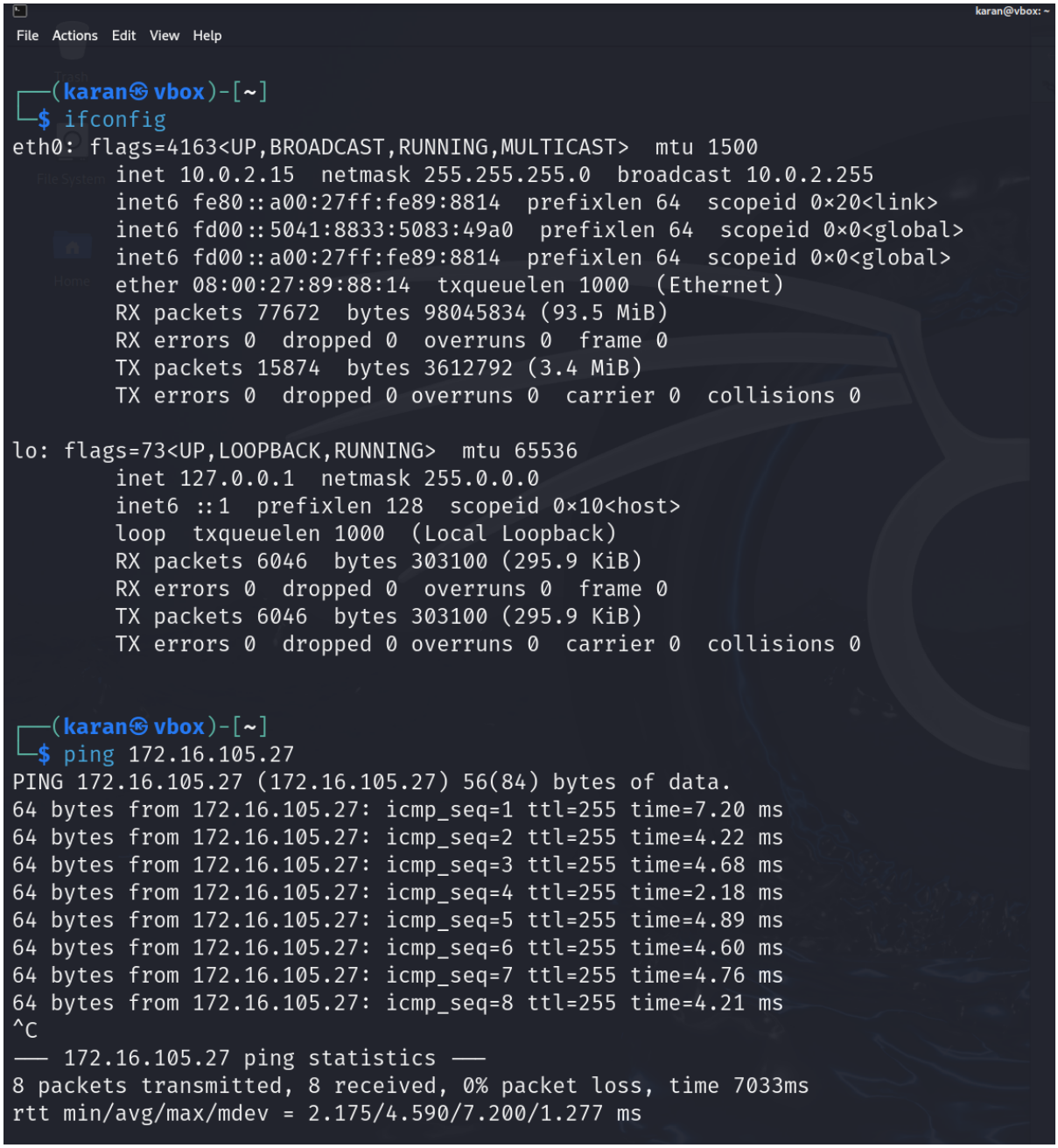
