



Nessus®
vulnerability scanner

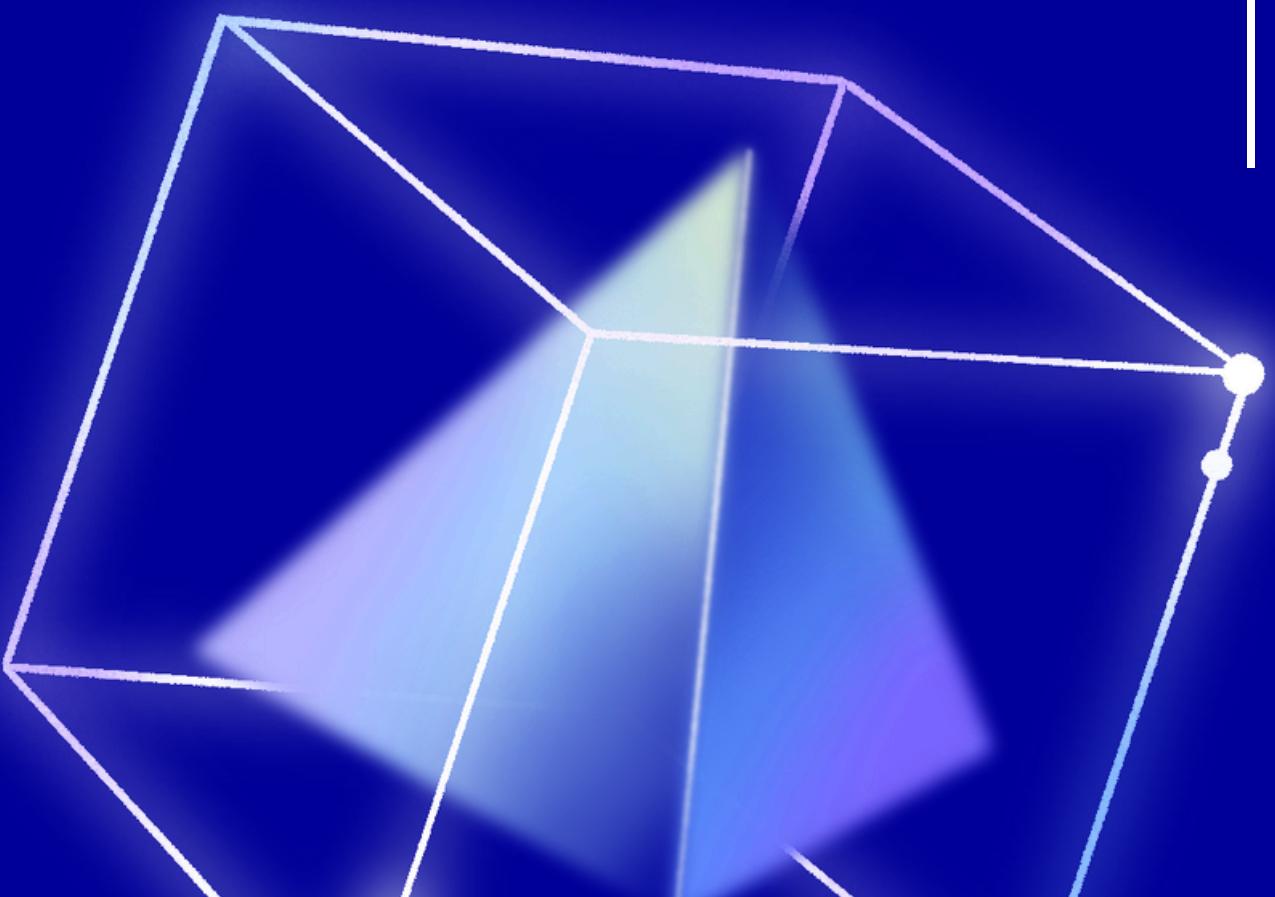
Nessus (Vulnerability Scanner)

Pemateri Tokupens



DAFTAR ISI

• Pengenalan	01
• Nessus Kompatibel dgn	02
• Persiapan Instalasi	03
• Kelebihan Dan Fitur	04
• Persiapan Scanning	05
• Membuat Laporan	06



PENGENALAN

nessus adalah alat tangguh dari Tenable yang dapat memindai kerentanan dalam jaringan, sistem operasi, database, dan aplikasi.

nessus memberikan laporan rinci tentang kelemahan keamanan dan memprioritaskan keparahannya.

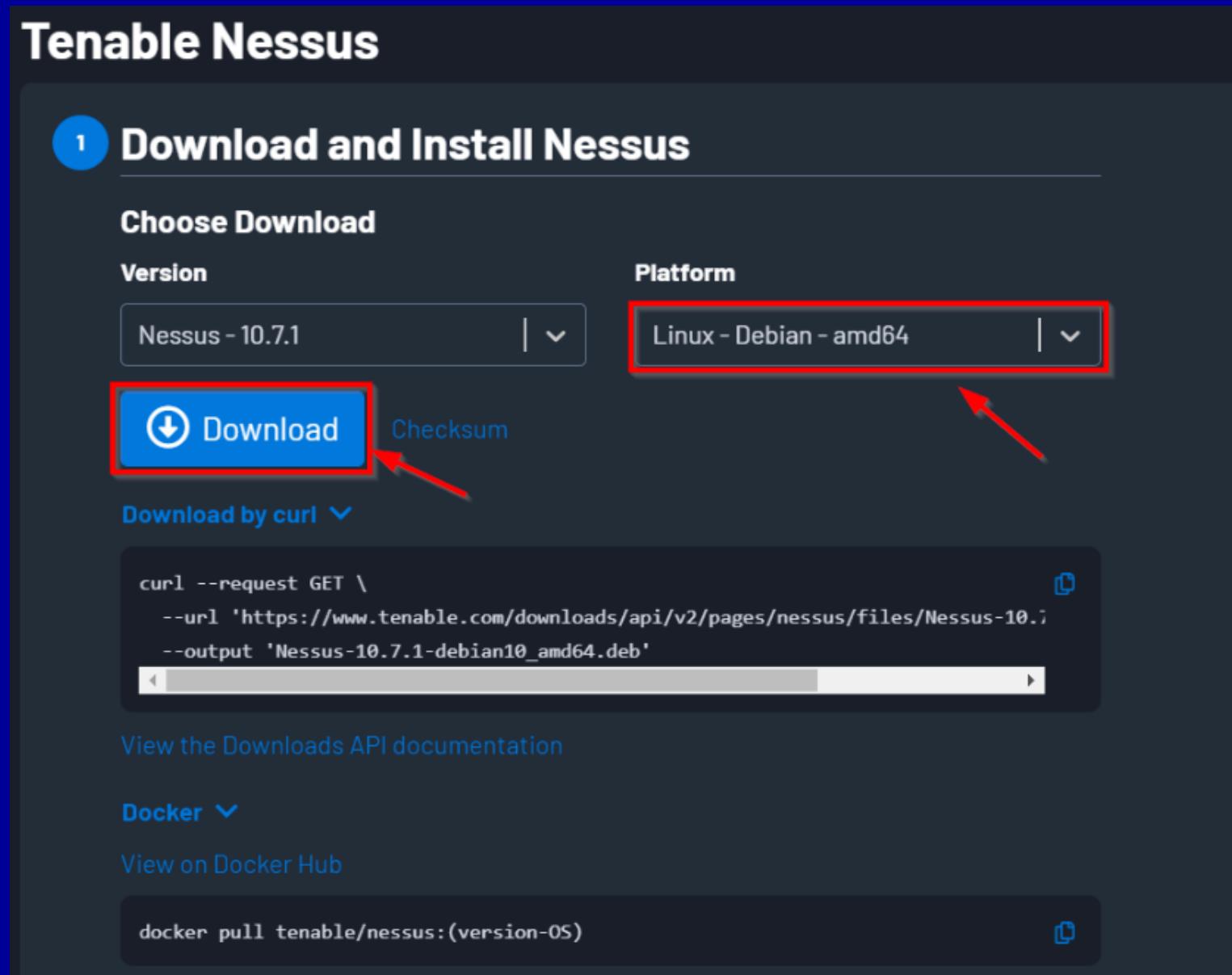
nessus memindai dan mencari kesalahan konfigurasi, patch yang hilang, dan CVE (Kerentanan dan Eksposur Umum) dan sering digunakan dalam penilaian keamanan dan pengujian penetrasi.

Nessus Kompatibel Dengan:

- *Amazon Linux 2*
- Debian
- Fedora
- FreeBSD
- MacOS
- Red Hat
- SUSE
- Windows dan
Windows Server



PERSIAPAN INSTALASI



Tahap pertama Anda mengunduh, menginstal, dan memulai Nessus Essentials di Kali Linux. Nessus tidak diinstal sebelumnya dengan Kali dan perlu diunduh dari situs web Nessus.

