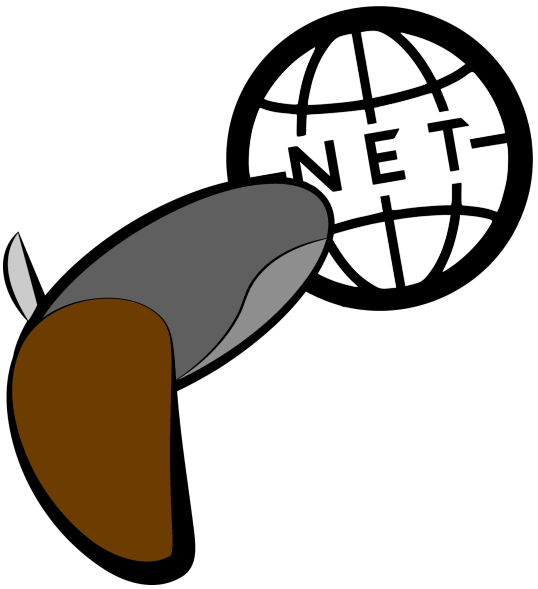


MANUALE D’USO

NetGun

Versione	0.2
Data	15/02/2023
Destinatario	Professore Carmine Gravino
Presentato da	Carlo Colizzi, Giulio Incoronato, Antonio Mazzarella

Revision History

Data	Versione	Descrizione	Autori
07/02/2023	0.1	Stesura del Manuale di installazione	Antonio Mazzarella
15/02/2023	0.2	Revisione Totale	Giulio Incoronato

Team Members

Nome	Informazioni di contatto
Carlo Colizzi	c.colizzi@studenti.unisa.it
Giulio Incoronato	g.incoronato2@studenti.unisa.it
Antonio Mazzarella	a.mazzarella5@studenti.unisa.it

Sommario

1 Introduzione

1.1 Scopo del Sistema

NetGun ha l'obiettivo di essere un Framework per il Penetration Testing (Testing Black Box di infrastrutture in rete).

È possibile racchiudere il sistema in 3 componenti principali. La componente per lo scanning, la componente per l'enumerazione dei dati raccolti, e le utilities che assistono l'utente in tutte le fasi del pre e post scanning.

Inoltre ha il fine di facilitare una pratica complessa come i Penetration Test, così da permettere ai PT di concentrarsi su aspetti più delicati, automatizzando e velocizzando le task alla base di questo tipo di Testing.

1.2 Scopo del documento

Lo scopo di questo documento è quello di mostrare i passaggi necessari per utilizzare gli use case definiti nel Requirements Analysis Document.

1.3 Relazione con altri documenti

Di seguito l'elenco di tutti i documenti in relazione con il manuale:

- Requirements Analysis Document (RAD)
- System Design Document (SDD)
- Object Design Document (ODD)
- Test Plan (TP)
- Test Case Specification (TCS)
- Codice Sorgente

- Matrice di tracciabilità

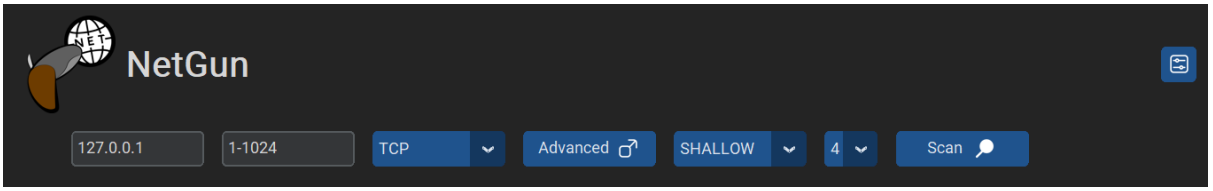
2 Use Case

2.1 Utente effettua il Deep Scanning (UC_2)

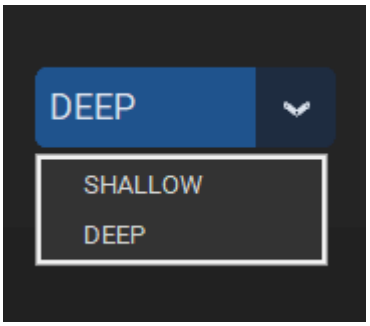
Lo Use Case fornisce la funzionalità ad un Utente di effettuare uno scanner di rete sulla versione dei servizi in esecuzione sulle porte aperte.

