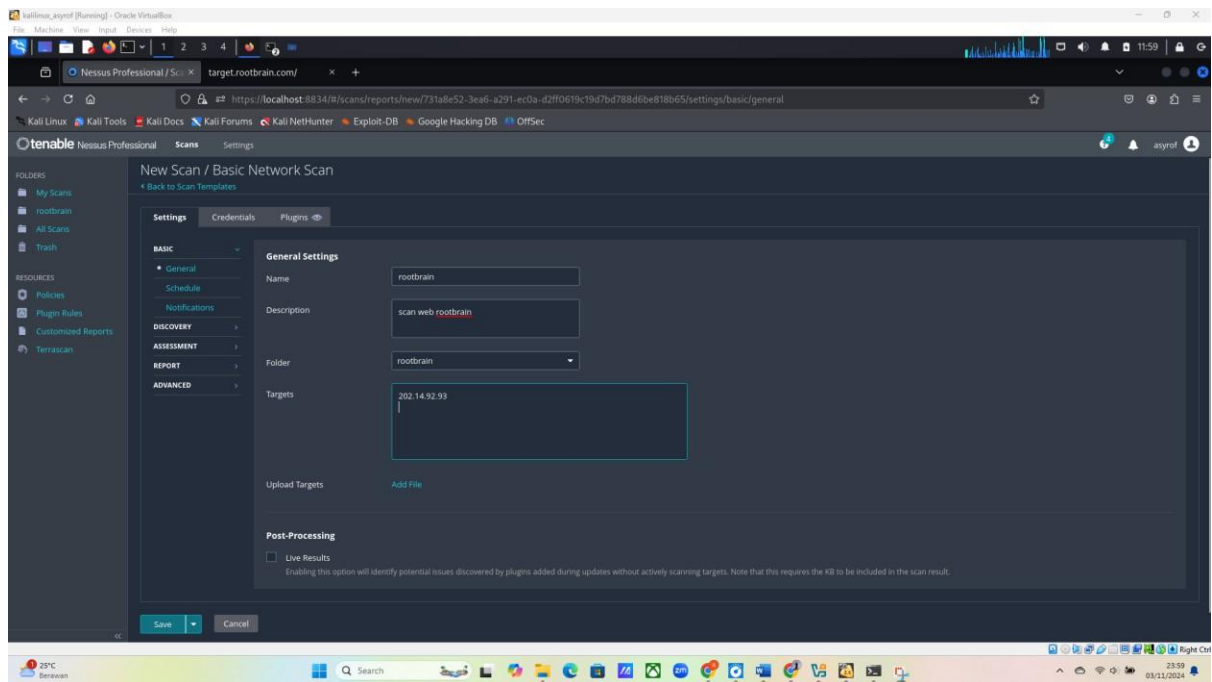
Buat folder rootbrain pada nessus :



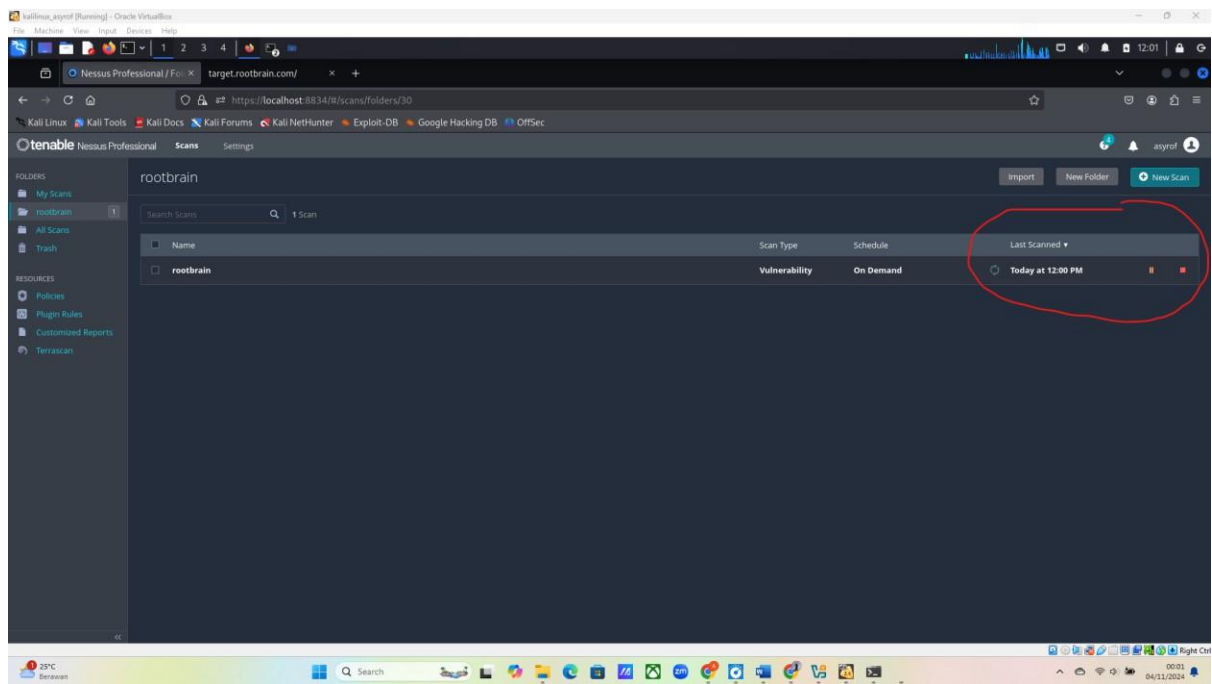
Setelah membuat folder klik create scan lalu pilih fitur scan yang dibutuhkan, saya memilih basic network scan :