PERSIAPAN INSTALASI

unduh Nessus, kunjungi halaman unduh dan pilih file Linux-Debian-amd64.

Kemudian, pilih “Download” untuk mendownload file ke Kali. Alternatifnya, Anda dapat menggunakan curl untuk mengunduh file atau mengunduh dan menginstal Nessus sebagai image Docker.

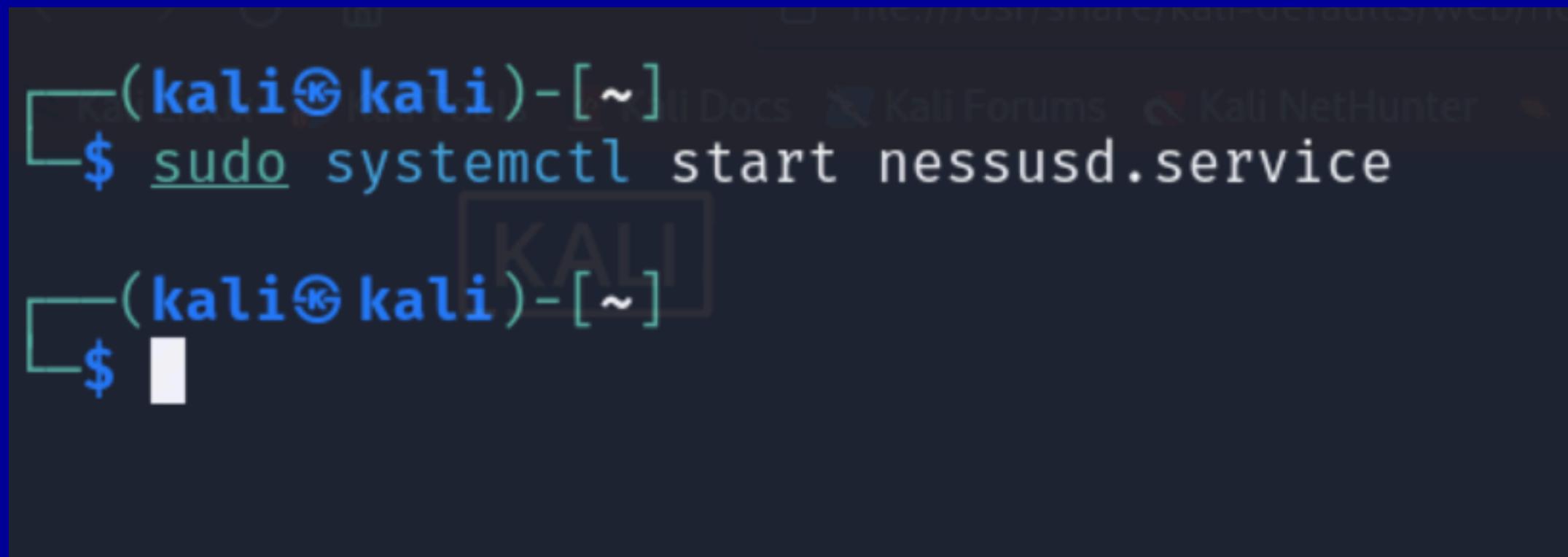
PERSIAPAN INSTALASI

```
└──(kali㉿kali)-[~/Downloads]
└─$ sudo dpkg -i Nessus-10.7.1-debian10_amd64.deb
[sudo] password for kali:
Selecting previously unselected package nessus.
(Reading database ... 406202 files and directories current
Preparing to unpack Nessus-10.7.1-debian10_amd64.deb ...
Unpacking nessus (10.7.1) ...
Setting up nessus (10.7.1) ...
HMAC : (Module_Integrity) : Pass
SHA1 : (KAT_Digest) : Pass
SHA2 : (KAT_Digest) : Pass
SHA3 : (KAT_Digest) : Pass
TDES : (KAT_Cipher) : Pass
```

Untuk menginstal Nessus, cukup masukkan perintah berikut di terminal, pastikan Anda berada di folder yang sama dengan file yang diunduh.

`sudo dpkg -i Nessus.deb`

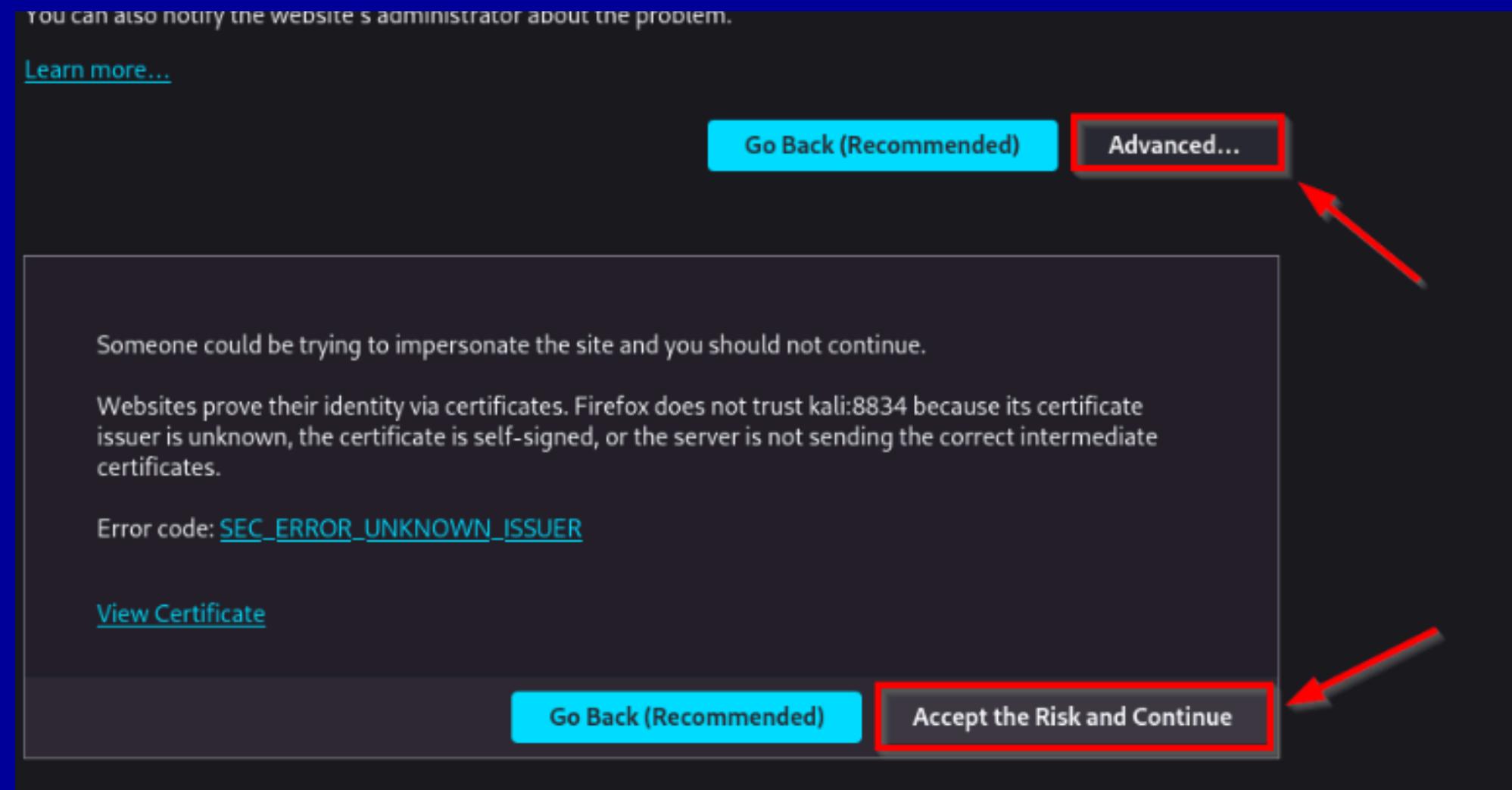
PERSIAPAN INSTALASI



```
(kali㉿kali)-[ ~ ]$ sudo systemctl start nessusd.service
(kali㉿kali)-[ ~ ]$ █
```

Untuk mulai menginstal plugin yang diperlukan sebelum Anda dapat menggunakan Nessus, masukkan sudo systemctl start nessusd.service di baris perintah.

PERSIAPAN INSTALASI



memulai dengan buka <https://kali:8834/> di browser web
Anda untuk mengakses dan mengkonfigurasi Nessus.

