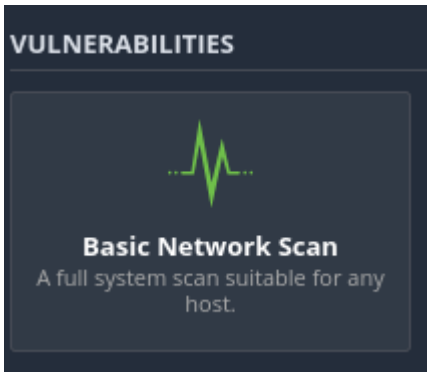
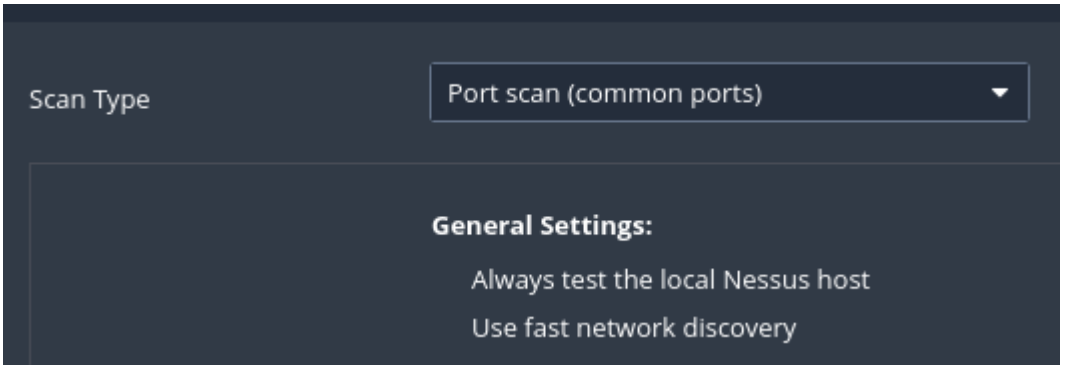
Analisi del Report di Nessus su Metasploitable

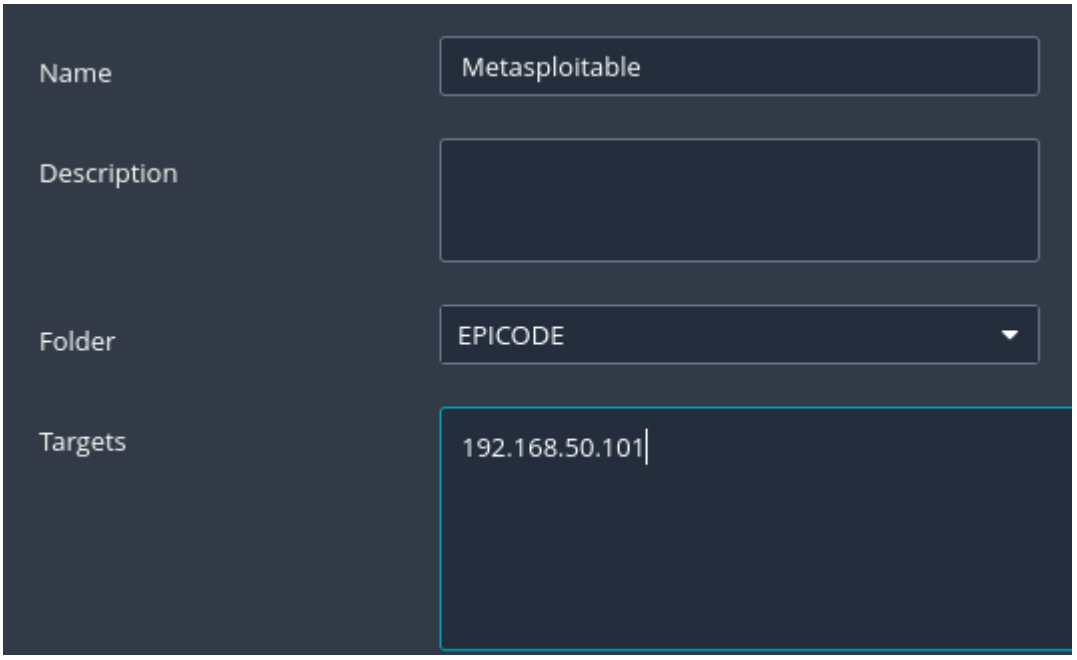
L'obiettivo di questo esercizio è acquisire familiarità con l'utilizzo di Nessus, uno dei principali strumenti di vulnerability assessment, in questo caso utilizzato per analizzare un una macchina vulnerabile Metasploitable.

