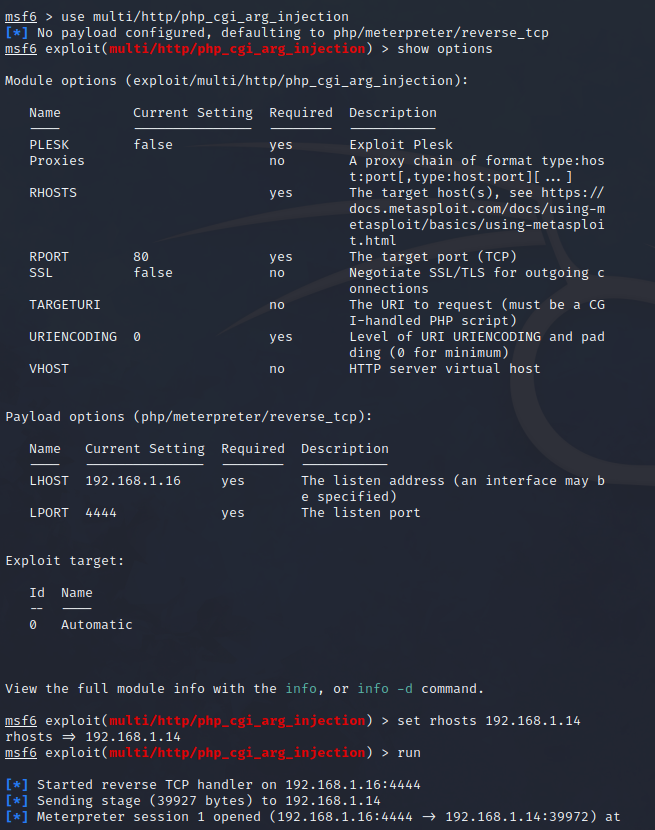
Exploit con Metasploit

Dopo una scansione su nmap o Nessus di Metasploitable2 con Kali, notiamo che il servizio http sulla porta 80 è attivo e quindi può presentare delle vulnerabilità.

Proviamo a creare una shell sul servizio http della macchina vittima utilizzando il programma Metasploit, di conseguenza cerchiamo un exploit nel programma che potrebbe essere inerente a qualche servizio web.

Decidiamo di utilizzare gli exploit riguardanti il protocollo php (utilizzato insieme a html per le applicazioni web).

multi/http/php\_cgi\_arg\_injection questo è l’exploit che andremo ad utilizzare per creare una shell dal nostro terminale alla web app.



Dopo aver configurato le opzioni del comando manteniamo il payload di default che ci consiglia Metasploit.

Una volta fatto possiamo far partire il nostro attacco e possiamo notare che siamo dentro alla web app e abbiamo creato una connessione tra noi e la macchina vittima.