La precondizione per effettuare lo scanner è che l'utente deve aver messo i filtri desiderati nelle operazioni di filtering.

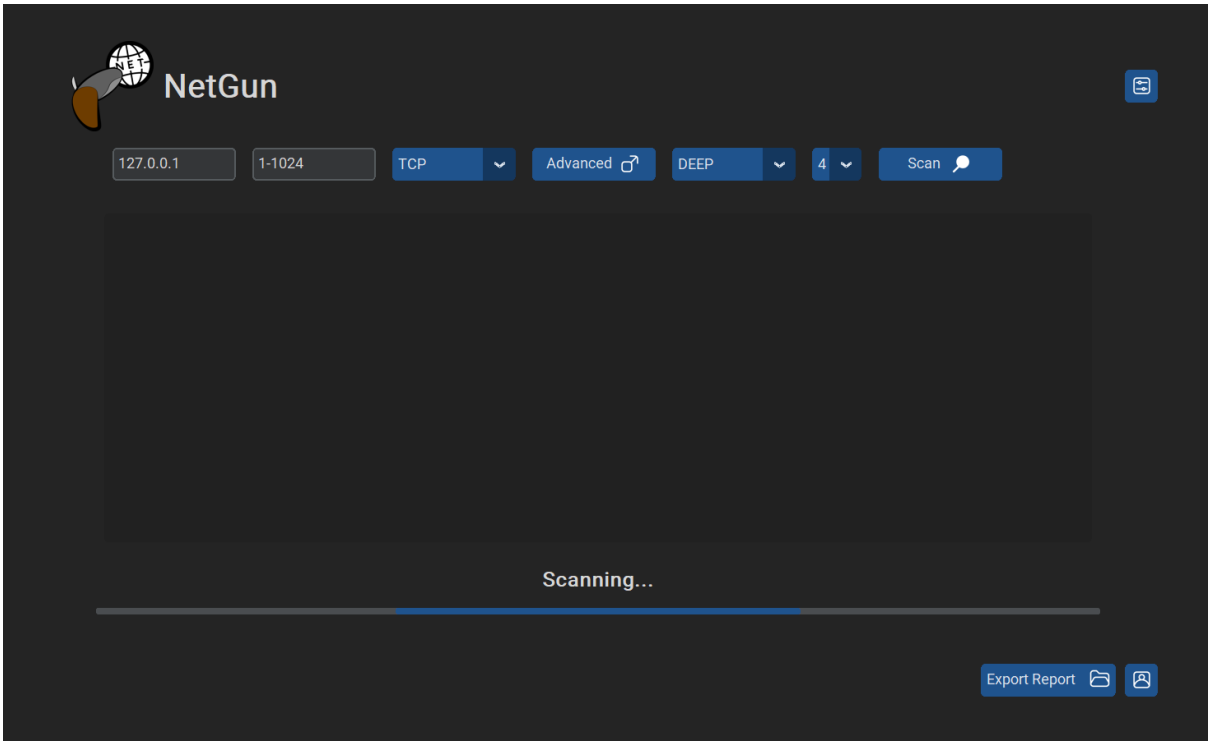
Dopo aver fatto il filtering l'utente avrà la seguente schermata.



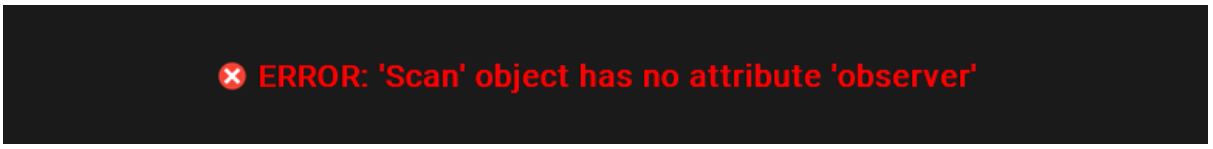
Cliccando su **SHALLOW** si aprirà un piccolo drop-down menù.



