

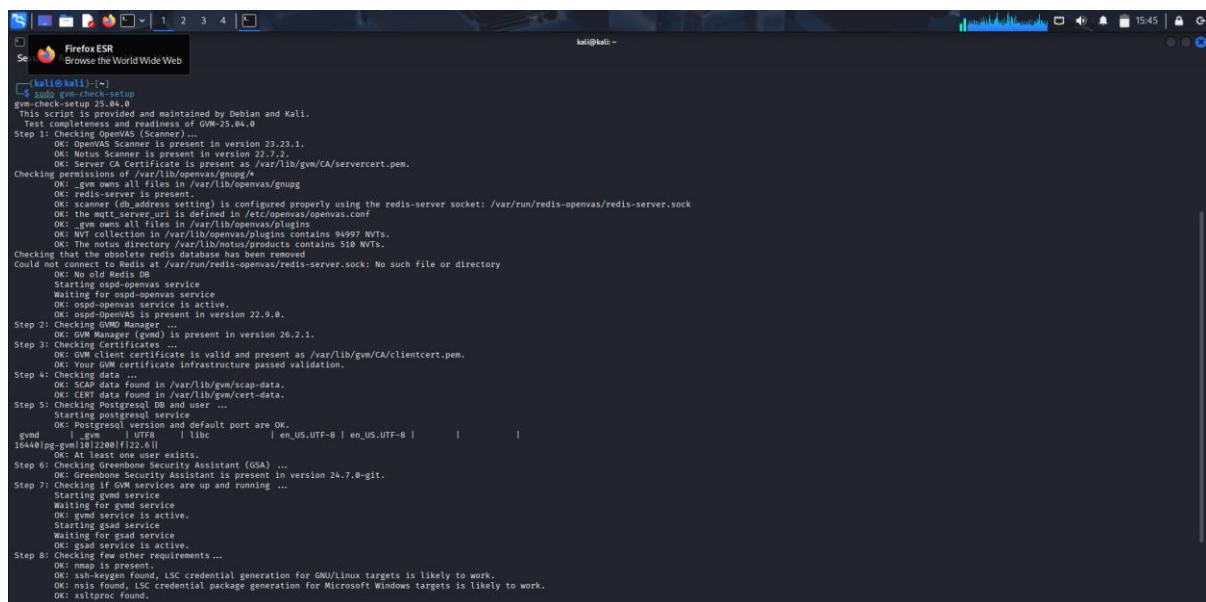
## W12D4\_PROGETTO 3\_ANALISI DELLE VULNERABILITA' E AZIONI DI RIMEDIO

La protezione delle reti e dei sistemi passa attraverso l'analisi delle vulnerabilità fatta in maniera costante. Durante un PT, nel momento in cui si effettua una scansione completa sul target attraverso l'utilizzo di tool come ad esempio Nessus o Greenbone, si vanno a rilevare tutti i servizi TCP e UDP attivi sulle porte che possono essere aperte o chiuse. Lo scanner effettua una ricerca delle vulnerabilità note per la versione del servizio con l'obiettivo di arrivare ad una Remediation action al termine della fase di exploit, cioè una o più azioni necessarie per andare a sanare i problemi di sicurezza che potrebbero altrimenti essere sfruttati.

L'utilizzo dello scanner di rete Greenbone sul target metasploitable aiuta ad individuare tutta una serie di vulnerabilità note che ne restituisce una fotografia in base alla gravità (CVSS), questo per dare priorità all'azione di rimedio da adottare di conseguenza.

Sul target metasploitable con ip 192.168.50.106 si implementa una scansione delle porte TCP e UDP ovvero i protocolli di trasporto sui quali si trovano porte e servizi.