Saat Anda mencoba mengakses URL, Anda akan melihat
pesan peringatan. Klik “Lanjutan...” dan pilih “Terima
Resiko dan Lanjutkan.”

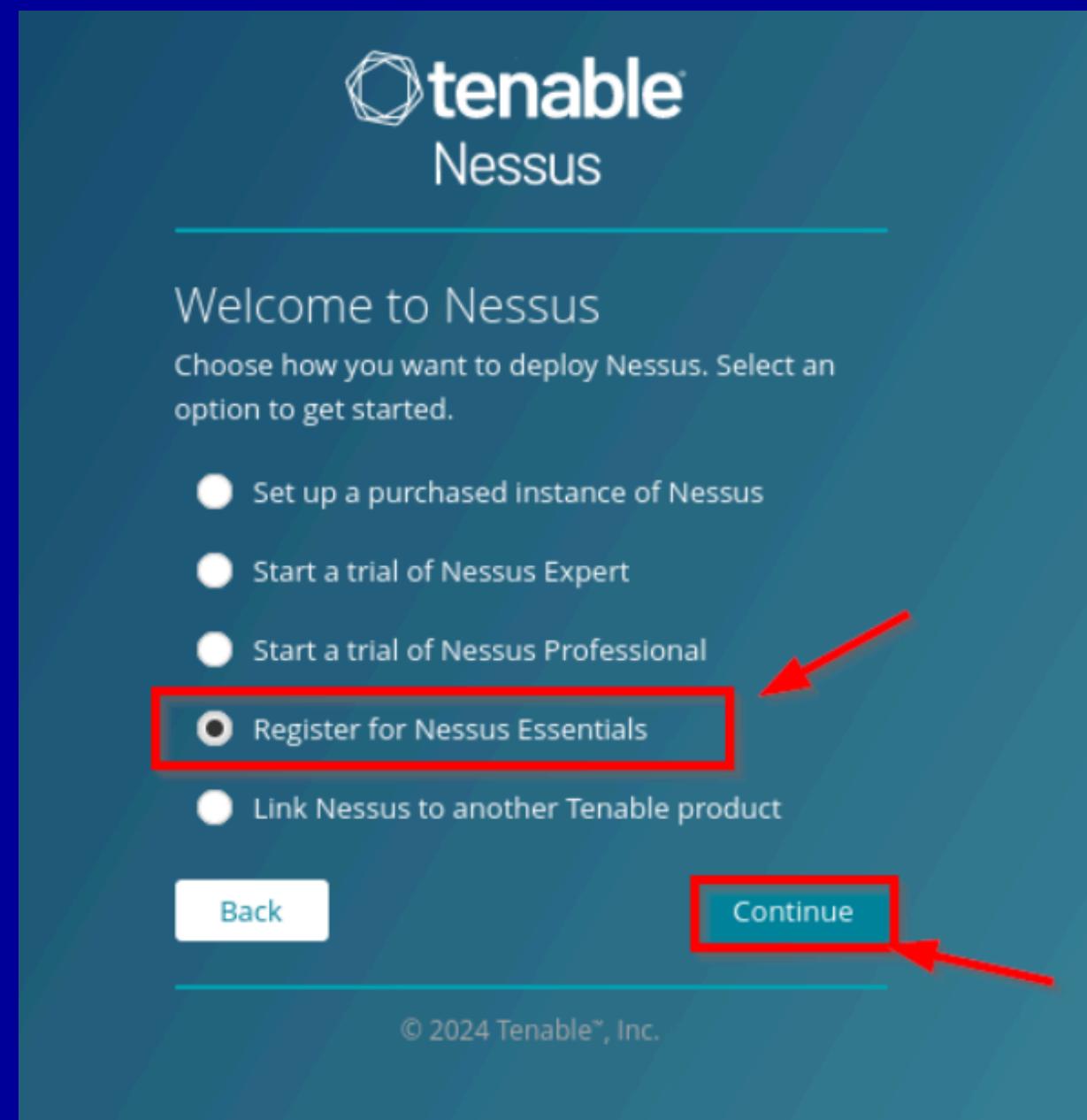
Tahap 6

PERSIAPAN INSTALASI



lanjut ada tampilan selamat datang Nessus.
Klik "Lanjutkan" untuk melanjutkan.

PERSIAPAN INSTALASI



Layar berikutnya pilih register for Nessus Essentials.

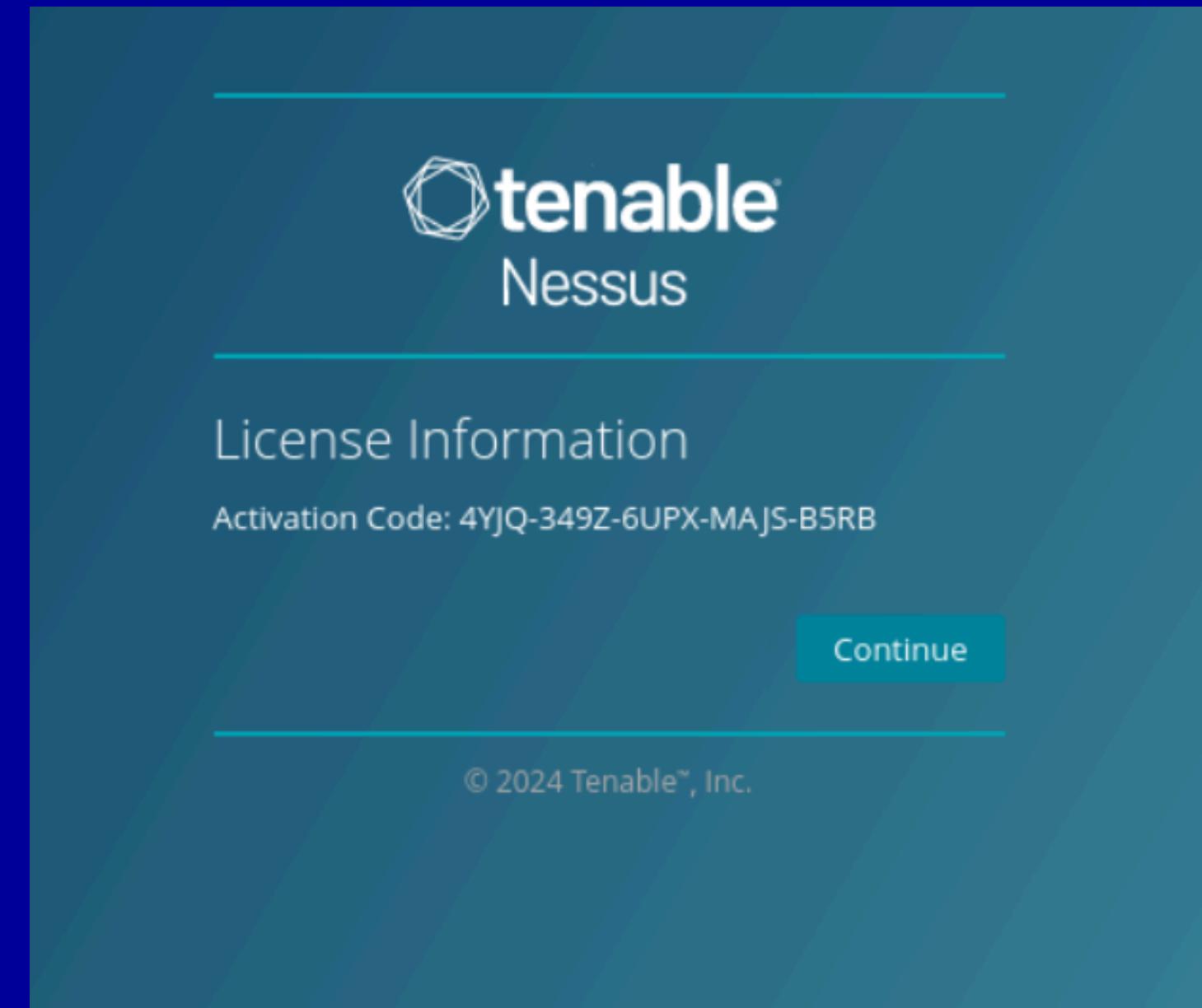
PERSIAPAN INSTALASI



Berikan nama dan alamat email lalu klik “Register”.

Tahap 8

PERSIAPAN INSTALASI



selanjutnya ada diberikan kode aktivasi. Salin dan simpan kode ini di suatu tempat untuk referensi di masa mendatang. Klik “Continue”.