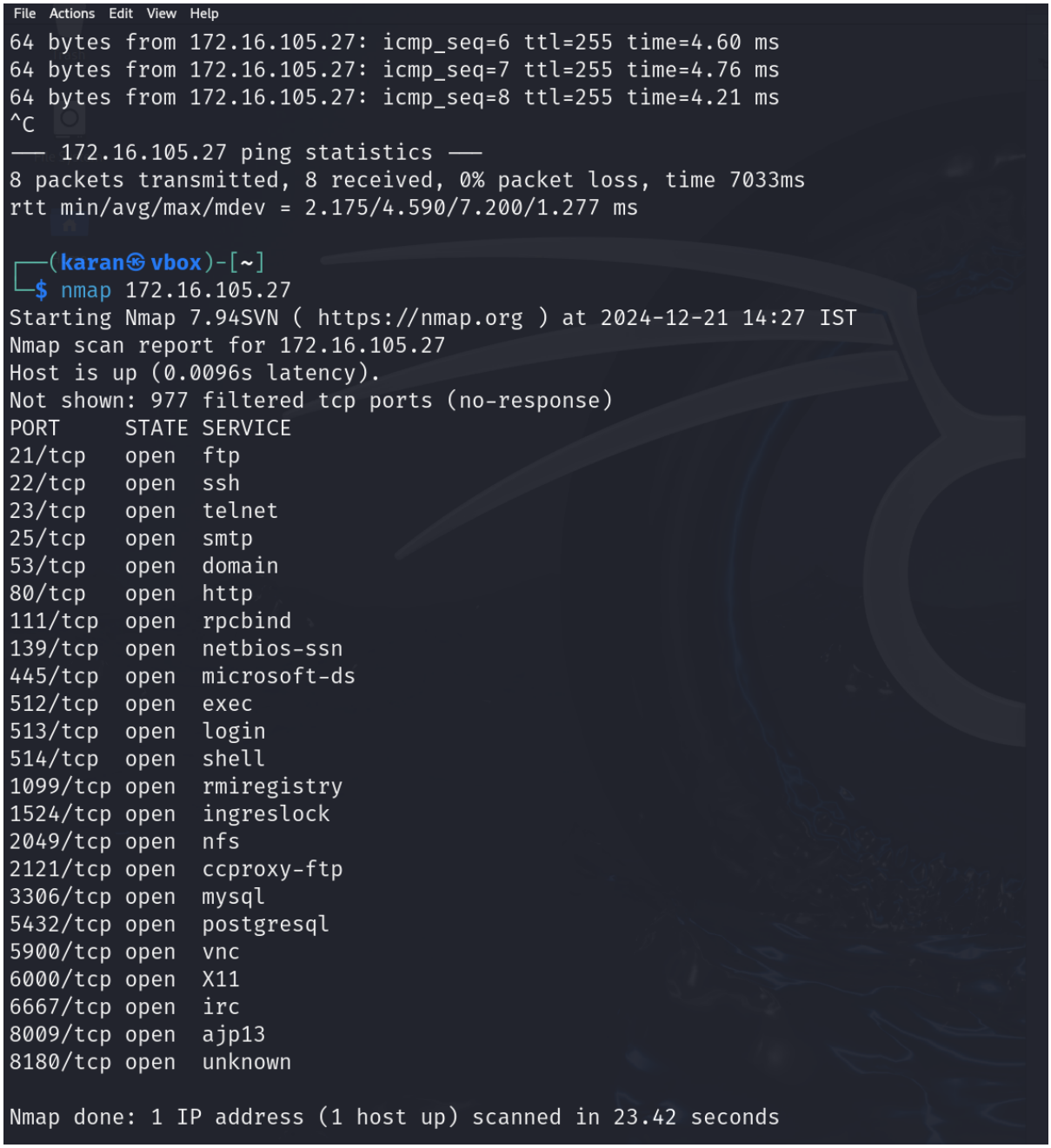
FOSS CLUB – EVALUATION ASSIGNMENT :