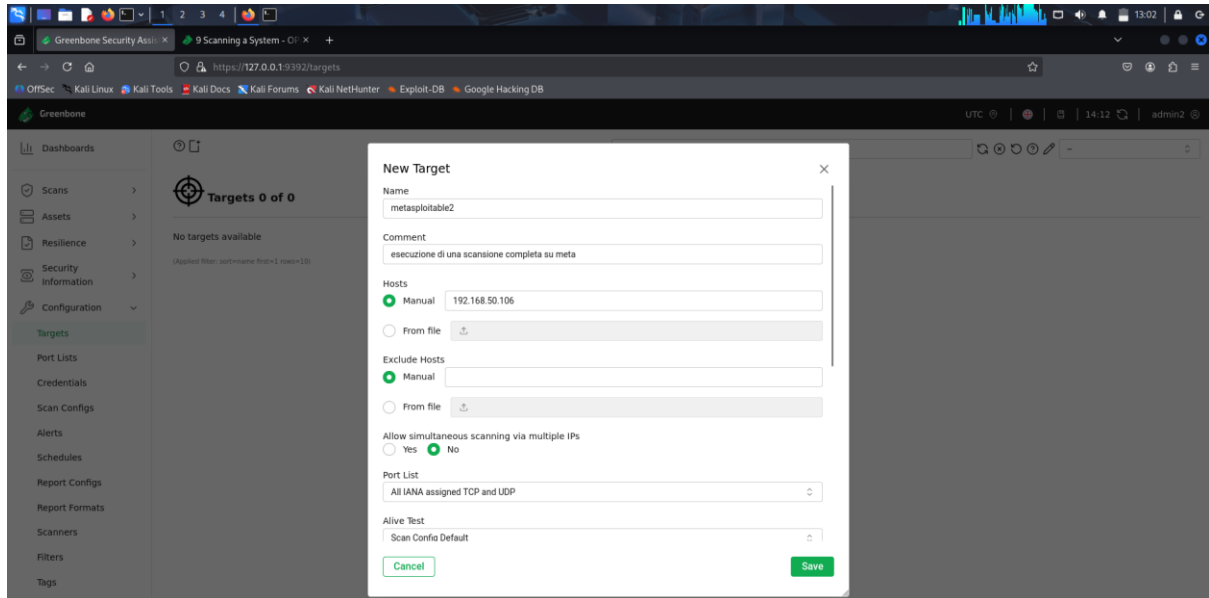
### Avvio del tool Greenbone



```
kali@kali:~$ sudo gvm-check-setup
gvm-check-setup 25.04.0
This script is provided and maintained by Debian and Kali.
Test completeness and readiness of GVM-25.04.0
Step 1: Checking OpenVAS (Scanner)...
OK: OpenVAS Scanner is present in version 23.23.1.
OK: Notus Scanner is present in version 22.7.2.
OK: Server CA Certificate is present as /var/lib/gvm/CA/servercert.pem.
Checking permissions of /var/lib/openvas/gnupg/...
OK: _gvm owns all files in /var/lib/openvas/gnupg
OK: redis-server is present.
OK: scanner (db.address setting) is configured properly using the redis-server socket: /var/run/redis-openvas/redis-server.sock
OK: the mqtt_server_uri is defined in /etc/openvas/openvas.conf
OK: _gvm owns all files in /var/lib/openvas/plugins
OK: NVT collection in /var/lib/openvas/plugins contains 94997 NVTs.
OK: The notus directory /var/lib/notus/products contains 510 NVTs.
Checking that the obsolete redis database has been removed
Could not connect to Redis at /var/run/redis-openvas/redis-server.sock: No such file or directory
OK: No old Redis DB
Starting osdp-openvas service
Waiting for osdp-openvas service
OK: osdp-openvas service is active.
OK: osdp-OpenVAS is present in version 22.9.0.
Step 2: Checking GVM Manager ...
OK: GVM Manager (gvm) is present in version 26.2.1.
Step 3: Checking Certificates ...
OK: GVM client certificate is valid and present as /var/lib/gvm/CA/clientcert.pem.
OK: Your GVM certificate infrastructure passed validation.
Step 4: Checking data ...
OK: SCAP data found in /var/lib/gvm/scap-data.
OK: CERT data found in /var/lib/gvm/cert-data.
Step 5: Checking PostgreSQL DB and user ...
Starting postgresql service
OK: PostgreSQL version and default port are OK.
gvm | _gvm | UTF8 | libc | en_US.UTF-8 | en_US.UTF-8 | | |
10440/pg-gvm1012200/f122.6.0
OK: At least one user exists.
Step 6: Checking Greenbone Security Assistant (GSA) ...
OK: Greenbone Security Assistant is present in version 24.7.0-git.
Step 7: Checking if GVM services are up and running ...
Starting gvm service
Waiting for gvm service
OK: gvm service is active.
Starting gsad service
Waiting for gsad service
OK: gsad service is active.
Step 8: Checking few other requirements...
OK: nmap is present.
OK: ssh-keygen found, LSC credential generation for GNU/Linux targets is likely to work.
OK: nsls found, LSC credential generation for Microsoft Windows targets is likely to work.
OK: xsltproc found.
```

