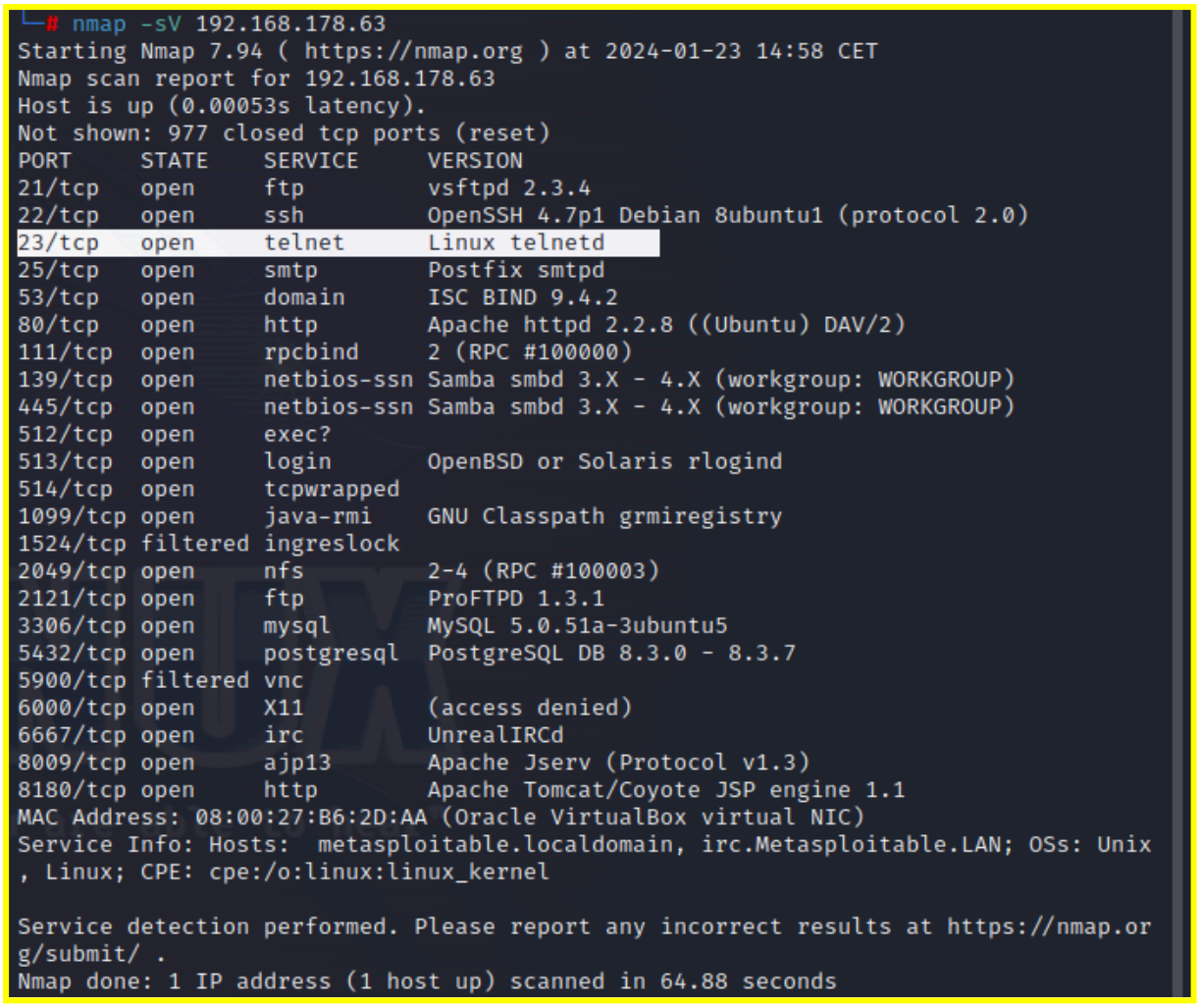
S7L2

Oggi, andremo ad eseguire un exploit sul servizio telnet, sfruttando una sua vulnerabilità.