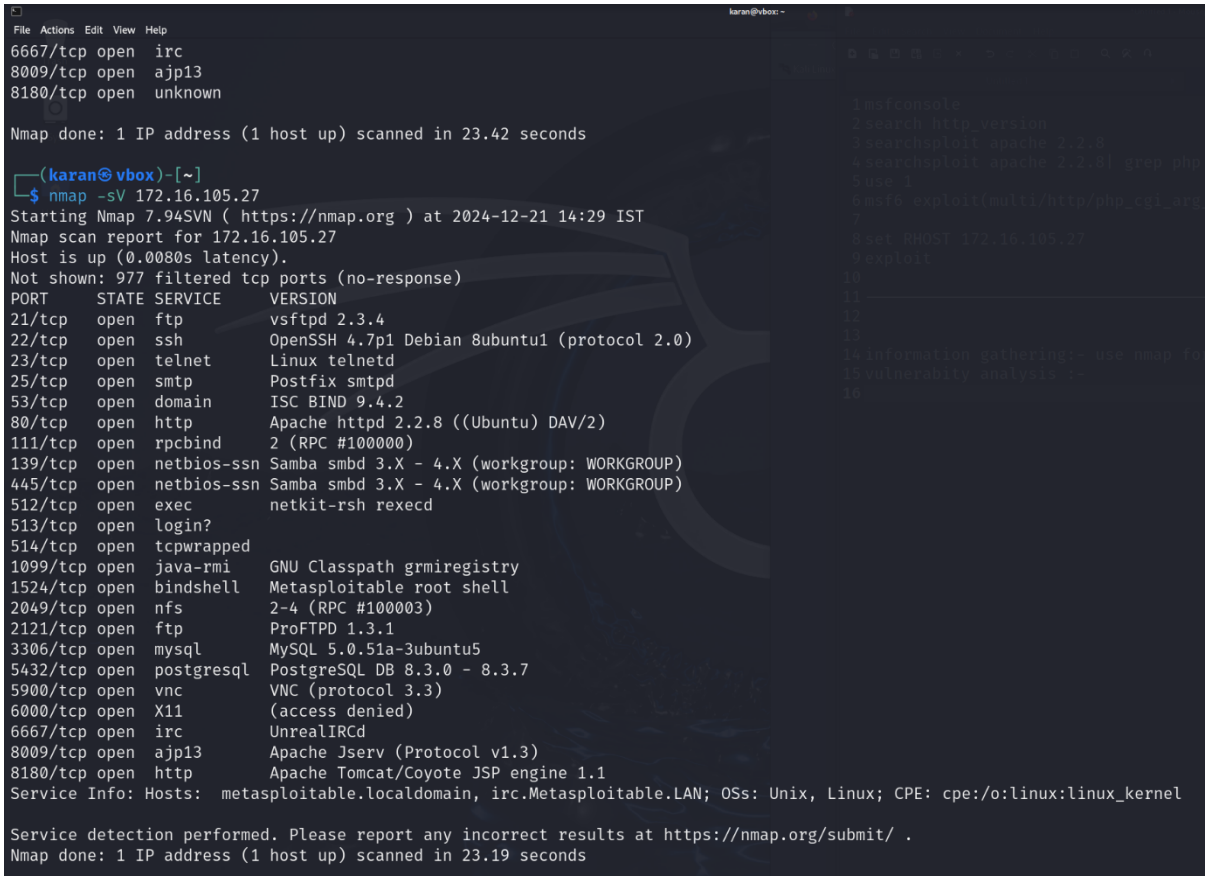


ifconfig – To get IP address of the network we are connected to

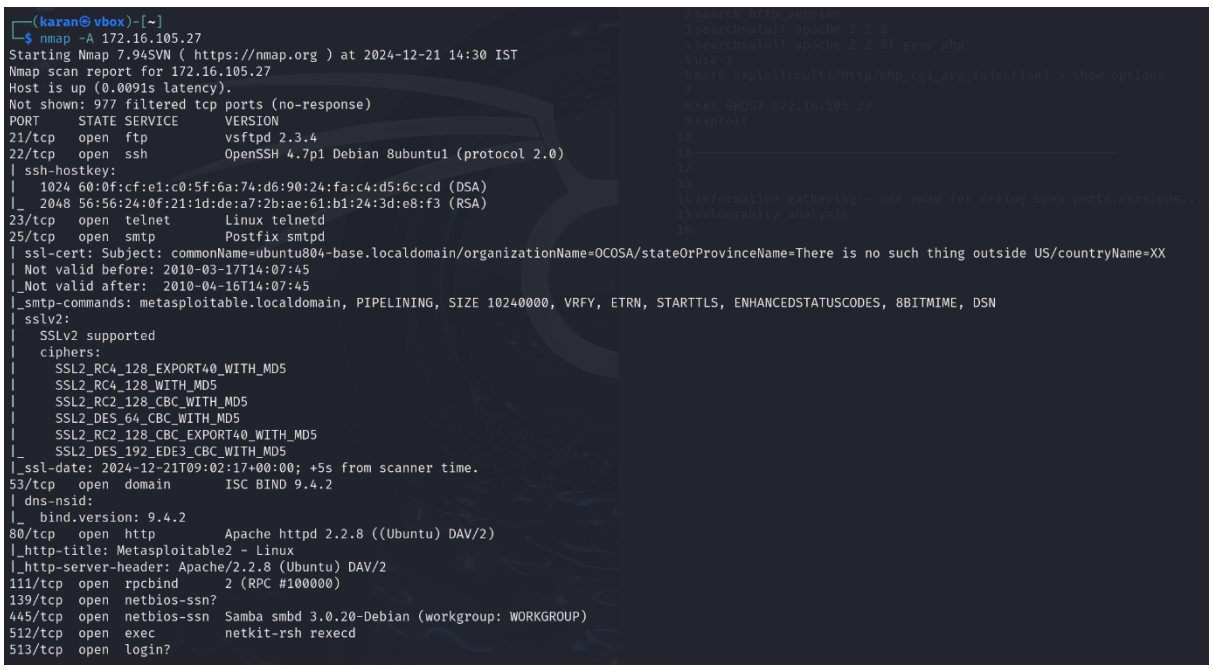