L'attività è stata strutturata in tre fasi principali:

1. **Configurazione della scansione** (da https://localhost:8834/ impostando tutti i parametri richiesti); vedi gli screenshot sotto dell'impostazione utilizzata per Metasploitable

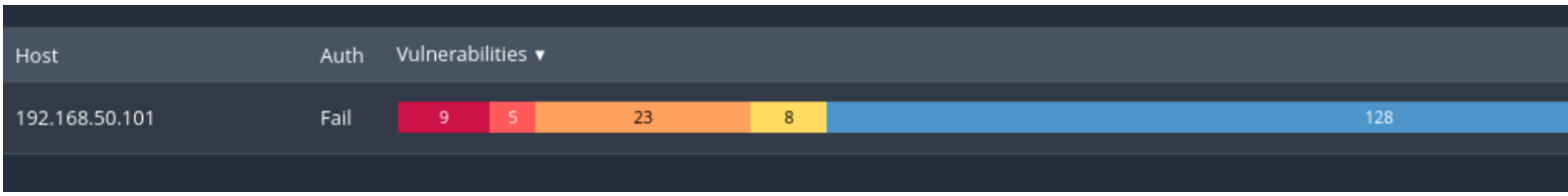






Abbiamo selezionato un Basic Network Scan con la scansione delle porte comuni più utilizzate e nella sezione target abbiamo inserito l'indirizzo IP della macchina Metasploitable.

2. **Esecuzione della scansione** attraverso Nessus con la configurazione utilizzata; (vedi screenshot sotto)



Questo è ciò che viene visualizzato in seguito alla scansione. In blu abbiamo la voce Info, mentre in rosso, arancione e giallo sono rappresentate le vulnerabilità (da low a critica).

3. **Analisi del report generato da Nessus**, con approfondimento delle vulnerabilità rilevate, valutazione dei rischi e studio delle possibili soluzioni

Aggiungo qui sotto qualche informazione aggiuntiva su qualche vulnerabilità trovata:

VULNERABILITA' CRITICA

Bind Shell Attiva (PORTA 1524)

- **Descrizione**: Shell remota disponibile senza credenziali.

- **Soluzione**: Verificare compromissione e reinstallare il sistema.

Sistema Operativo Obsoleto (PORTA 80/HTTP)

- **Descrizione**: Ubuntu 8.04 non riceve più patch dal 2013.
- **Soluzione**: Migrare a una versione supportata.

VNC Debole (PORTA 5900)

