

L'esercizio di oggi ha come finalità l'exploit su meta utilizzando il protocollo telnet

```
kali@kali: ~  
..a$$$$$$$$SSSS$$$$$$$$$$$$$$$$$$$$SS##==--K N I T A A /SSSS$'  
-----,6$$$$$$'  
ll66$$$$'  
.,;lll6666'  
...;lllll6'  
.....;lll;..  
'.....;.;..  
  
=[ metasploit v6.3.27-dev ]  
+ -- --[ 2335 exploits - 1220 auxiliary - 413 post ]  
+ -- --[ 1385 payloads - 46 encoders - 11 nops ]  
+ -- --[ 9 evasion ]  
  
Metasploit tip: Open an interactive Ruby terminal with  
irb  
Metasploit Documentation: https://docs.metasploit.com/  
  
msf6 > use auxiliary/scanner/telnet/telnet_version  
msf6 auxiliary(scanner/telnet/telnet_version) > show option  
[-] Invalid parameter "option", use "show -h" for more information  
msf6 auxiliary(scanner/telnet/telnet_version) > show options  
  
Module options (auxiliary/scanner/telnet/telnet_version):  
  
Name Current Setting Required Description  
----  
PASSWORD no The password for the specified username  
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html  
RPORT 23 yes The target port (TCP)  
THREADS 1 yes The number of concurrent threads (max one per host)  
TIMEOUT 30 yes Timeout for the Telnet probe  
USERNAME no The username to authenticate as  
  
View the full module info with the info, or info -d command.  
  
msf6 auxiliary(scanner/telnet/telnet_version) > set RHOSTS 192.168.50.101  
RHOSTS => 192.168.50.101  
msf6 auxiliary(scanner/telnet/telnet_version) > exploit
```