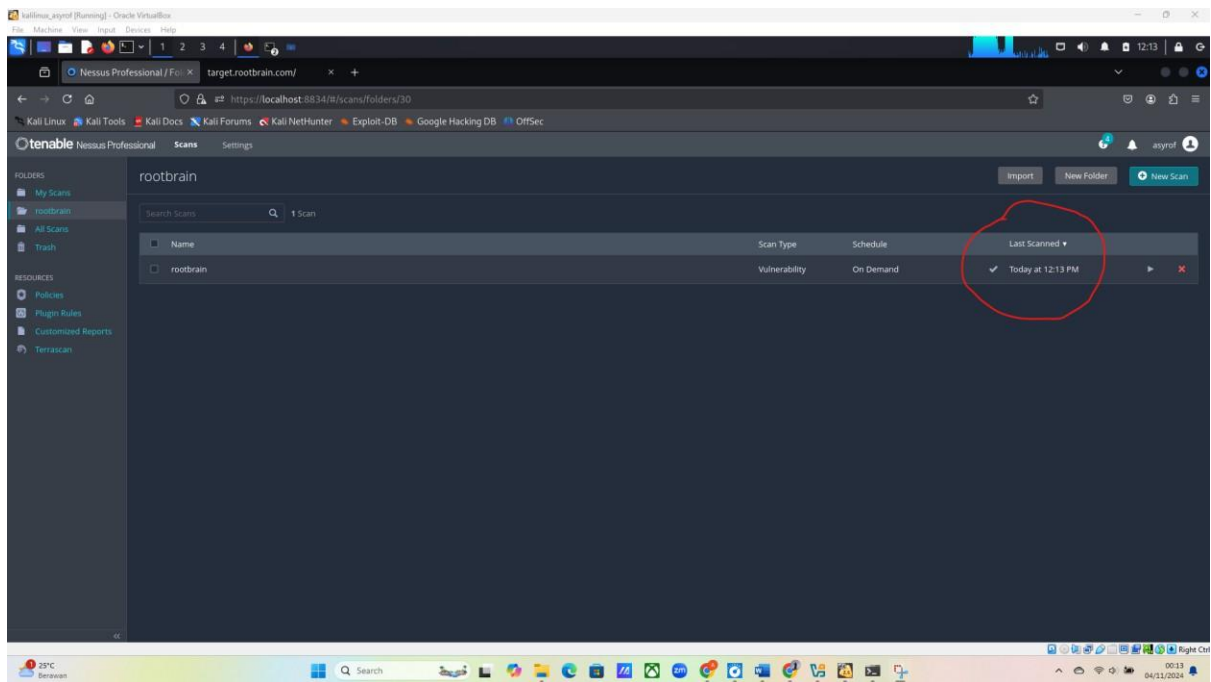
Masukkan nama,deskripsi dan Alamat ip dari web target.rootbrain.com lalu save :



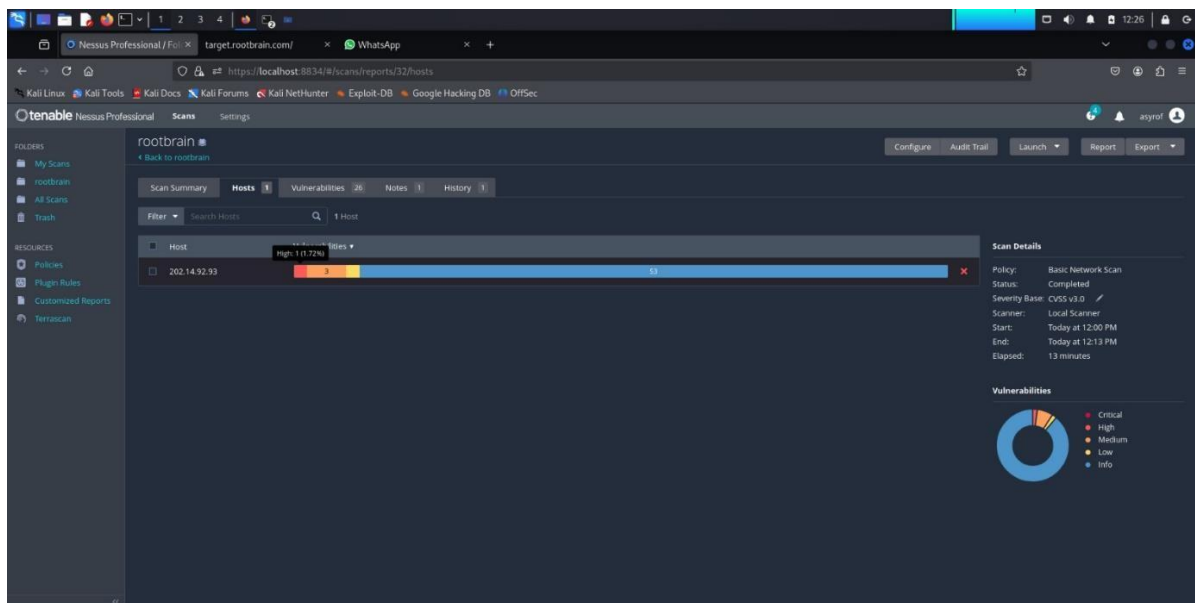
Klik folder rootbrain lalu jalankan scanning dan tunggu sampai scanning selesai :