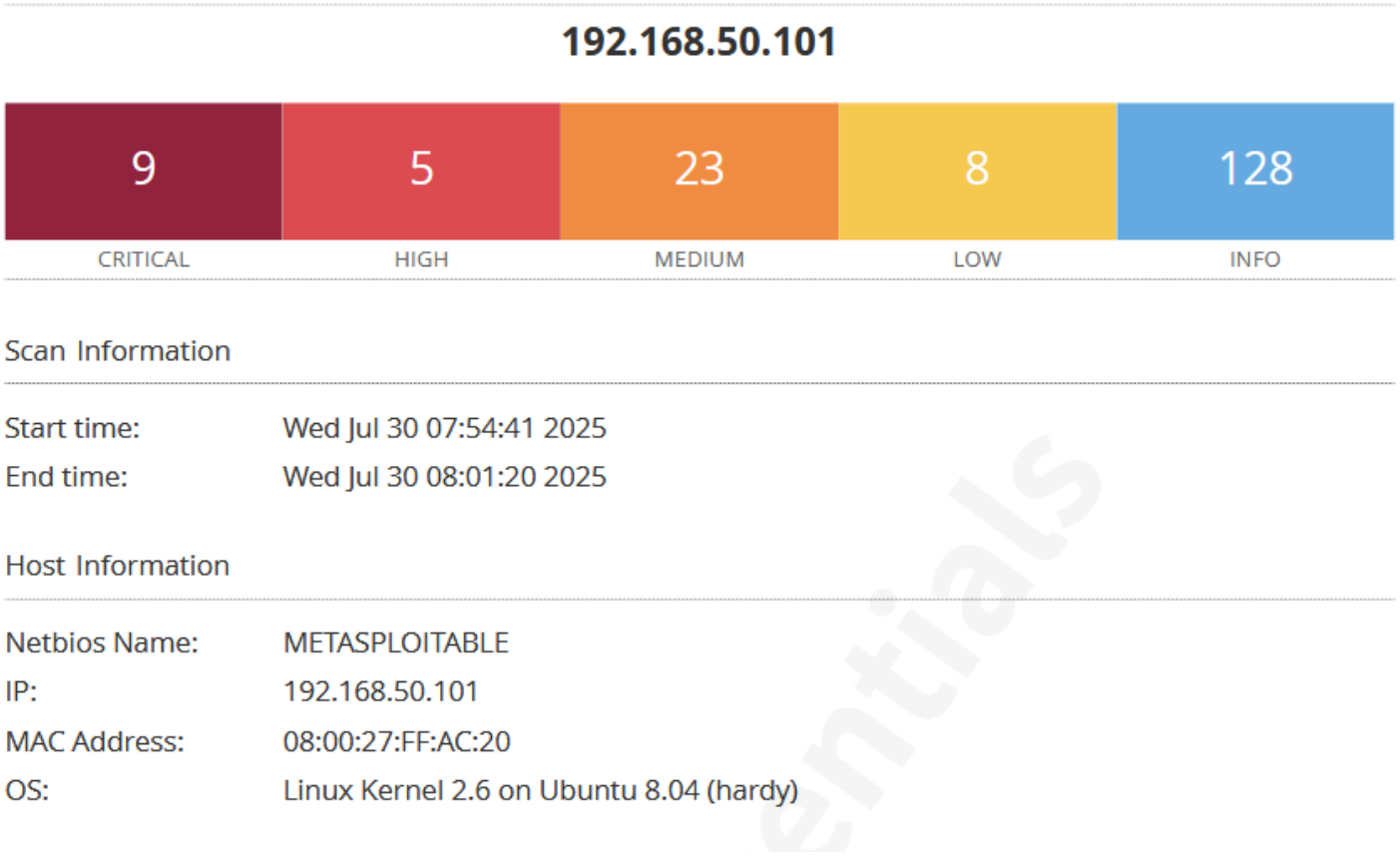
- **Descrizione**: Accesso con password “password”.
- **Soluzione**: Impostare una password complessa e/o disabilitare il servizio se non necessario.

VULNERABILITA’ MEDIA

HTTP TRACE (PORTA 80/HTTP)

- **Descrizione:** Permette attacchi Cross Site Tracing (XST), ovvero un trucco usato dagli hacker per **r**ubare informazioni riservate, come le credenziali di accesso (username, password o cookie), mentre una persona sta usando un sito web.
- **Soluzione:** Disabilitare TRACE/TRACEEnable, quindi questa funzione va disattivata perché non necessaria.

Ecco lo screenshot del report generato (che allego insieme a questo pdf)



192.168.50.101

9	5	23	8	128
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time:	Wed Jul 30 07:54:41 2025
End time:	Wed Jul 30 08:01:20 2025

Host Information

Netbios Name:	METASPLOITABLE
IP:	192.168.50.101
MAC Address:	08:00:27:FF:AC:20
OS:	Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

Concludo dicendo che l'attività che abbiamo svolto fornisce una base pratica utile per chi si approccia al mondo della sicurezza informatica e del penetration testing.