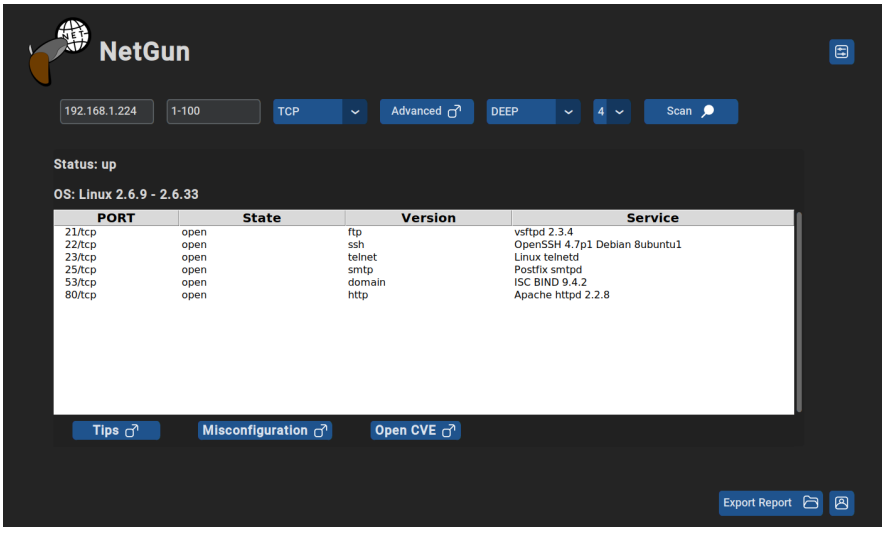
Dove sarà possibile selezionare la modalità **DEEP**.
Fatto ciò basterà cliccare su Scan per avviare lo scanning richiesto da filtering con modalità **DEEP**.



Se lo scan avrà problemi a partire o un qualsiasi problema, verrà generato un pop up con scritto l'errore. ESEMPIO:

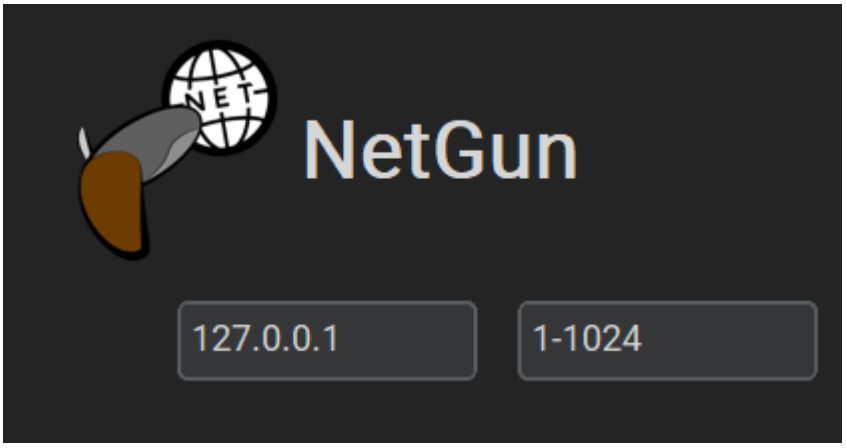


Alla fine dello scan verrà inserita una tabella con tutti i risultati dello scan.