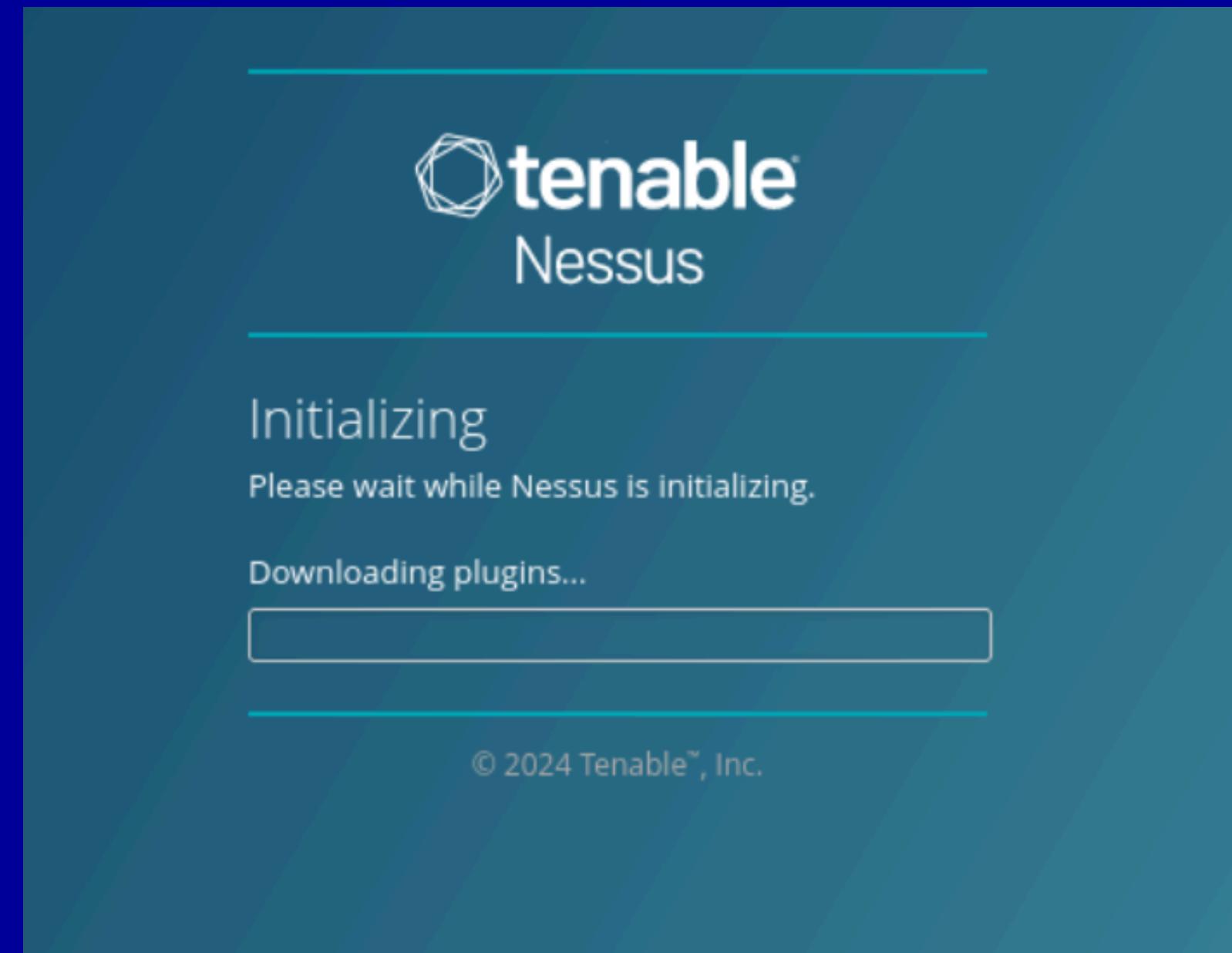
PERSIAPAN INSTALASI



Anda harus membuat akun pengguna administrator Nessus, yang akan digunakan untuk login ke Nessus.