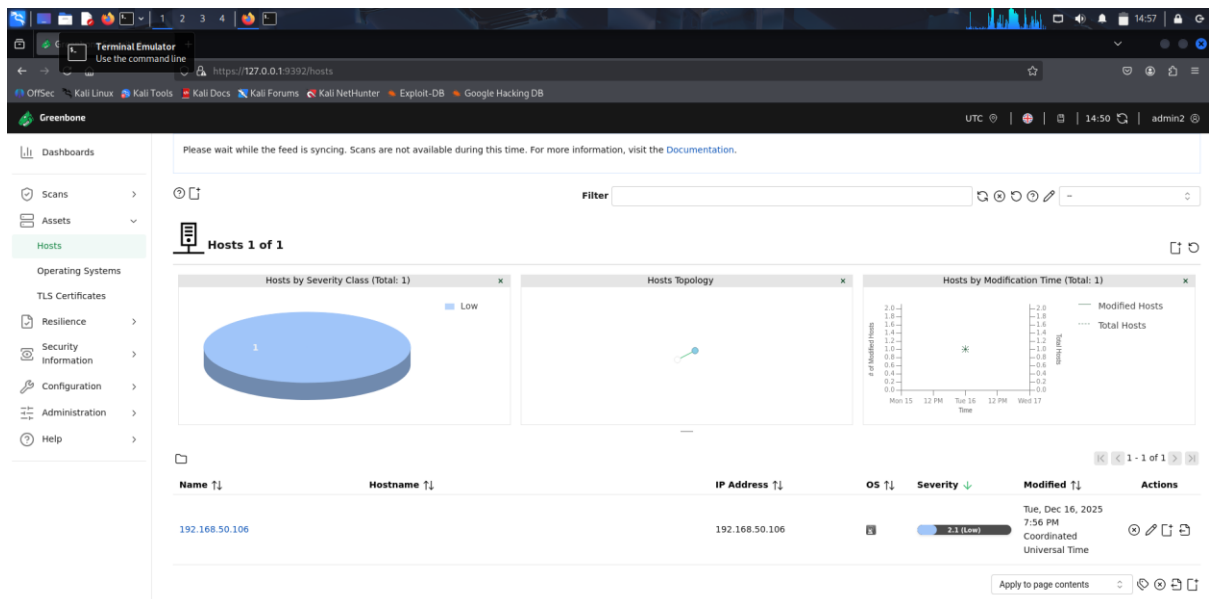
## Selezione delle porte ed individuazione del target

IP: 192.168.50.106



## Primi risultati della scansione

-host



Sistema operativo

abon

Terminal Emulator

Greenbone Security Ass...

Use the command line

https://127.0.0.1:9392/operatingsystems

OfSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

Greenbone

UTC 14:38 admin2

Dashboards

Scans

Assets

Hosts

Operating Systems

TLS Certificates

Resilience

Security Information

Configuration

Administration

Help

Operating Systems 1 of 1

Operating Systems by Severity Class (Total: 1)