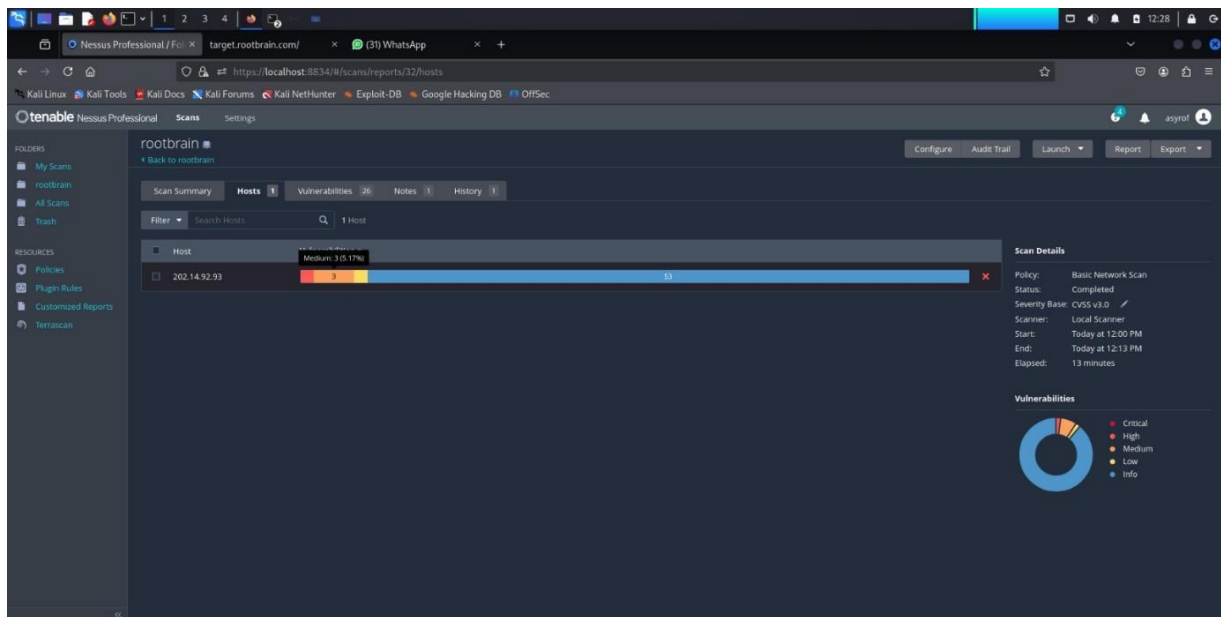
Jika scan sudah selesai akan muncul muncun logo centang :



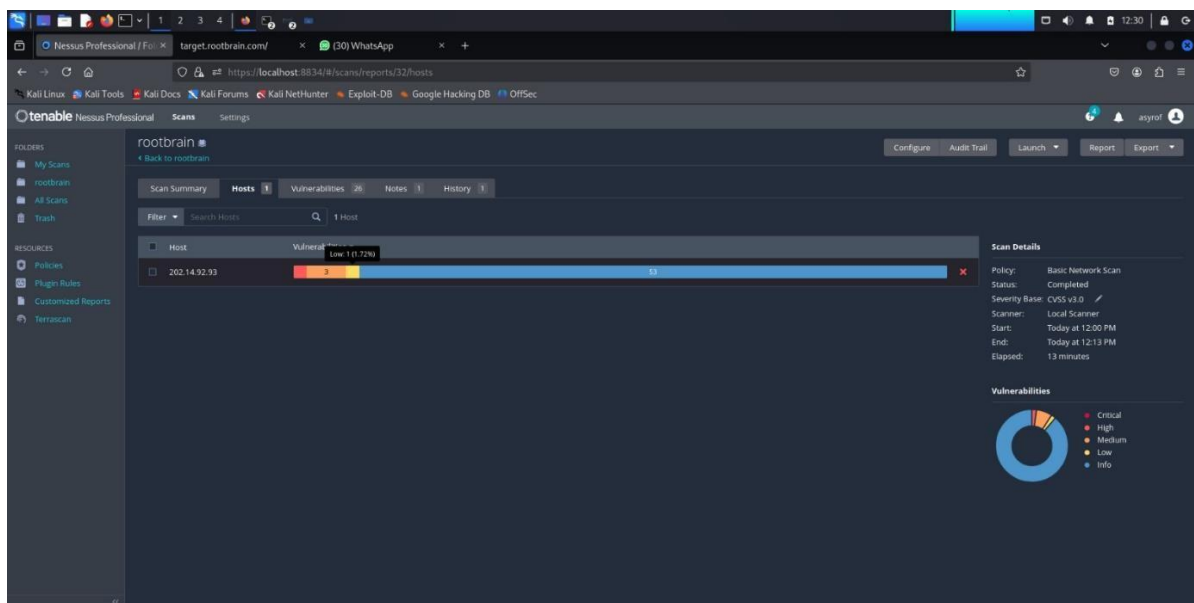
High



Medium :