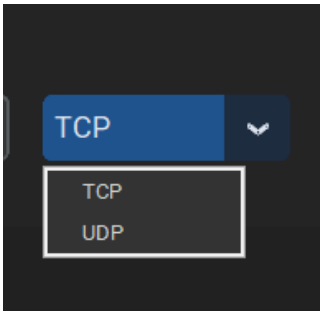


2.2 Utente effettua il Filtering (UC_3)

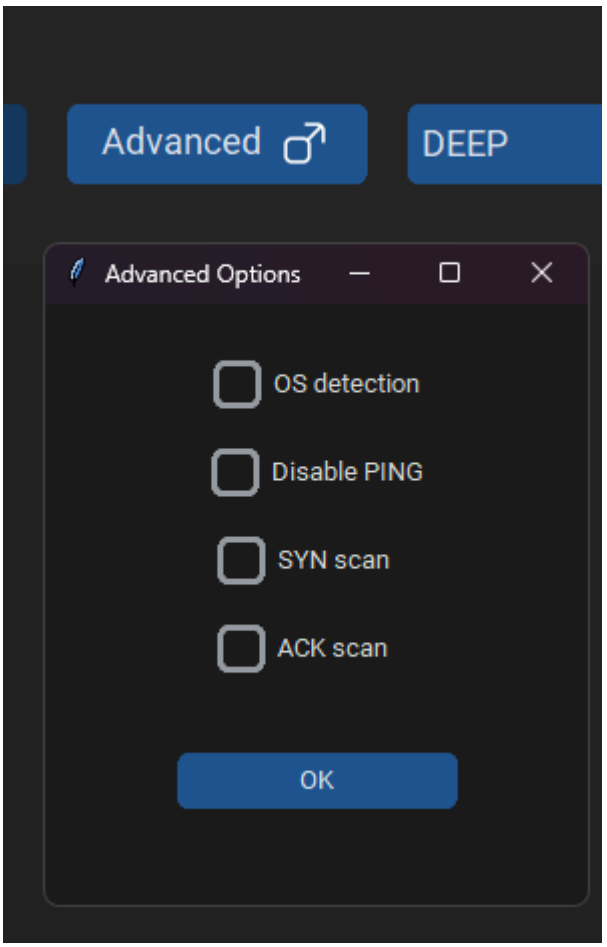
Questo Use Case permette all'utente di inserire tutte le opzioni di filtro nello scanning.
Nella prima parte l'utente sarà chiamato a inserire l'**IP** e il **range di porte** da analizzare:



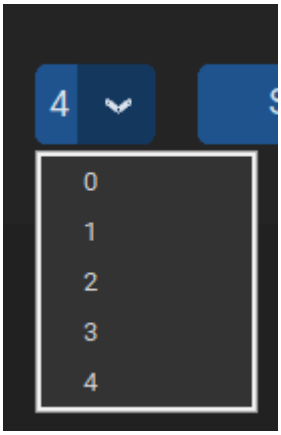
Successivamente il **protocollo** (Solo uno dei due selezionabili):



Le opzioni avanzate (tutte selezionabili in simultanea tranne per **SYN** e **ACK**).



La modalità selezionata in UC_2 e per finire l'**aggressività** dello scanning:

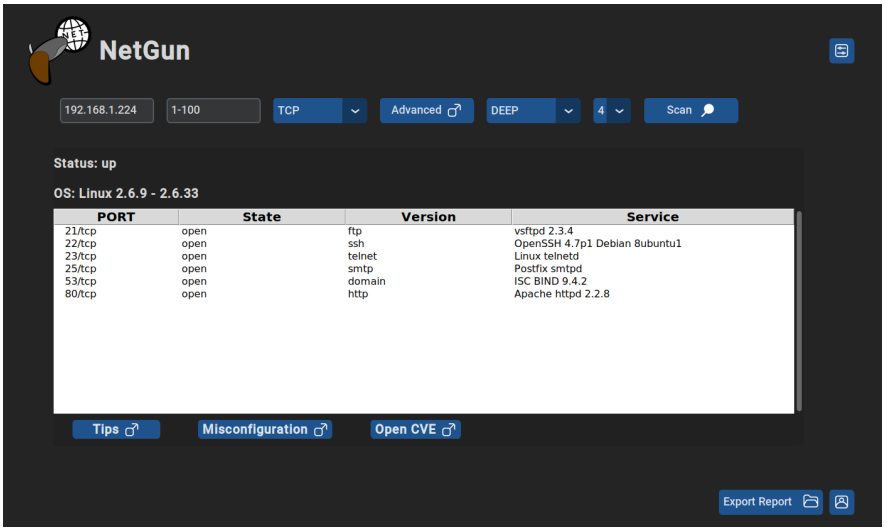


Fatto ciò basterà cliccare su scan per far partire lo scan del endpoint inserito nel primo step.