ping – To see if the system is reachable in the network and to check latency



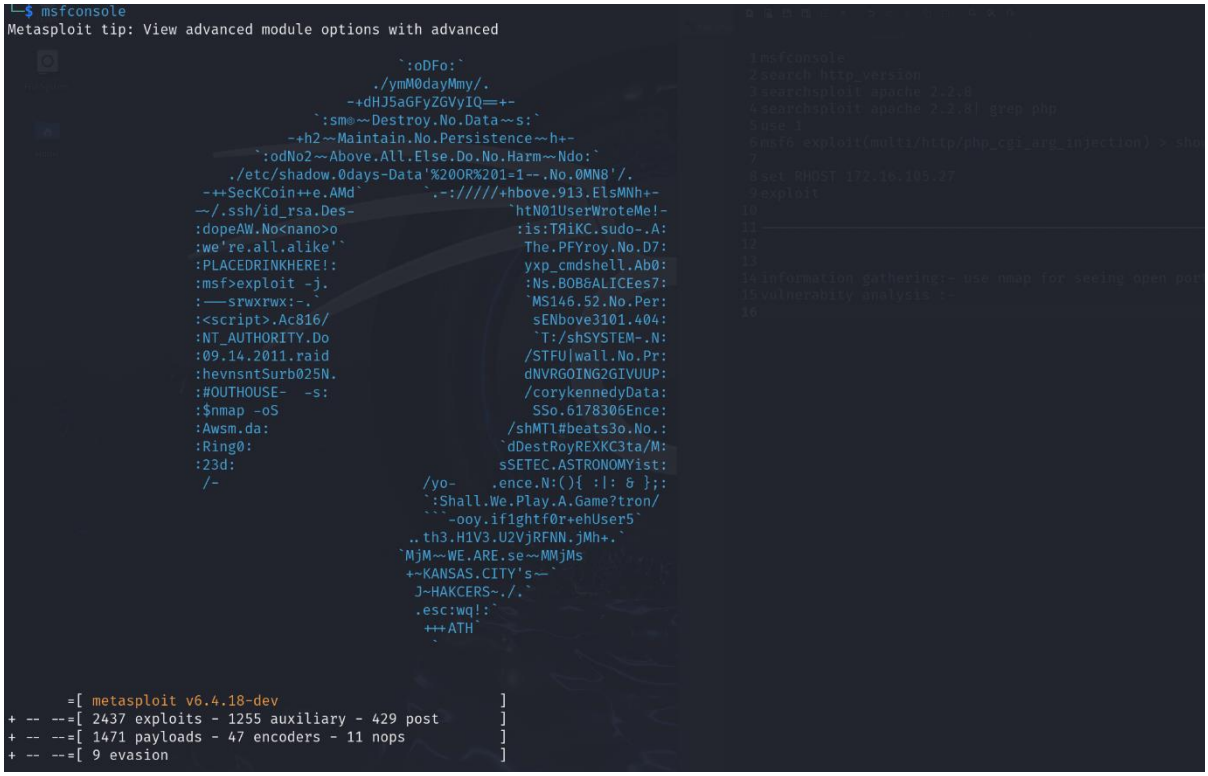
nmap – It is a scanning tool, allows us to view all the ports open