Low :



Info :

The screenshot shows the Nessus Professional interface for a scan named 'rootbrain'. The 'Hosts' tab is active, displaying a table with one host: 202.14.92.93. The host has 53 vulnerabilities, with a bar chart showing the distribution of severity levels. The 'Vulnerabilities' tab is also visible, showing a bar chart of vulnerability counts by severity. The 'Scan Details' panel on the right provides information about the scan policy, status, severity base, scanner, start/end times, and elapsed time.

Host	Vulnerabilities
202.14.92.93	53

Scan Details

- Policy: Basic Network Scan
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: Today at 12:00 PM
- End: Today at 12:13 PM
- Elapsed: 13 minutes

Vulnerabilities

- Critical
- High
- Medium
- Low
- Info

Bagian vulnerabilities :

The screenshot shows the Nessus Professional interface for a scan named 'rootbrain'. The 'Vulnerabilities' tab is active, displaying a table of 26 vulnerabilities. The 'Scan Details' panel on the right provides information about the scan policy, status, severity base, scanner, start/end times, and elapsed time.

Sev	CVSS	VPR	EPSS	Name	Family	Count
MED	ISC Bind (Multiple Issues)	DNS	2
MED	SSL (Multiple Issues)	General	7
LOW	2.1*	4.2	0.8808	ICMP Timestamp Request Remote Date Disclosure	General	1
INFO	HTTP (Multiple Issues)	Web Servers	7
INFO	SSH (Multiple Issues)	General	2
INFO	SSH (Multiple Issues)	Misc.	2
INFO	SSH (Multiple Issues)	Service detection	2
INFO	TLS (Multiple Issues)	General	2
INFO	TLS (Multiple Issues)	Service detection	2
INFO	Nessus SYN scanner	Port scanners	8
INFO	Service Detection	Service detection	7
INFO	Apache HTTP Server Version	Web Servers	2

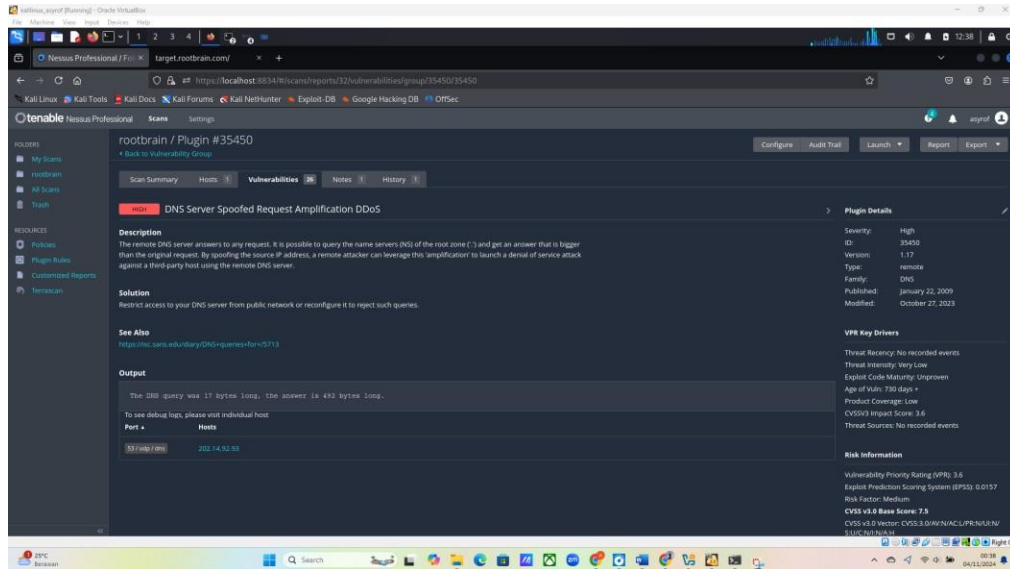
Scan Details

- Policy: Basic Network Scan
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: Today at 12:00 PM
- End: Today at 12:13 PM
- Elapsed: 13 minutes

Vulnerabilities

- Critical
- High
- Medium
- Low
- Info

➤ High (DNS Server spoofed request amplification DDoS) :