Most Vulnerable Operating Systems

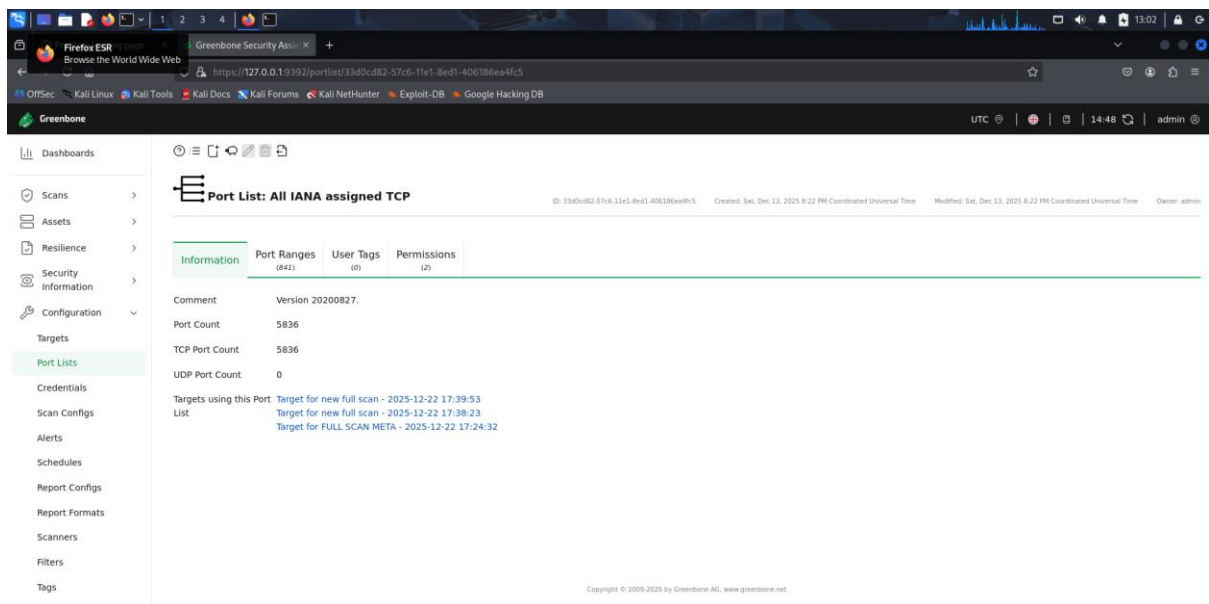
Operating Systems by CVSS (Total: 1)

Name	Title	Severity			Hosts		Modified	Actions
		Latest	Highest	Average	All	Best OS		
cpe:/o:linux:kernel		2.1 (Low)	2.1 (Low)	2.1 (Low)	1	1	Tue, Dec 16, 2025 7:56 PM Coordinated Universal Time	