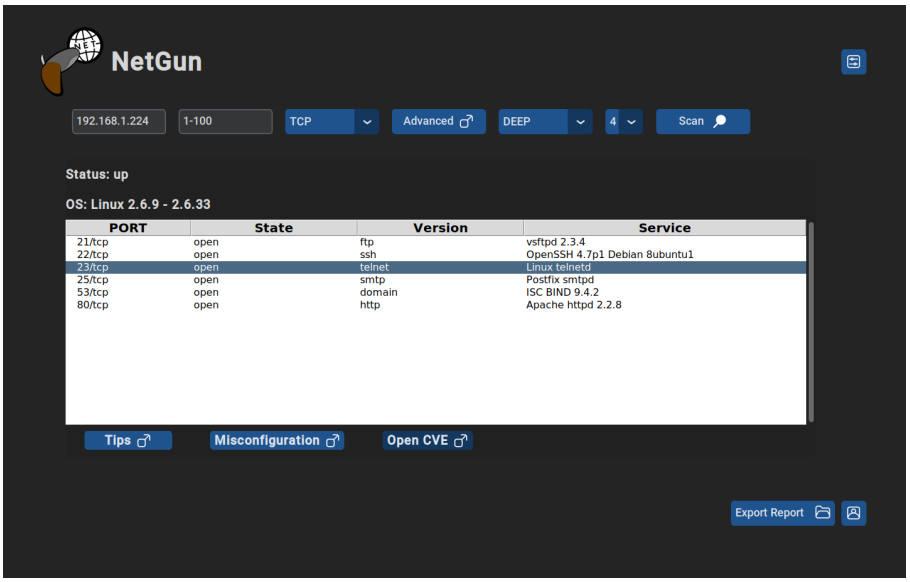
2.3 Utente effettua una ricerca delle CVE (UC_5)

Questo use case permette di ricercare le CVE presenti sulla porta aperta selezionata.

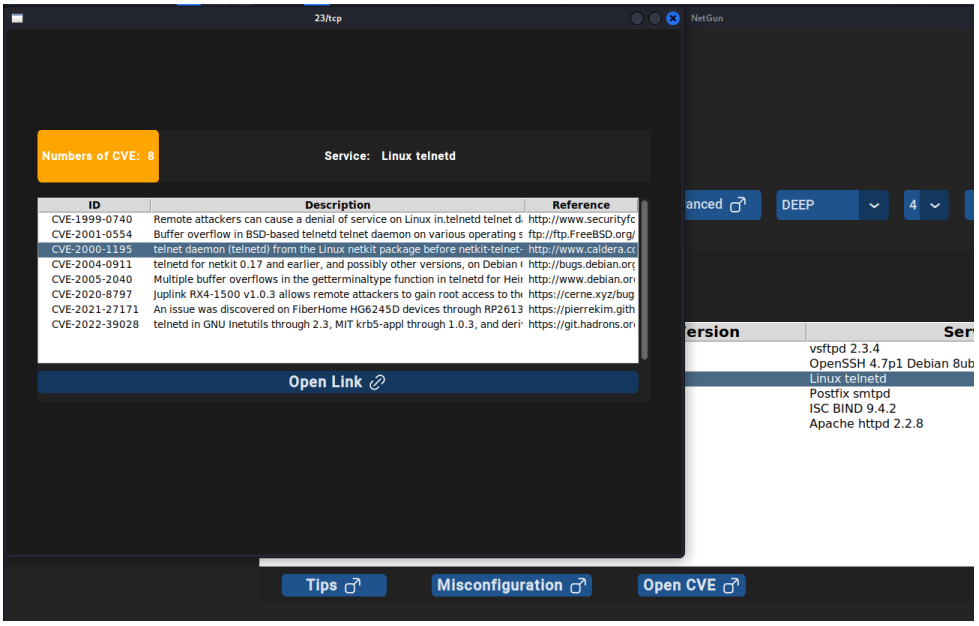
Una volta finito lo scan si avrà questa schermata:



Basterà cliccare sopra una di esse e poi sul bottone **Open CVE:**



Da qui si avrà un'altra tabella selezionabile come quella dello scan completato. Ci sarà un colore a seconda del numero di CVE trovate che va dal verde al rosso e un insieme di risultati che vengono mostrati su una tabella:



Cliccando su una riga e poi sul pulsante **Link**, si aprirà una pagina Web con informazioni utili su quella vulnerabilità: