Obbiettivo : exploitare la phpmyadmin su metasploitable

Cerchiamo con search su metasploit la parola php (linguaggio utilizzato lato server) e CGI (interfaccia che ci fa visualizzare i contenuti presenti nel web server)

A computer screen shot of a program

Description automatically generated

Trovato l’exploit con questi due parametri utilizziamo il payload che ci offre di default,

selezioniamo l’rhost e avviamo l’exploit

una volta avviata l’interfaccia meterpreter useremo il comando syninfo per accertarci di essere dentro

A computer screen shot of a computer program

Description automatically generated