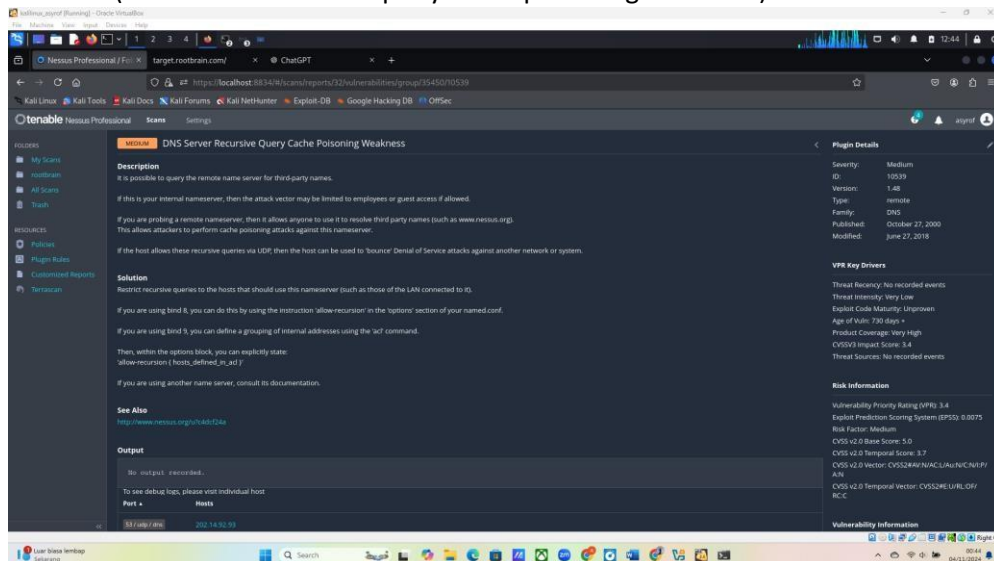


Deskripsi tersebut menjelaskan tentang potensi serangan DDoS (Denial of Service) yang memanfaatkan server DNS yang rentan. Dalam serangan ini, penyerang dapat memalsukan alamat IP mereka dan mengirimkan permintaan kecil ke server DNS. Server yang tidak terkonfigurasi dengan baik ini akan merespons dengan memberikan data yang jauh lebih besar daripada permintaan yang dikirimkan. Dengan cara ini, penyerang bisa membuat server target, yang alamat IP-nya dipalsukan, menerima banyak respons dari server DNS tersebut. Akibatnya, layanan di server target bisa menjadi tidak tersedia bagi pengguna yang sah karena dibanjiri oleh data.

Solusi :

Batasi akses ke server DNS Anda dari jaringan publik atau konfigurasi ulang untuk menolak pertanyaan tersebut.

➤ Medium (DNS server recursive query cache poisoning weakness)



Deskripsi ini menjelaskan risiko yang ada pada server DNS yang bisa mencari nama domain pihak ketiga. Jika server ini hanya diakses oleh karyawan atau tamu, risikonya terbatas. Namun, jika orang luar bisa mengaksesnya, mereka dapat menggunakan server tersebut untuk mencari nama domain lain, seperti www.nessus.org. Hal ini bisa menyebabkan serangan cache poisoning, di mana penyerang memasukkan informasi palsu ke dalam server. Selain itu, jika server mengizinkan kueri melalui UDP, penyerang bisa memanfaatkan server ini untuk melancarkan serangan Denial of Service (DoS) terhadap jaringan lain dengan mengirimkan banyak permintaan.

Solusi :

Batasi kueri rekursif ke host yang harus menggunakan nameserver ini (seperti yang ada di LAN yang terhubung dengannya).

Jika Anda menggunakan bind 8, Anda dapat melakukannya dengan menggunakan instruksi 'allow-recursion' di bagian 'options' dari `named.conf` Anda.

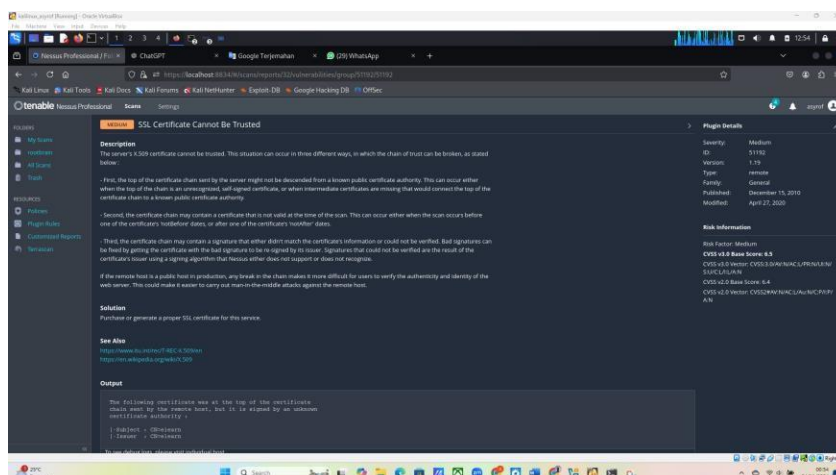
Jika Anda menggunakan bind 9, Anda dapat menentukan pengelompokan alamat internal menggunakan perintah 'acl'.

Kemudian, di dalam blok options, Anda dapat secara eksplisit menyatakan:

`'allow-recursion { hosts_defined_in_acl }'`

Jika Anda menggunakan nameserver lain, lihat dokumentasinya.

