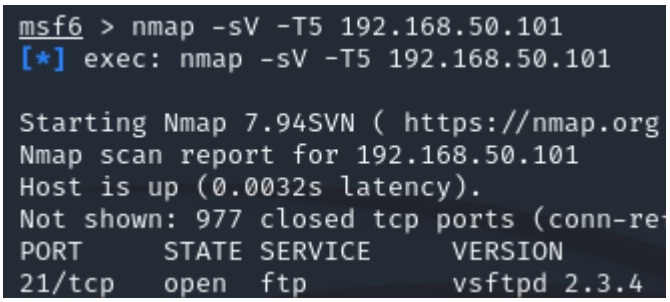
Iniziamo facendo una scansione delle porte della macchina metasploitable:



Quindi quello che ci interessa è la versione del servizio vsftpd; ora possiamo cercare con metasploit se ci sono degli exploit che si possono usare:

Ne abbiamo trovato uno in particolare che possiamo utilizzare scrivendo “use 0”.
A questo punto controlliamo le opzioni dell’exploit e modifichiamo quelle che ci interessano, come RHOST, mettendo l’IP della macchina target, lanciamo l’exploit con “run” e siamo nella shell della metasploitable, ora navighiamo verso la directory root e ne creiamo una: Test_metasploit.