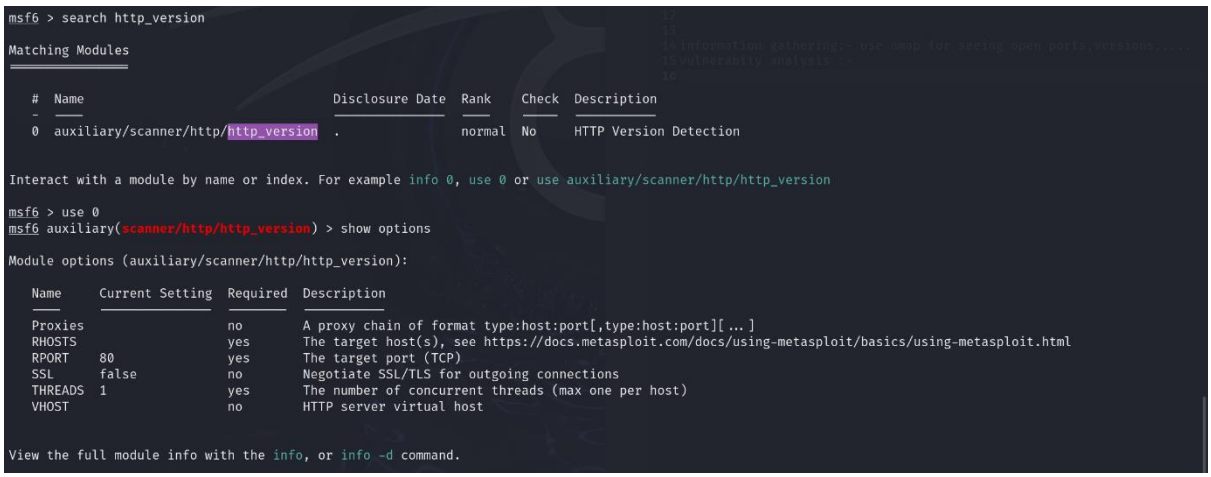


nmap -sV -- service version scan,returns the versions of the services running on open ports