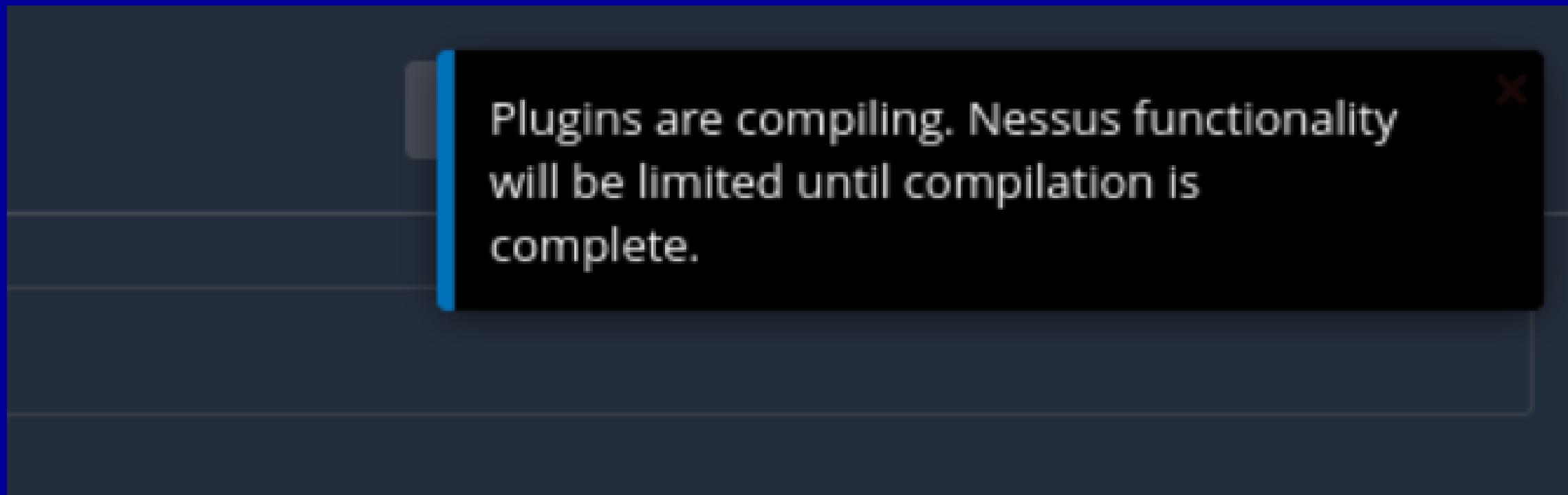
Tahap 10

PERSIAPAN INSTALASI



Sekarang Nessus akan mulai mengunduh Plugin

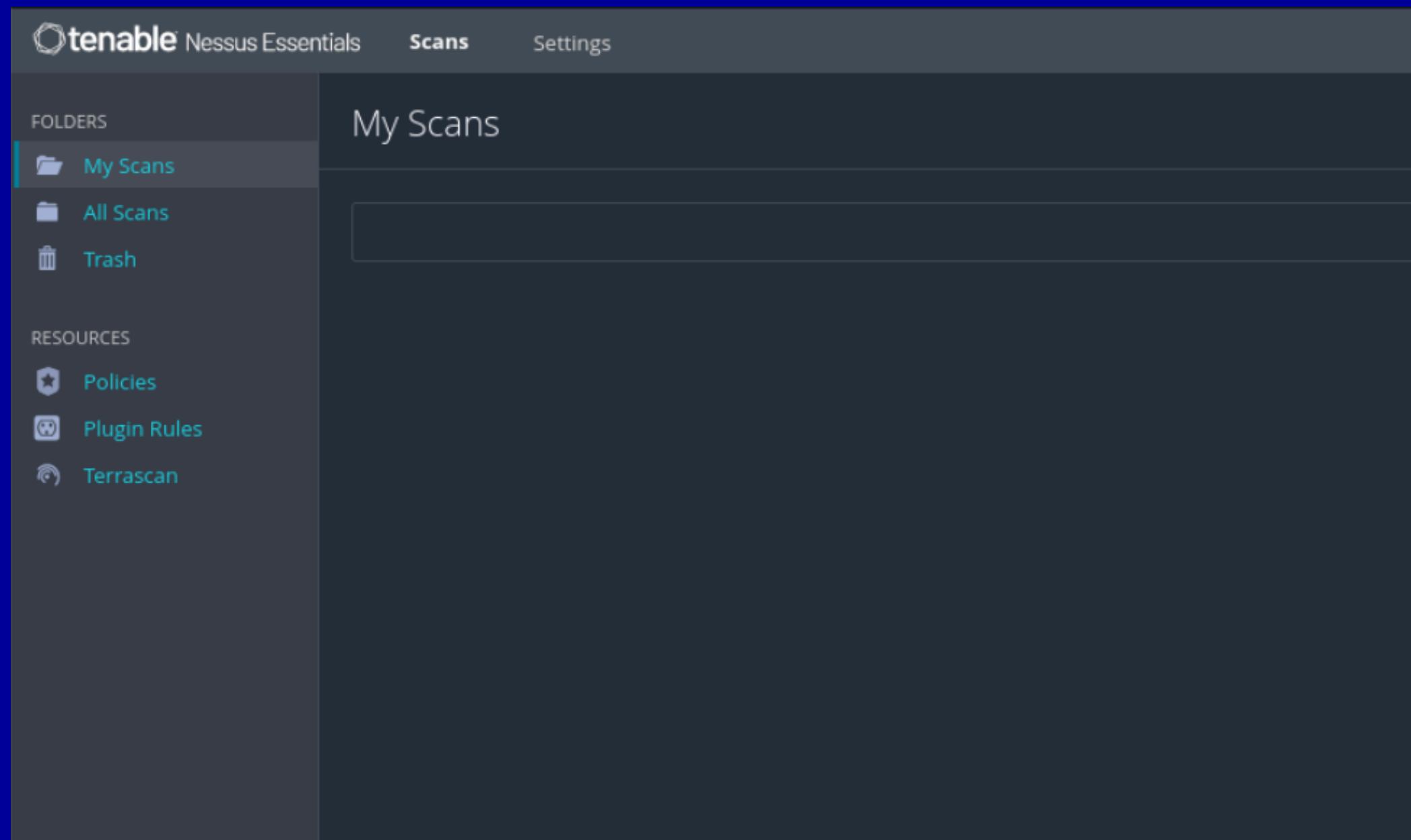
PERSIAPAN INSTALASI



selesai, Anda akan masuk ke dashboard Nessus. Dari sini, Nessus akan mulai mengonfigurasi plugin, yang memerlukan waktu beberapa saat untuk diselesaikan.

Tahap 12

PERSIAPAN INSTALASI



Anda sudah masuk, Anda dapat mulai menggunakan Nessus.

KELEBIHAN DAN FITUR NESSUS



Nessus dilengkapi dengan database kerentanan yang luas yang terus diperbarui.



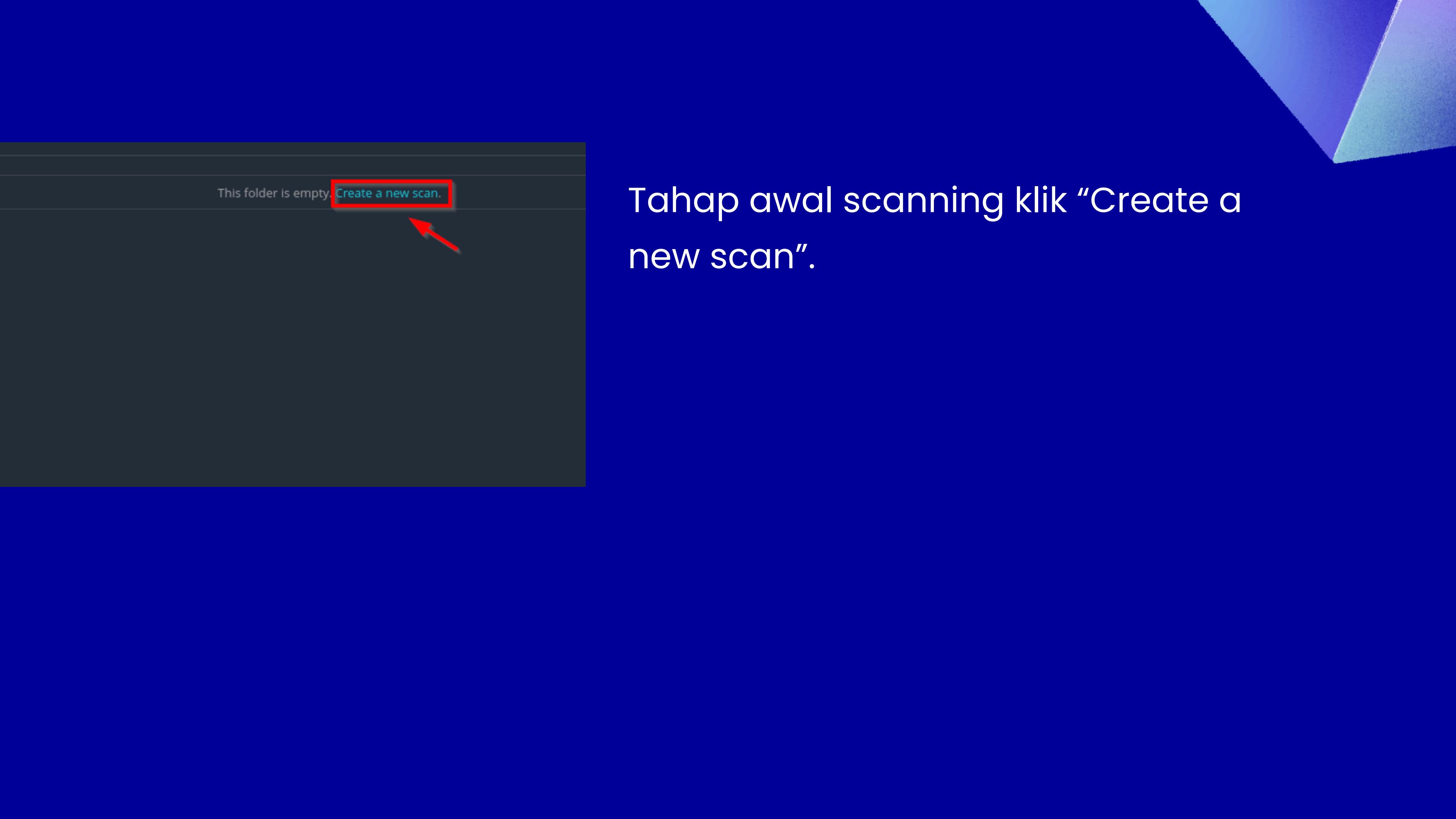
Nessus dirancang untuk melakukan pemindaian dengan cepat. sehingga sangat membantu administaror sistem.



Laporan Nessus cukup detail tentang kerentanan yang ditemukan, rekomendasi perbaikan, dan penilaian risiko.



Nessus menawarkan fleksibilitas dalam konfigurasi pemindaian. .

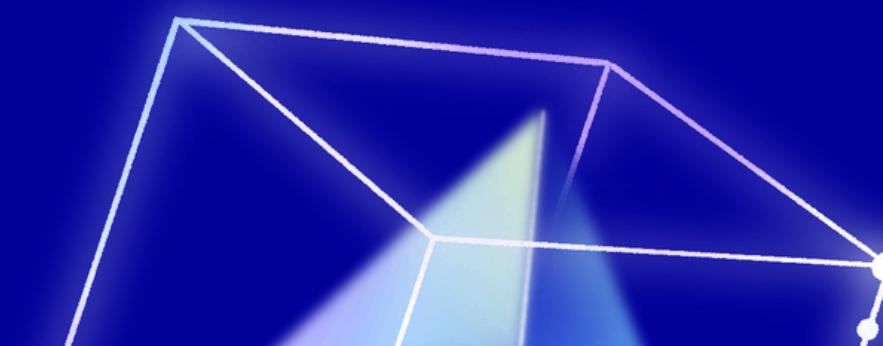


This folder is empty. [Create a new scan.](#)

Tahap awal scanning klik “Create a new scan”.



PERSIAPAN SCANNING DENGAN NESSUS



Scanner

DISCOVERY

Host Discovery
A simple scan to discover live hosts and open ports.

VULNERABILITIES

Basic Network Scan
A full system scan suitable for any host.

Advanced Scan
Configure a scan without using any recommendations.

Advanced Dynamic Scan
Configure a dynamic plugin scan without recommendations.

Malware Scan
Scan for malware on Windows and Unix systems.

Mobile Device Scan
Assess mobile devices via Microsoft Exchange or an MDM.

Web Application Test
Scan for published and unknown web vulnerabilities using Nmap Scanner.

Spectre and Meltdown
Remote and local checks for CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754

WannaCry Ransomware
Remote and local checks for MS17-010.

Ripple20 Remote Scan
A remote scan to fingerprint hosts potentially running the Treck stack in the network.

Zerologon Remote Scan
A remote scan to detect Microsoft Netlogon Elevation of Privilege (Zerologon).

Solarigate
Remote and local checks to detect SolarWinds Solarigate vulnerabilities.

ProxyLogon : MS Exchange
Remote and local checks to detect Exchange vulnerabilities targeted by HAFNIUM.

