

Oggi proveremo a scoprire la password per entrare nel protocollo **TELNET** usando il software **METASPLOIT**

Con **TELNET_VERSION** usiamo un exploit ausiliario per trovare la versione e le credenziali per entrare

MODULO AUSILIARIO: Modulo che utilizza varie funzioni che non riguardano direttamente l'exploitation fornendo informazioni aggiuntive come scansioni e rilevamento di vulnerabilità

Scegliamo il secondo Modulo **auxillary/scanner/telnet/telnet_version**

[illegible]

Settiamo L'ip della vittima

```
View the full module info with the info, or info -d command.
```

```
msf6 auxiliary(scanner/telnet/telnet_version) > set rhost 192.168.1.40
rhost => 192.168.1.40
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	192.168.1.40	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) > 
```

In questo caso noi non conosciamo user e password ma l'exploit sfrutta la vulnerabilità di telnet e riporta il banner iniziale

[illegible]

Ecco il banner iniziale della macchina metasploit con all'interno msfadmin/msfadmin che sono le password per entrare nella macchina