nmap -A -- used for OS scanning

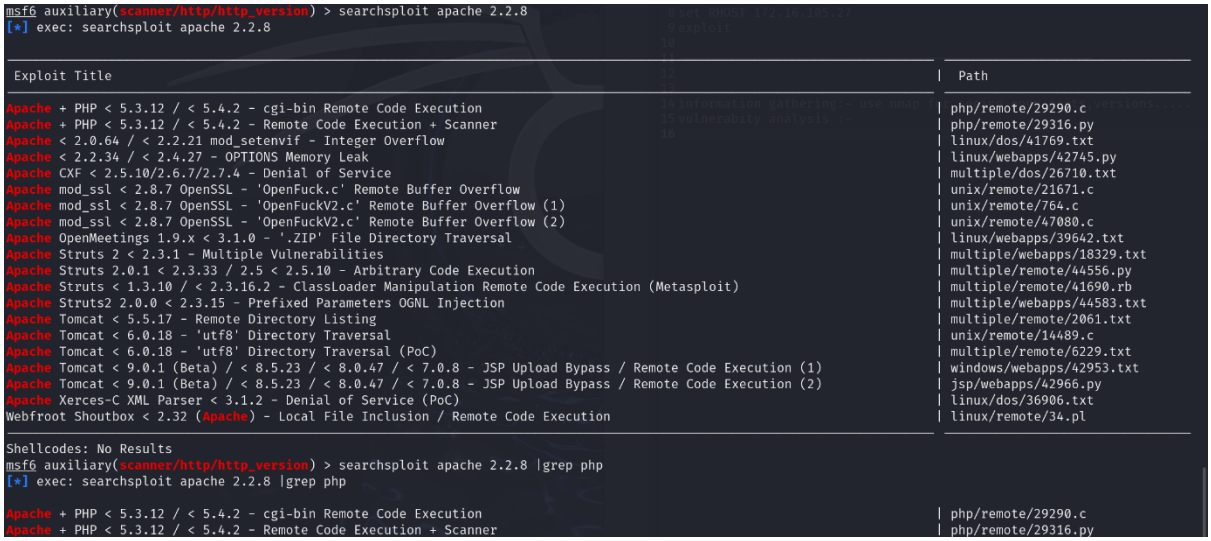


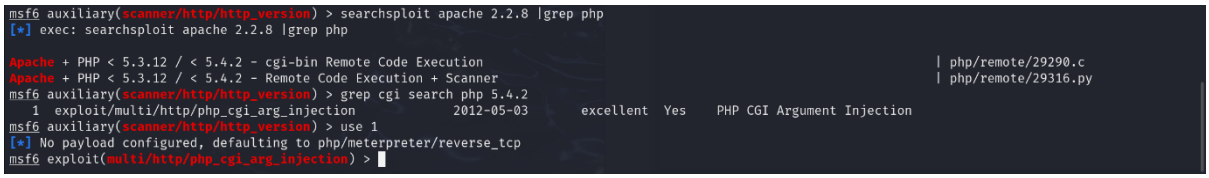


msfconsole – To launch the Metasploit console,opens a shell where you search for exploits

search http_version - used to find exploits or auxiliary modules that deal with HTTP versions or related vulnerabilities

use 0 – to select a module



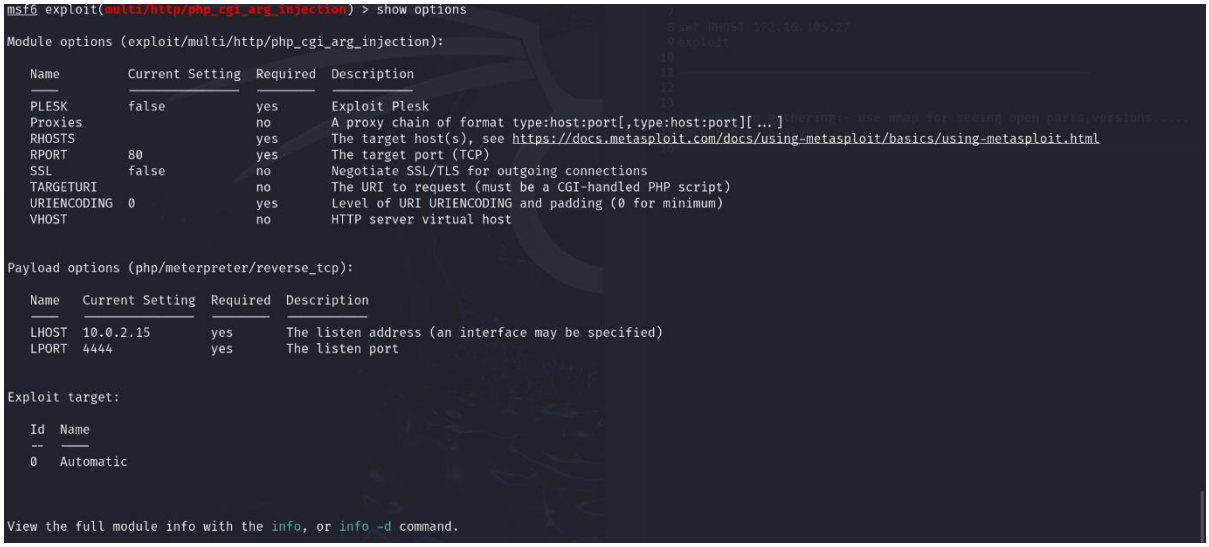


searchsploit apache 2.2.8 – find vulnerabilities in Apache 2.2.8 from Exploit Database

searchsploit apache 2.2.8 | grep php – filters using grep to only show vulnerabilities related to php

grep cgi search php 5.4.2 -- checks for exploits for CGI vulnerabilities in php 5.4.2

use 1 – load exploit into Metasploit



show options – displays list of configuration for the selected exploits