Log4Shell
Detection of Apache Log4j CVE-2021-44228

Log4Shell Remote Checks
Detection of Apache Log4j CVE-2021-44228 via Remote Direct Checks

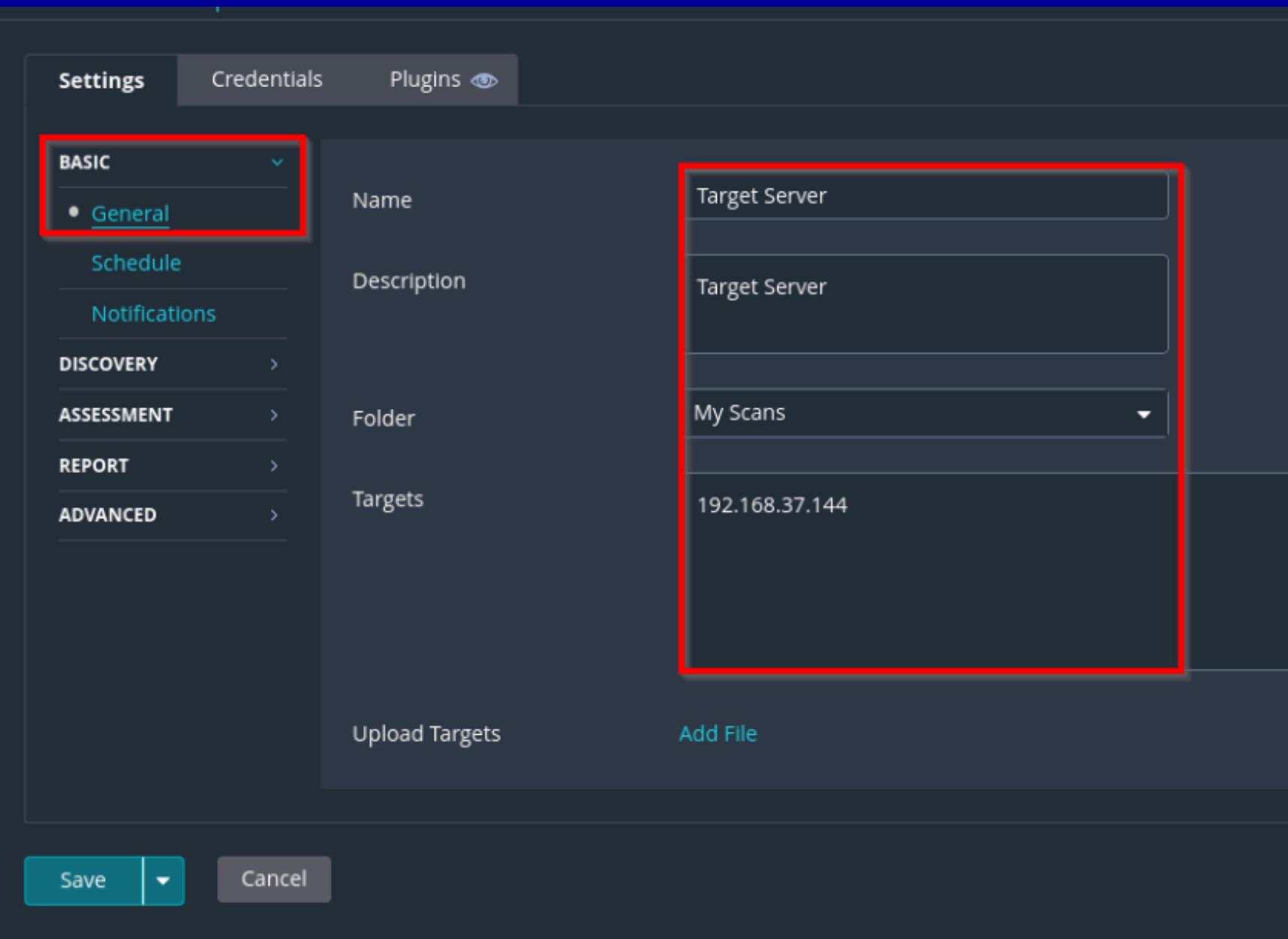
Log4Shell Vulnerability Ecosystem
Detection of Log4Shell Vulnerabilities

CISA Alerts AA22-011A and AA22-047A
Detection of vulnerabilities from recent CISA alerts.

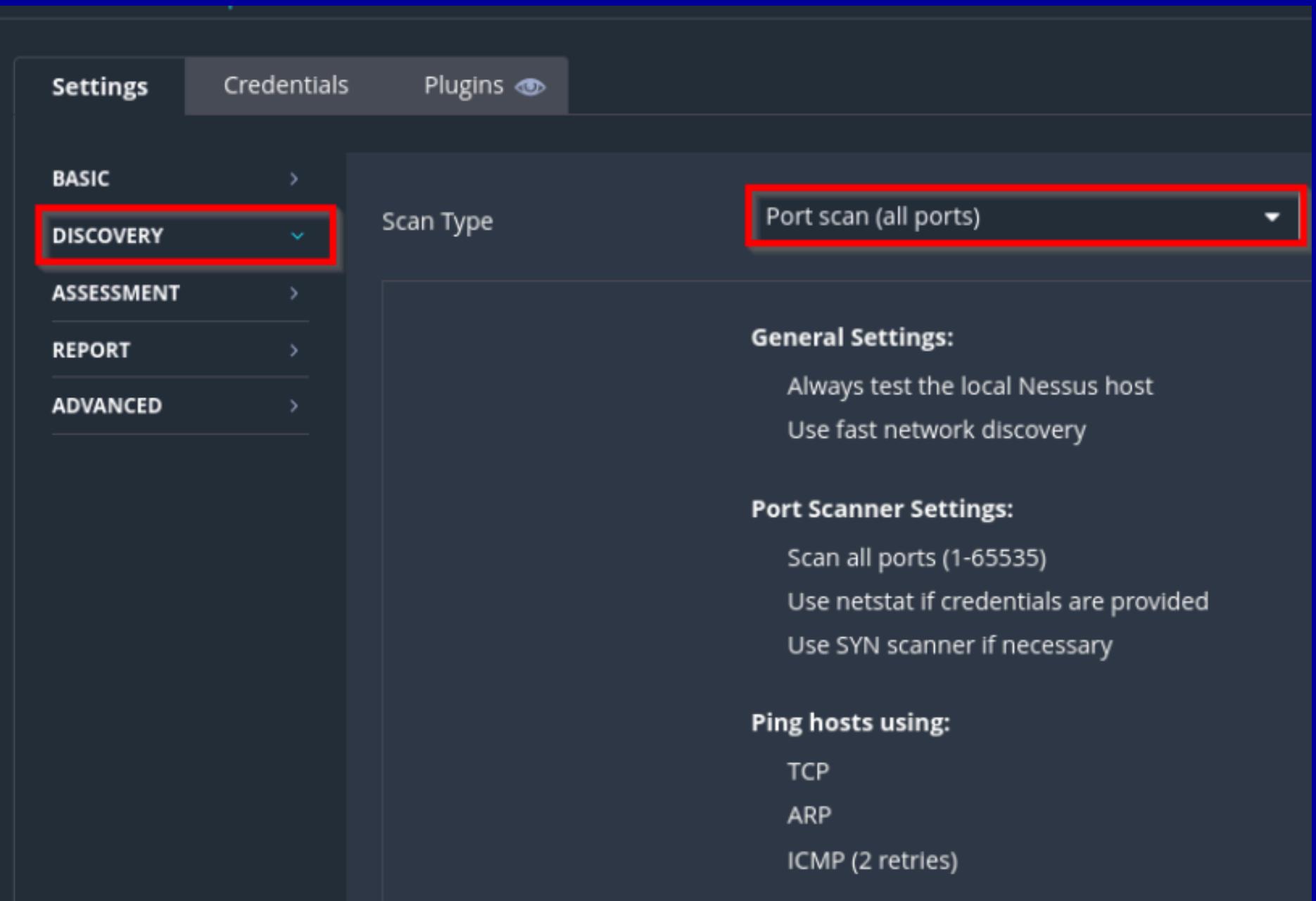
ContiLeaks
Detection of vulnerabilities revealed in the ContiLeaks chats.