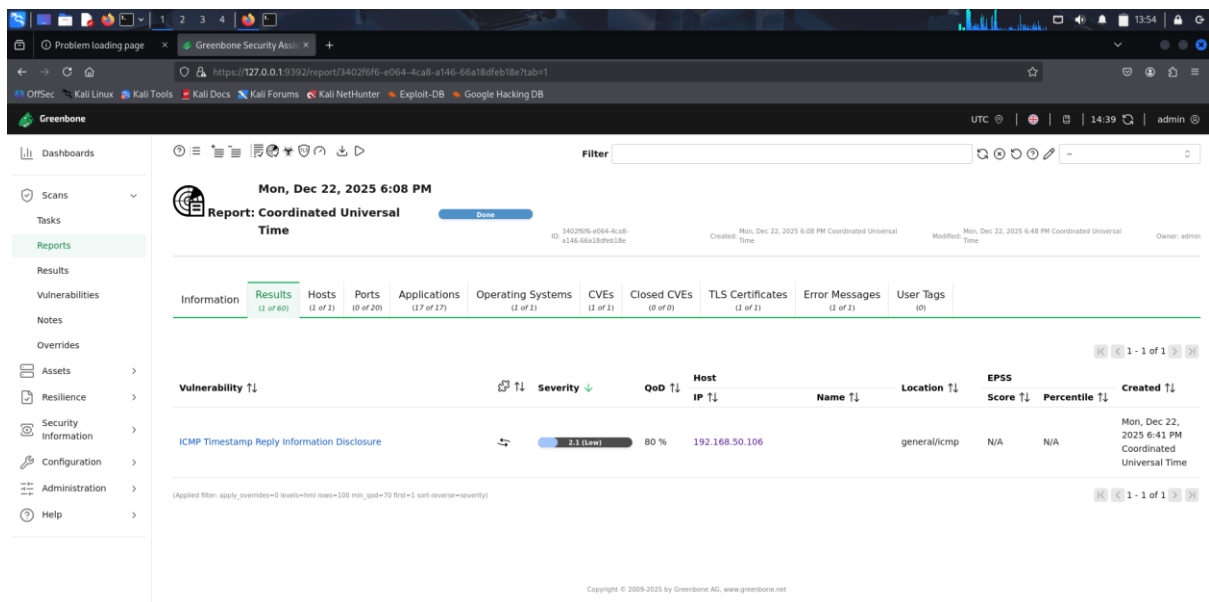
Apply to page contents

Applied filter: sort=reverse=latest\_severity first=1 rows=10

Copyright © 2009-2025 by Greenbone AG, www.greenbone.net



S



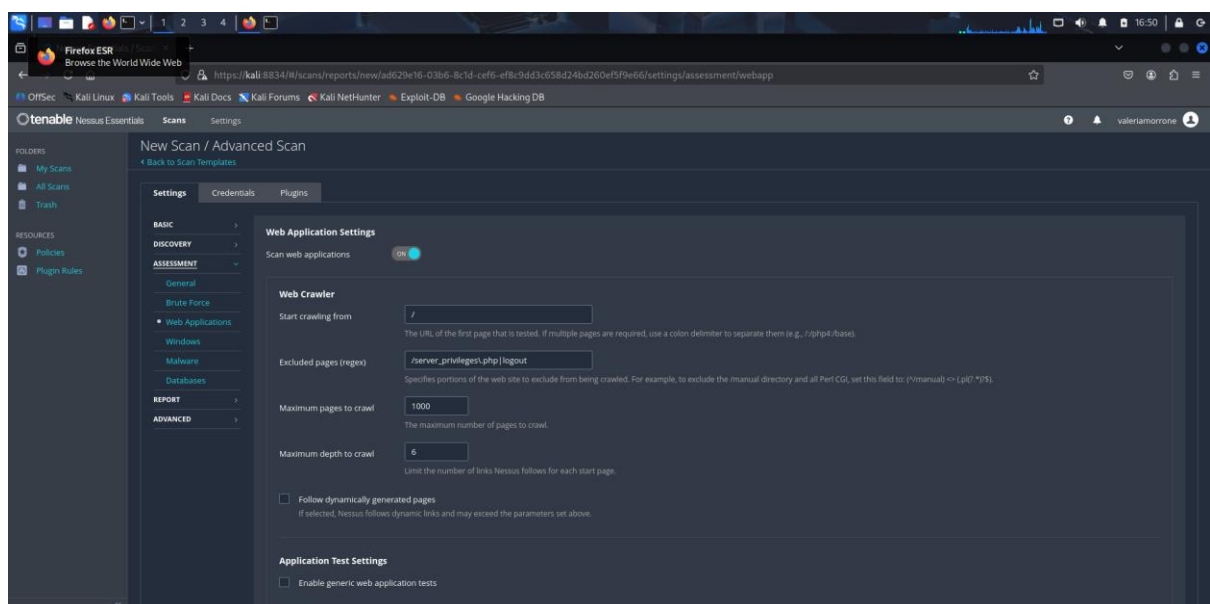
Sulla sezione report è possibile individuare e controllare quelle che sono le informazioni riguardanti la scansione.