➤ Medium (SSL certificate cannot be trusted) :

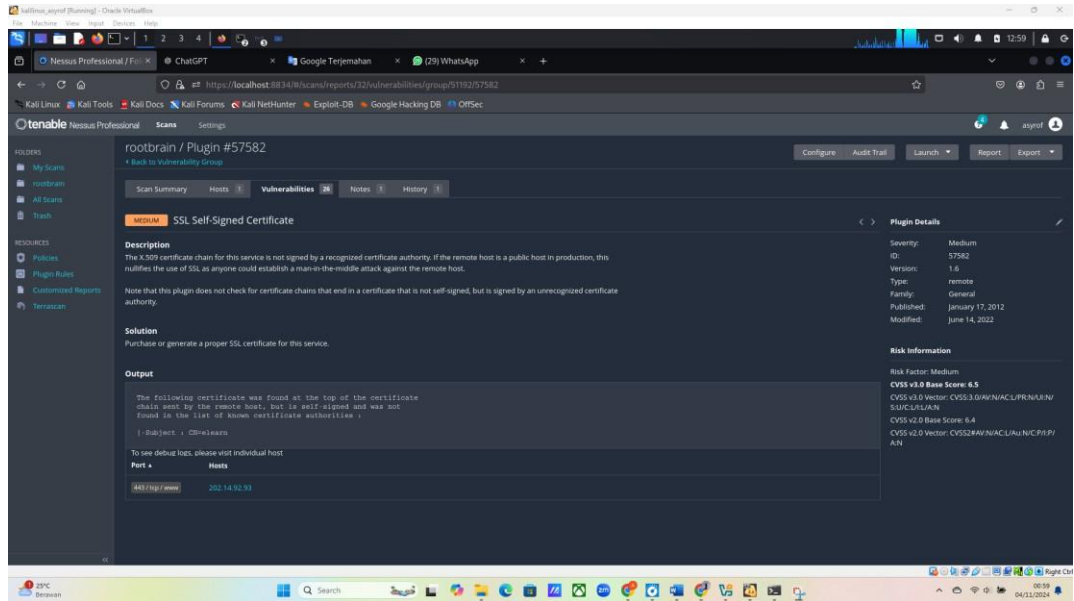


Deskripsi ini menjelaskan bahwa sertifikat X.509 server tidak dapat dipercaya karena ada tiga cara di mana rantai kepercayaannya bisa terputus. Pertama, sertifikat teratas dalam rantai mungkin tidak berasal dari otoritas sertifikat publik yang dikenal, seperti jika sertifikat tersebut adalah sertifikat yang ditandatangani sendiri atau jika ada sertifikat perantara yang hilang. Kedua, sertifikat mungkin tidak valid pada saat pemindaian, misalnya jika pemindaian dilakukan sebelum atau setelah tanggal berlaku sertifikat. Ketiga, tanda tangan pada sertifikat bisa tidak cocok atau tidak dapat diverifikasi, yang mungkin disebabkan oleh algoritma tanda tangan yang tidak didukung. Jika server ini adalah host publik, gangguan dalam rantai sertifikat dapat membuat sulit bagi pengguna untuk memverifikasi keaslian server, sehingga meningkatkan risiko serangan man-in-the-middle.

Solusi :

Beli atau buat sertifikat SSL yang tepat untuk layanan ini

➤ Medium (SSL self-signed certificate) :