Ransomware Ecosystem
Vulnerabilities used by ransomware groups and affiliates

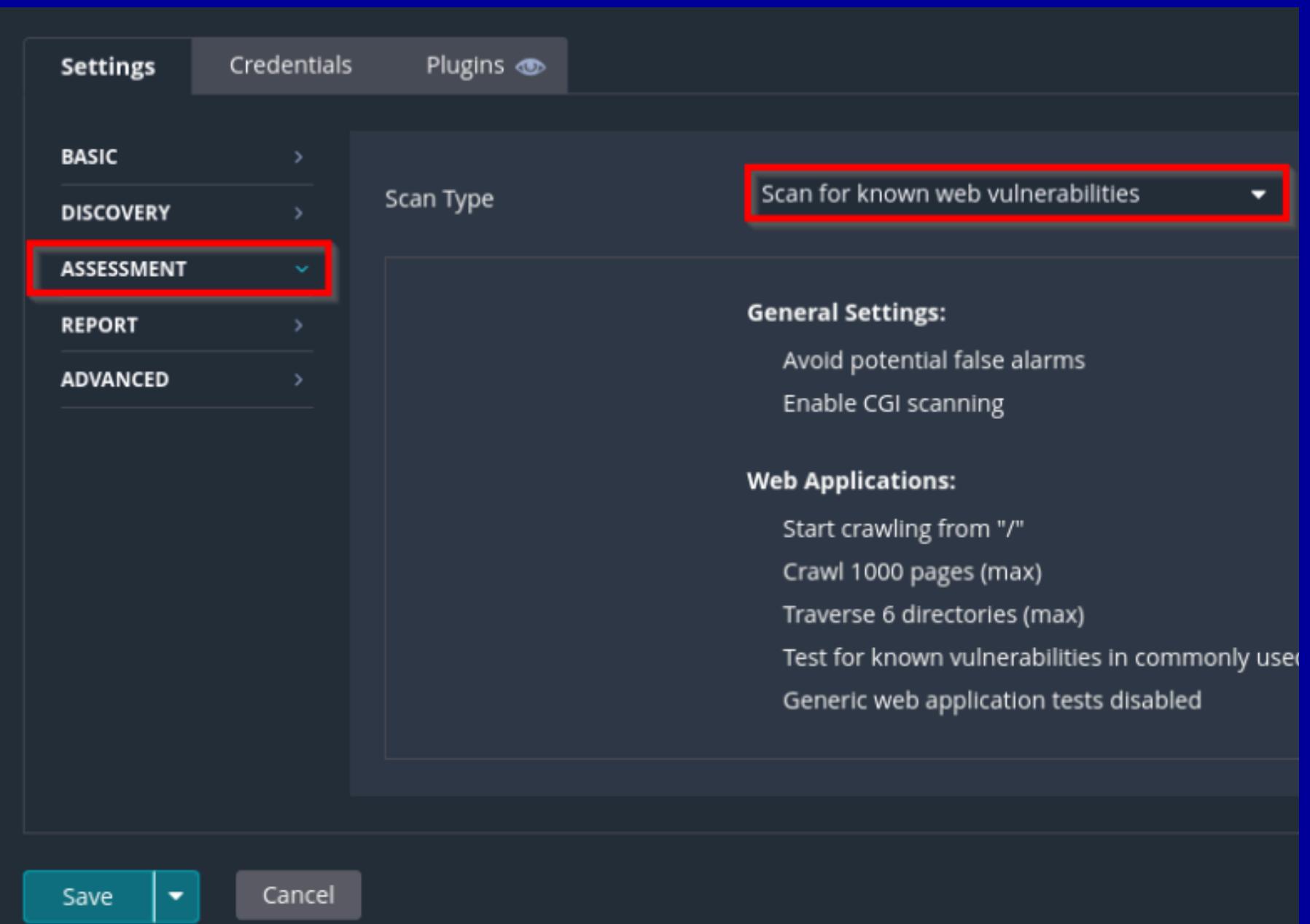
Tahap selanjutnya akan ada berbagai opsi scanning,tapi kali ini kita akan mencoba “basic scanning network”.



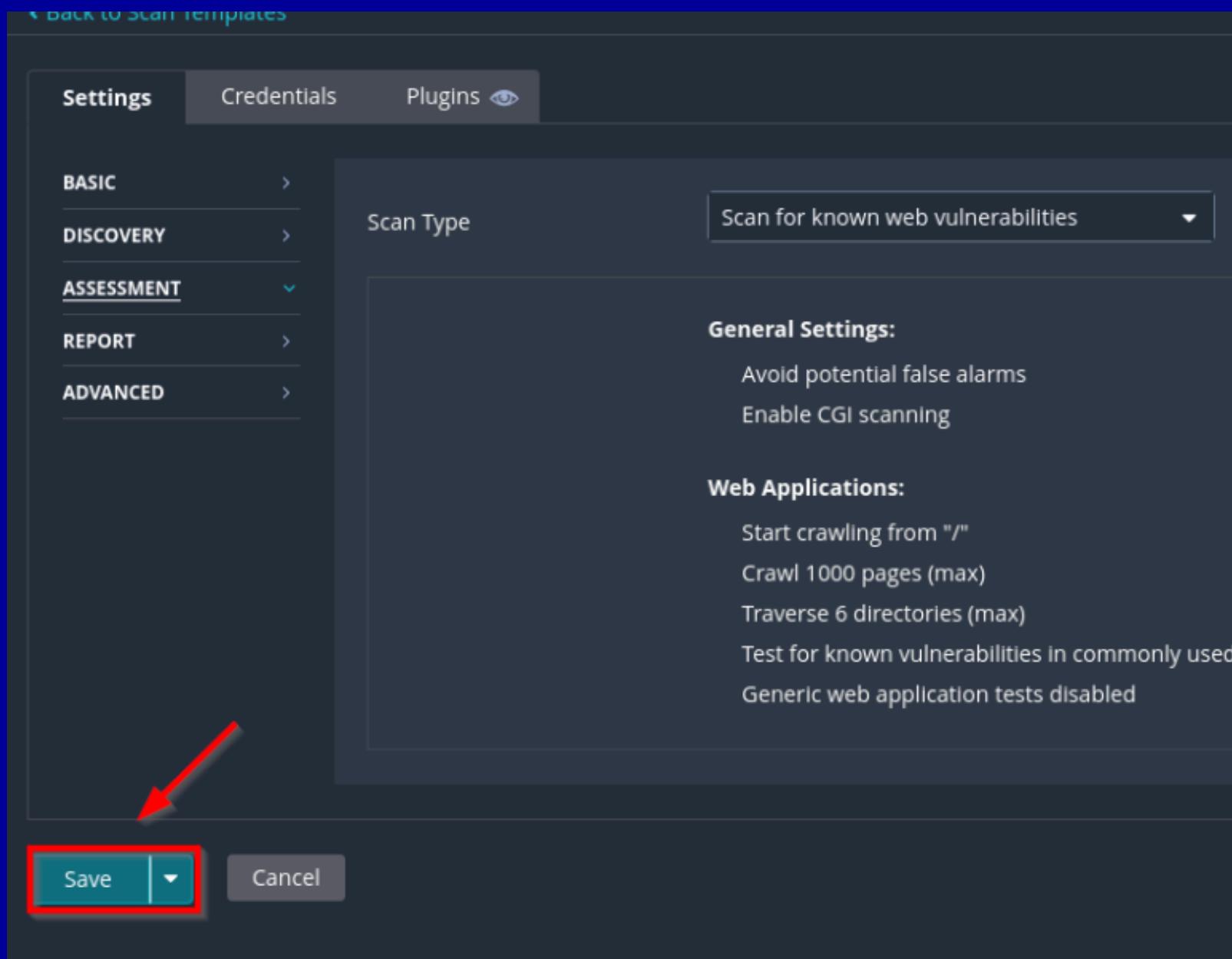
Lanjut anda harus mengkonfigurasi pengaturan itama sebelum meluncurkan pemindaian,berikut beberapa pengaturan yg disediakan.



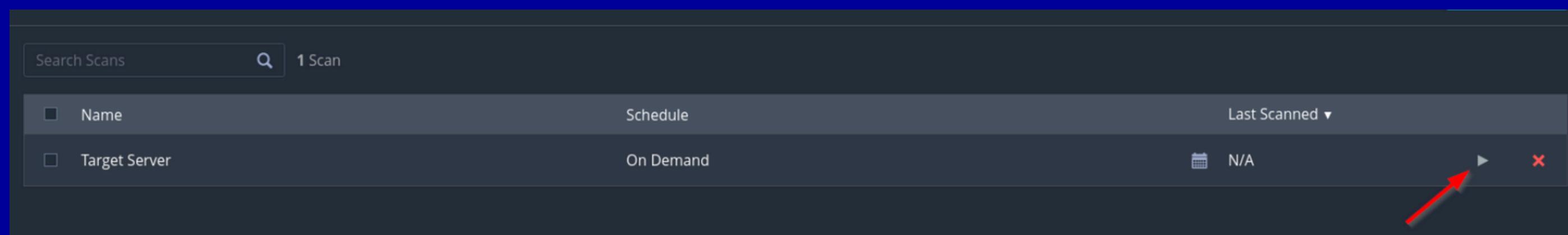
Langkah selanjutnya pilih pemindaian port yg diinginkan.pada tutorial ini kami menggunakan port scan (all ports).