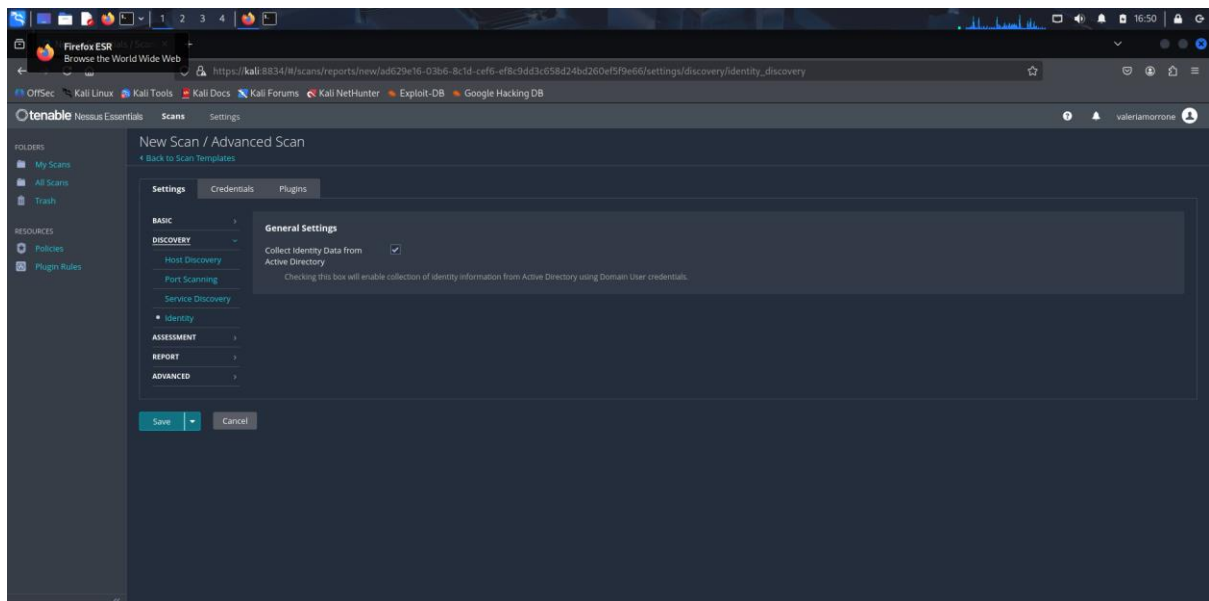
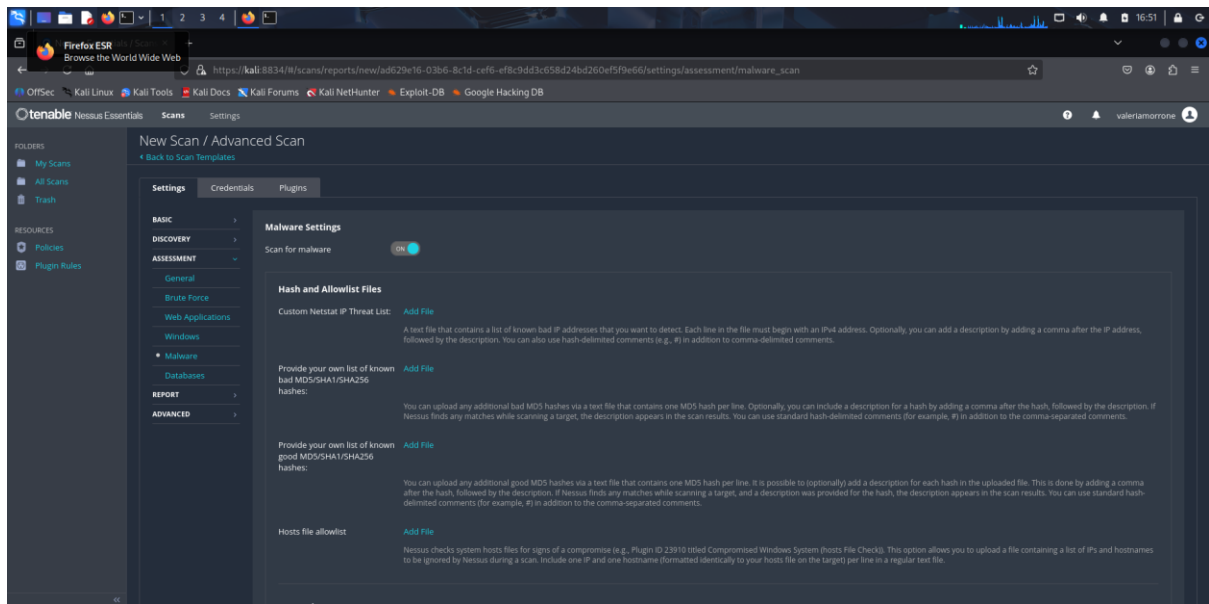
/

Sono state effettuate varie scansioni ma non sono state trovate vulnerabilità sul target.

*(è stato effettuato un tentativo anche con l'utilizzo dello scanner di rete Nessus ma non è andato a buon fine in quanto il programma consente un numero limitato di scansioni, per tale motivo l'attività è stata effettuata con il tool Greenbon.)*

*Segue immagine rappresentativa dei passaggi*





Da una prima scansione effettuata le vulnerabilità sulla macchina risultano essere 54 che sono poi scese successivamente a 14.

**NOTE FINALI:**

Implementate le azioni di rimedio per le vulnerabilità scelte e con livello di gravità più elevato, si effettua l'esecuzione di una seconda scansione della rete che deve restituire un risultato diverso da quello della precedente.

Una volta avuta quindi una panoramica delle porte e dei servizi attivi è importante ridurre al minimo i tentativi di attacco.

Fine progetto 22/12/2025