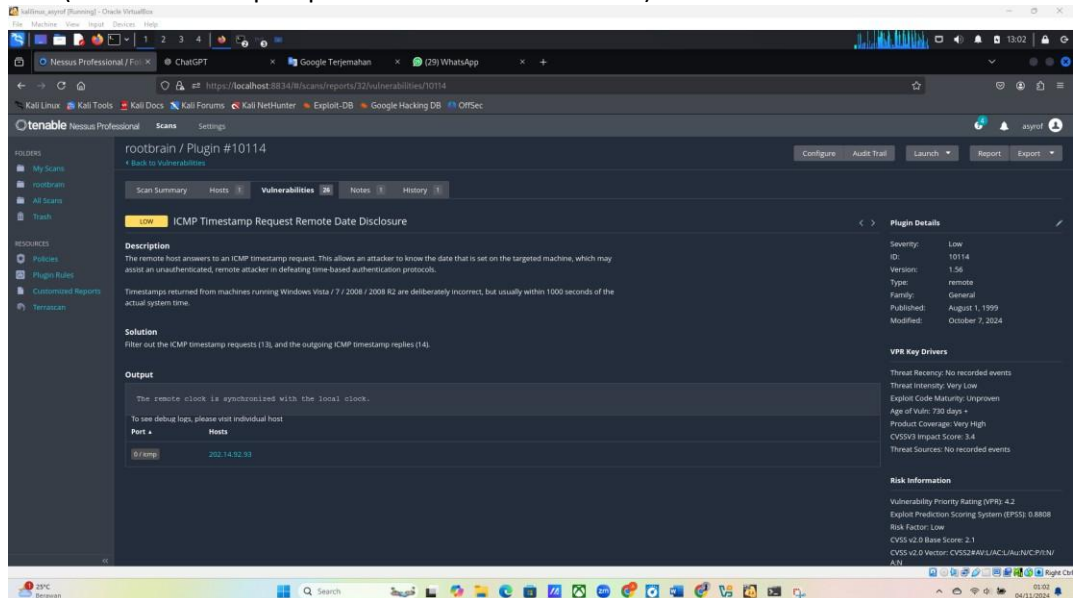


Deskripsi ini menjelaskan bahwa rantai sertifikat X.509 untuk layanan ini tidak ditandatangani oleh otoritas sertifikat yang dikenal. Jika host tersebut adalah host publik yang sedang digunakan, hal ini membuat penggunaan SSL tidak berarti, karena siapa pun bisa melakukan serangan man-in-the-middle terhadap host tersebut. Selain itu, perlu dicatat bahwa plugin ini tidak memeriksa rantai sertifikat yang diakhiri dengan sertifikat yang tidak ditandatangani sendiri tetapi ditandatangani oleh otoritas sertifikat yang tidak dikenal.

Solusi :

Beli atau buat sertifikat SSL yang tepat untuk layanan ini.

➤ Low (ICMP timestamp request remote date disclosure) :



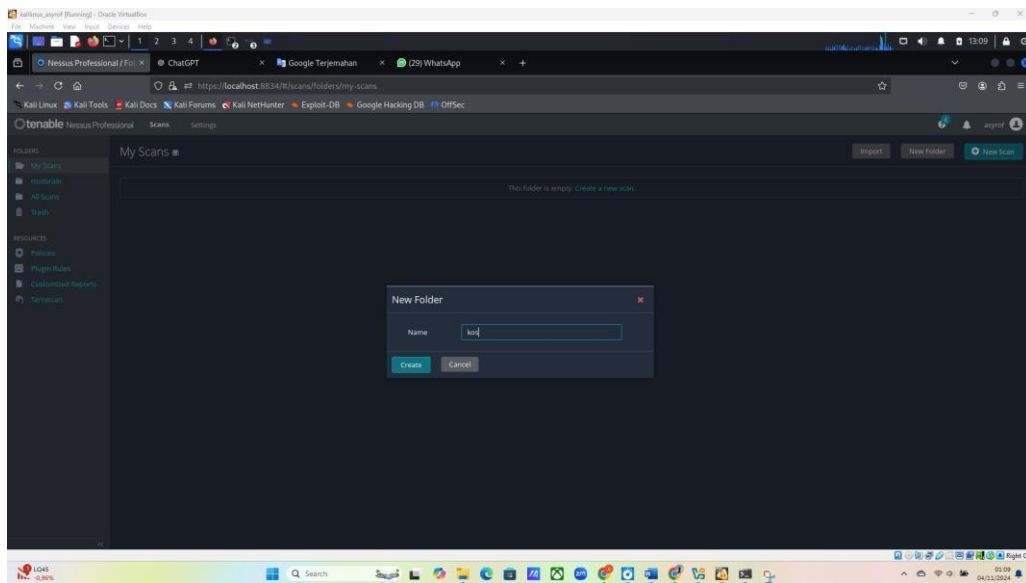
Deskripsi ini menjelaskan bahwa host jarak jauh merespons permintaan timestamp ICMP. Ini memungkinkan penyerang untuk mengetahui tanggal yang diatur pada mesin yang menjadi target, yang dapat membantu penyerang yang tidak terautentikasi untuk mengatasi protokol otentikasi berbasis waktu. Pada mesin yang menjalankan Windows Vista, 7, 2008, dan 2008 R2, timestamp yang dikembalikan biasanya sengaja tidak akurat, tetapi masih dalam rentang 1000 detik dari waktu sistem yang sebenarnya.

Solusi :

Filter permintaan stempel waktu ICMP (13), dan balasan stempel waktu ICMP yang keluar (14).

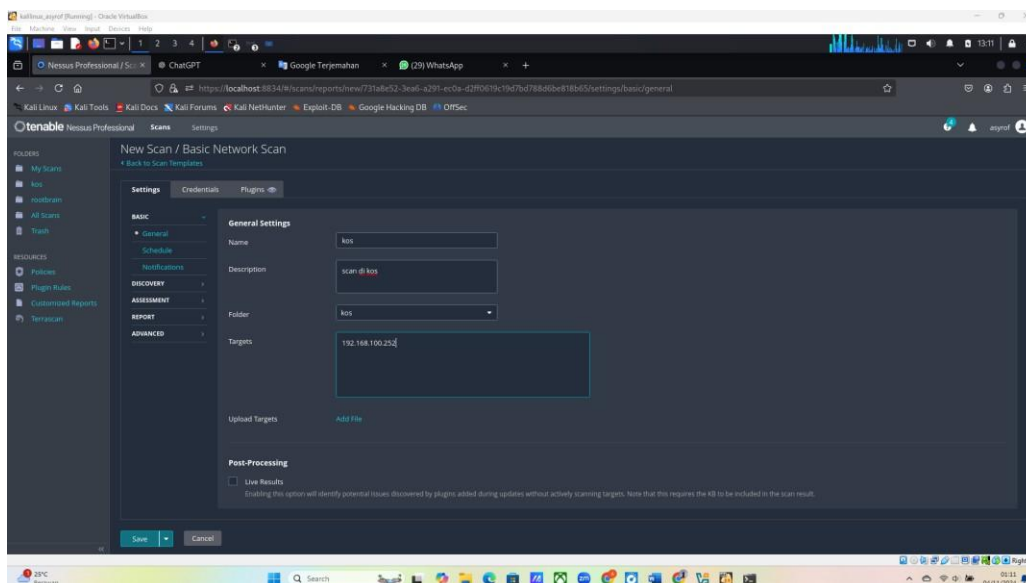
Buat yang sama untuk scan rumah :