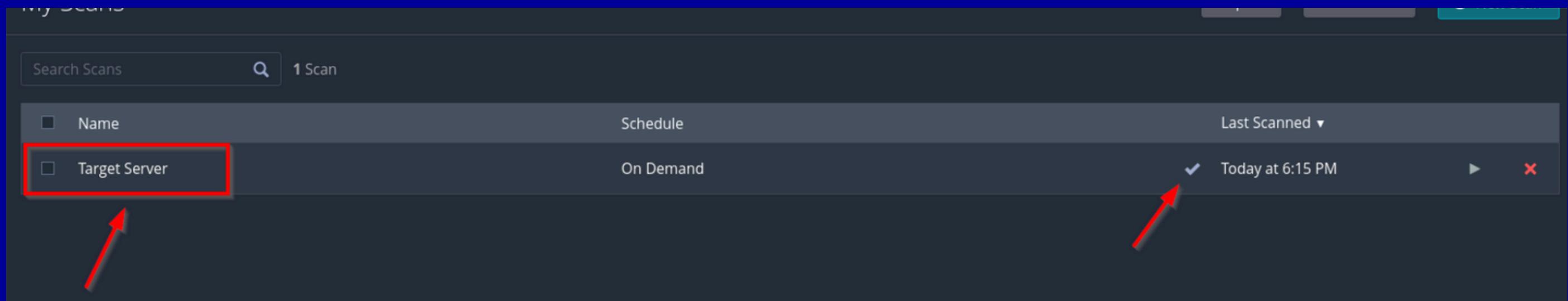
Langkah selanjutnya pilih jenis pemindaian yg diinginkan,terdapat berbagai macam pilihan.kami menggunakan "scan for known web vulnerabilities".



Lanjut klik "save" untuk menyimpan, ini merupakan pemindaian dasar, selebihnya anda bisa mencoba menjelajahi lagi.



Setelah Selesai anda dapat memulai pemindaian dengan membuka “my scanning” lalu mengklik tombol jalankan.



Klik pada hasil scanmu untuk melihat lebih detail.



Kita dapat memeriksa kerentanan yang terdeteksi dalam hasil pemindaian.

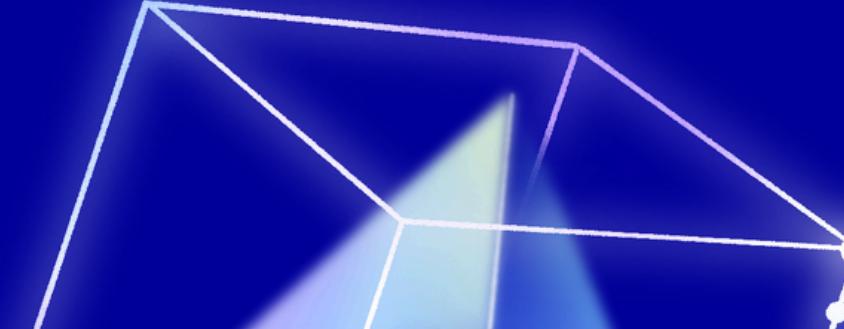
Filter ▾ Search Vulnerabilities  186 Vulnerabilities

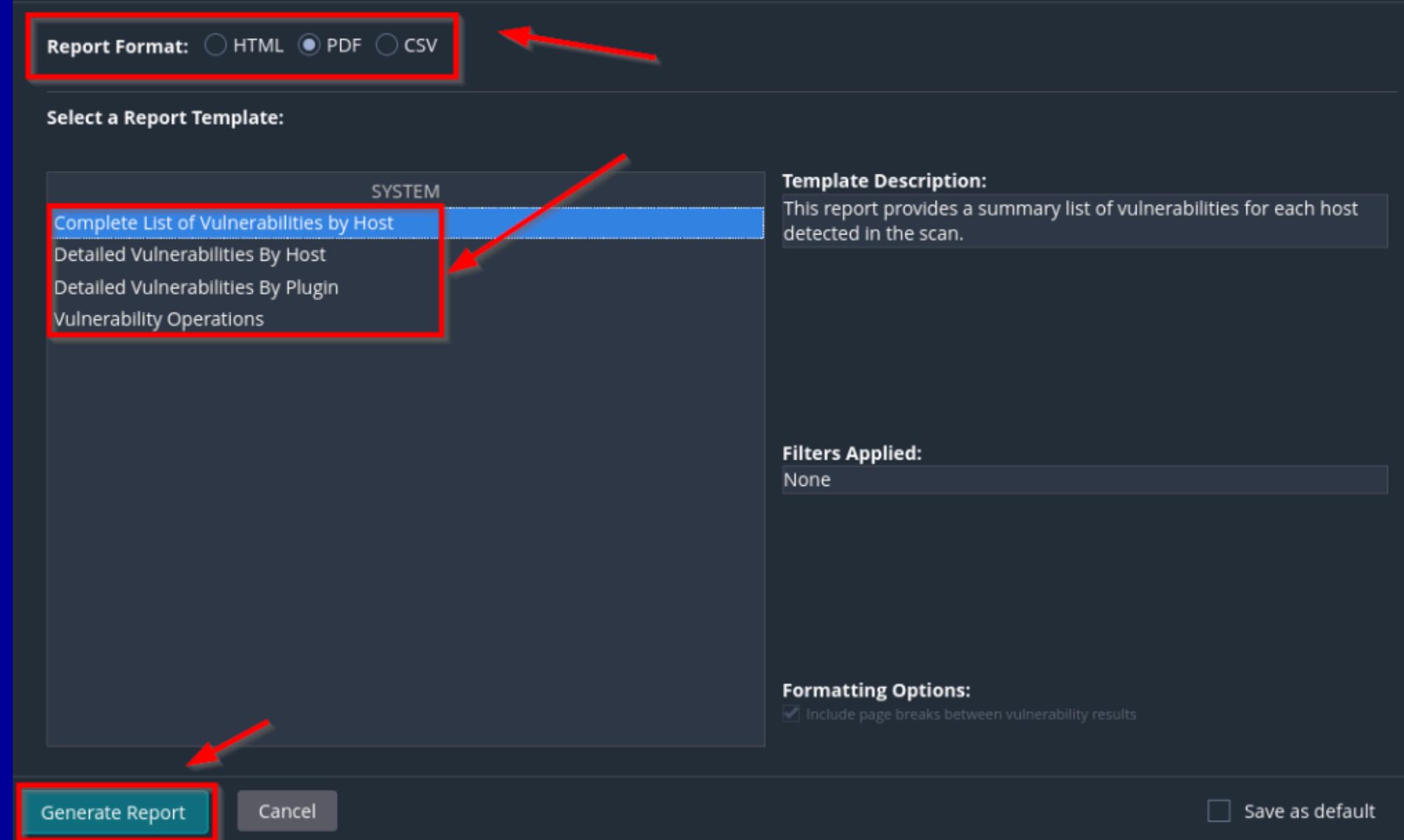
<input type="checkbox"/>	Sev	CVSS ▾	VPR	Name	Family	Count	
<input type="checkbox"/>	CRITICAL	10.0		PHP Unsupported Version Detection	CGI abuses	2	
<input type="checkbox"/>	CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclosure	RPC	1	
<input type="checkbox"/>	CRITICAL	10.0 *		Drupal Coder Module Deserialization RCE	CGI abuses	2	
<input type="checkbox"/>	CRITICAL	9.8	5.9	phpMyAdmin prior to 4.8.6 SQLi vulnerability (PMASA-2...	CGI abuses	2	
<input type="checkbox"/>	CRITICAL	9.8	7.4	GNU Bash Incomplete Fix Remote Code Injection (Shell...	CGI abuses	2	
<input type="checkbox"/>	CRITICAL	9.8	9.5	GNU Bash Environment Variable Handling Code Injecti...	CGI abuses	2	
<input type="checkbox"/>	CRITICAL	9.8	9.0	Apache 2.4.x < 2.4.56 Multiple Vulnerabilities	Web Servers	2	
<input type="checkbox"/>	CRITICAL	9.8	5.9	Apache 2.4.x < 2.4.54 Multiple Vulnerabilities	Web Servers	2	

untuk melihat kerentanan lebih detail kita dapat mengklik tab pada kerentanan.ini termasuk kerentanan yg terdeteksi dan dapat difilter berdasarkan tingkat keparahan.



LANGKAH-LANGKAH MEMBUAT LAPORAN DI NESSUS





Terakhir untuk membuat laporan dari hasil pemindaian, anda dapat memilih format apa dan anda juga dapat memilih template laporan.setelah selesai klik buat "generate report".

TERIMAKASIH!

BY TOKUPENS

