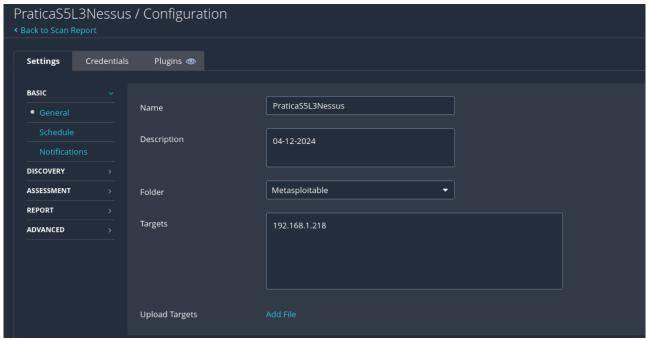
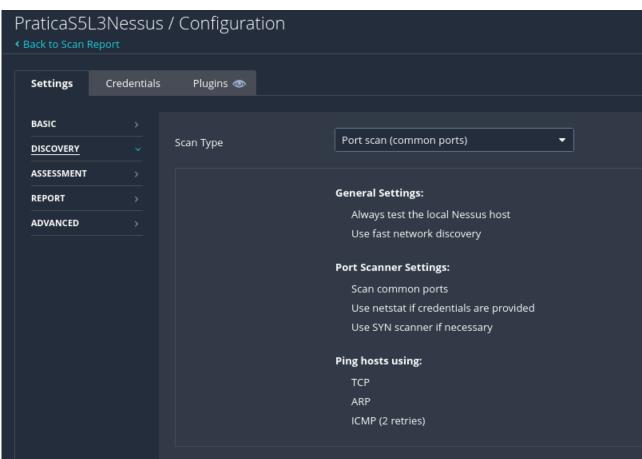
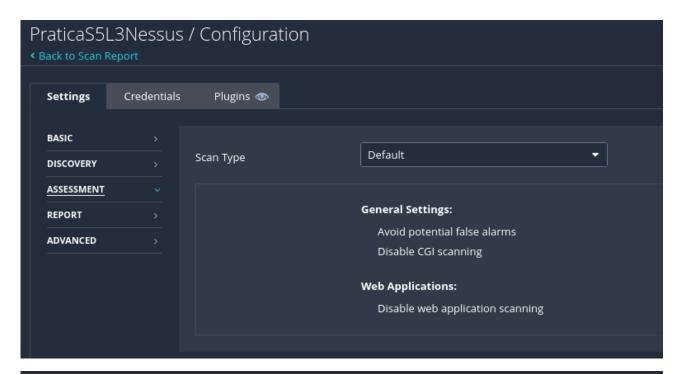
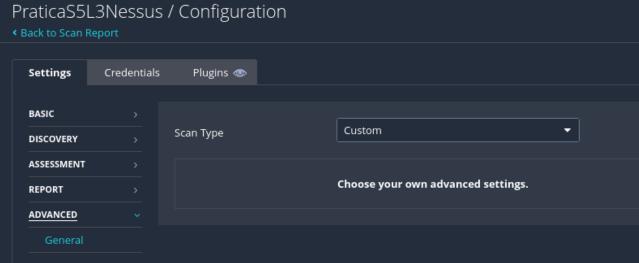
## PraticaS5L3

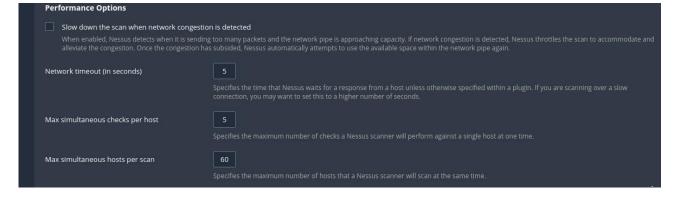
## Impostazioni Nessus











La scansione ha rilevato varie vulnerabilità.

Ne ho analizzate tre critiche

1) Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

Porta: 22

La vulnerabilità è grave perché mette a rischio la sicurezza delle comunicazioni SSH, le chiavi utilizzate per garantire la sicurezza delle connessioni potrebbero essere facilmente indovinate da un attaccante, quindi è necessario sostituirle e aggiornare il software per evitare che il sistema venga compromesso.

2) Bind Shell Backdoor Detection

Porta: 1524

Il sistema remoto ha una shell che sta ascoltando sulla porta 1524 e non richiede alcuna autenticazione per accedervi. Questo significa che chiunque riesca a connettersi a quella porta può inviare comandi direttamente al sistema, ottenendo il pieno controllo e la possibilità di eseguire comandi come amministratore.

3) Apache Tomcat AJP Connector Request Injection (Ghostcat)

Porta: 8009

La vulnerabilità Ghostcat (CVE-2020-1745) permette a un attaccante di leggere file importanti su un server Apache Tomcat vulnerabile, e in alcuni casi, di eseguire comandi dannosi. Per proteggere il sistema, è necessario aggiornare Tomcat e sistemare le impostazioni del server in modo che nessuno non autorizzato possa accedervi.