Buat folder

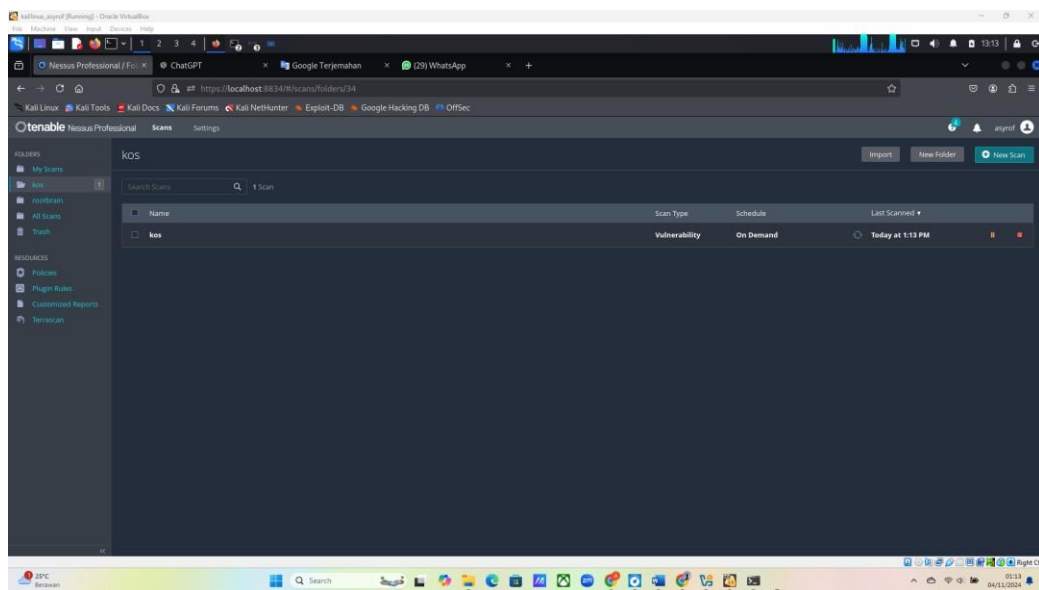


Kemudian create new scan lalu masukkan nama,deskripsi,dan ip kos lalu save :

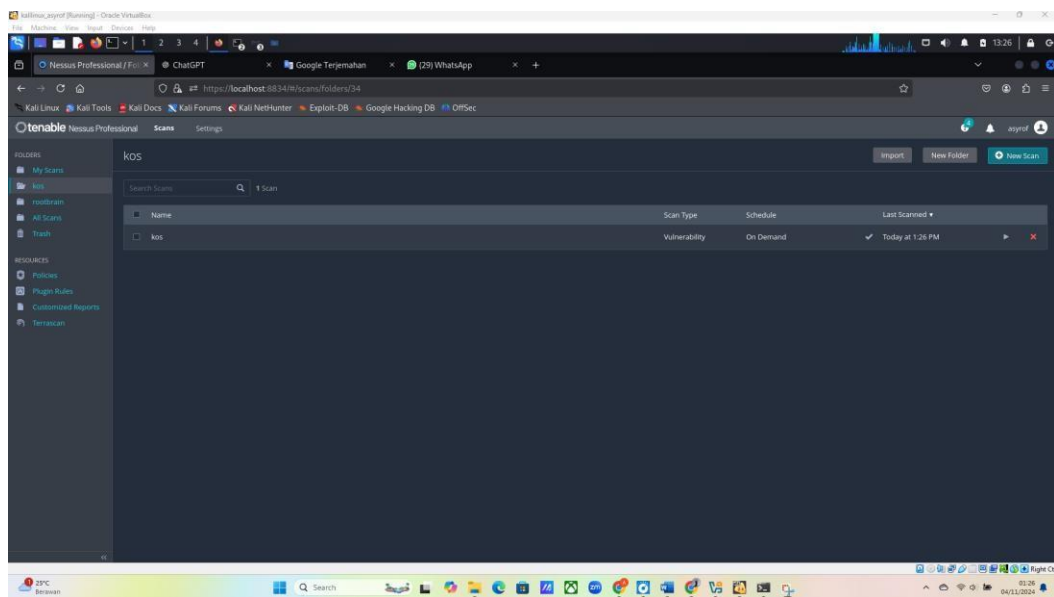
```
Connection-specific DNS Suffix . :  
Link-local IPv6 Address . . . . . : fe80::ce08:ec72:98ee:d2e1%18  
IPv4 Address. . . . . : 192.168.100.252  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . : 192.168.100.1
```



Klik tanda running scan dan tunggu hingga proses scan selesai :



Proses scan sudah selesai :



Tidak ada vulnerability yang critical/high :

