```
   ----       -------------    ------   ---------
   PASSWORD                    no       The password for the specified username
   RHOSTS     192.168.178.100  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) > exploit

[+] 192.168.178.100:23    - 192.168.178.100:23 TELNET _                  _       _ _        _     _      ____  \x0a _ __ ___   ___| |_ __ _ ___ _ __ _ __
| | ___ (_) |_ __ _| |__ | | ___|___ \ \x0a| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |\x0a| | | | | |  __/ || (_| \__ \
 |_) | | (_) | | || (_| | |_) | |  __// __/ \x0a|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|\x0a
    |_|                                          \x0a\x0a\x0aWarning: Never expose this VM to an untrusted network!\x0a\x0aContact: msfdev[at]metaspl
oit.com\x0a\x0aLogin with msfadmin/msfadmin to get started\x0a\x0a\x0ametasploitable login:
[*] 192.168.178.100:23    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) > ping 192.168.178.34
[*] exec: ping 192.168.178.34

PING 192.168.178.34 (192.168.178.34) 56(84) bytes of data.
^C
--- 192.168.178.34 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4104ms

Interrupt: use the 'exit' command to quit
msf6 auxiliary(scanner/telnet/telnet_version) > ping 192.168.178.122
[*] exec: ping 192.168.178.122

PING 192.168.178.122 (192.168.178.122) 56(84) bytes of data.
64 bytes from 192.168.178.122: icmp_seq=1 ttl=64 time=1139 ms
64 bytes from 192.168.178.122: icmp_seq=2 ttl=64 time=132 ms
64 bytes from 192.168.178.122: icmp_seq=3 ttl=64 time=90.9 ms
^C
Interrupt: use the 'exit' command to quit
--- 192.168.178.122 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2008ms
rtt min/avg/max/mdev = 90.945/454.038/1138.732/484.448 ms, pipe 2
msf6 auxiliary(scanner/telnet/telnet_version) > set RHOSTS 192.168.178.122
RHOSTS => 192.168.178.122
msf6 auxiliary(scanner/telnet/telnet_version) > exploit

[-] 192.168.178.122:23    - A network issue has occurred: The connection was refused by the remote host (192.168.178.122:23).
[*] 192.168.178.122:23    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) > telnet 192.168.178.100
[*] exec: telnet 192.168.178.100

Trying 192.168.178.100...
Connected to 192.168.178.100.
Escape character is '^]'.
                _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started
```