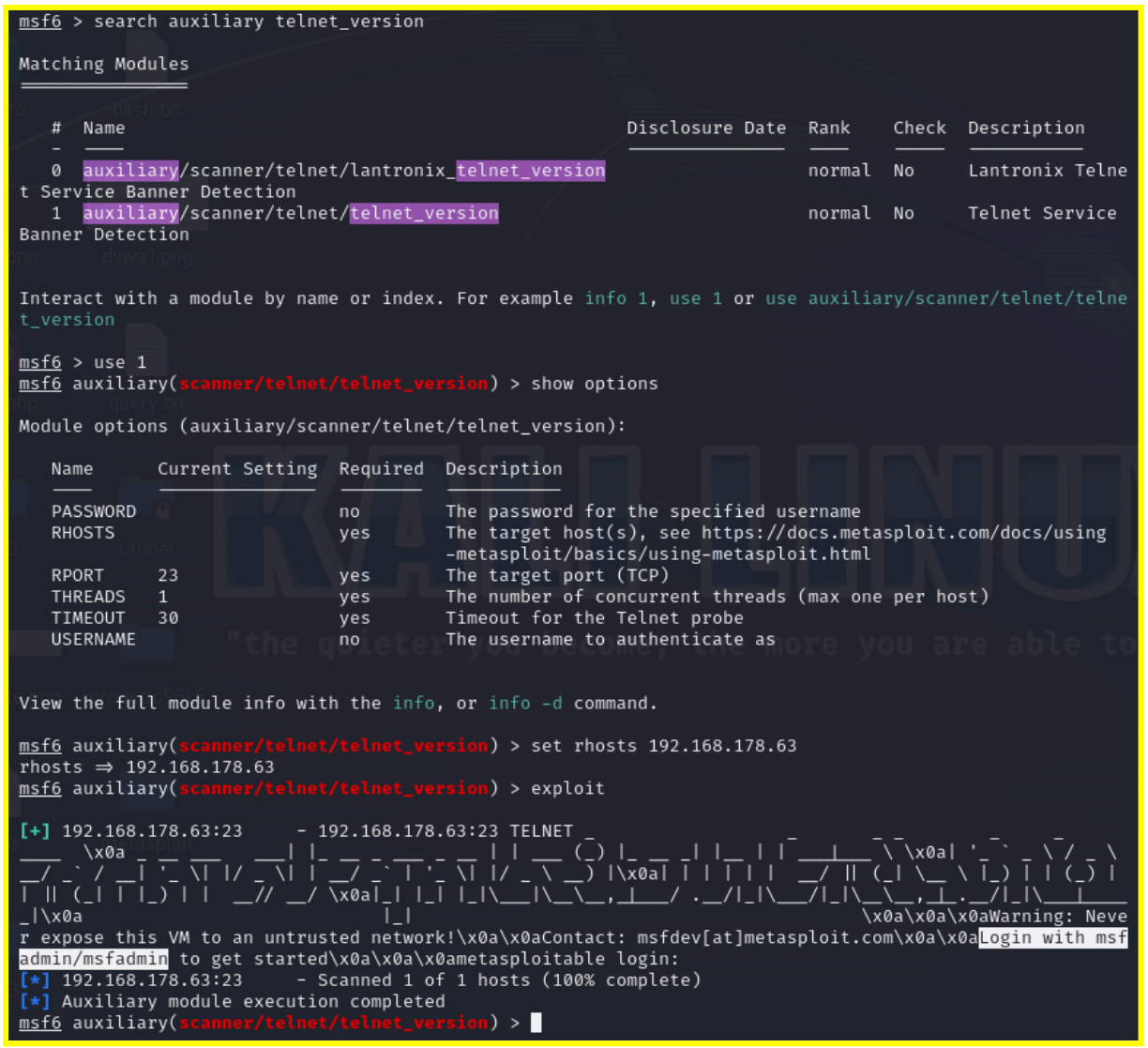
Eseguiamo una scansione sul target,per vedere quali servizi sono attivi e le rispettive porte aperte



```
└─# nmap -sV 192.168.178.63
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-23 14:58 CET
Nmap scan report for 192.168.178.63
Host is up (0.00053s latency).
Not shown: 977 closed tcp ports (reset)
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 telnetd
25/tcp   open     smtp        Postfix smtpd
53/tcp   open     domain      ISC BIND 9.4.2
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)
512/tcp  open     exec?
513/tcp  open     login       OpenBSD or Solaris rlogind
514/tcp  open     tcpwrapped
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 filtered vnc
6000/tcp open     X11         (access denied)
6667/tcp open     irc         UnrealIRCd
8009/tcp open     ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open     http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:B6:2D:AA (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix
, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.or
g/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 64.88 seconds
```

Dopo che abbiamo individuato il servizio,andiamo a cercare un exploit che sfrutti una vulnerabilità su quest'ultimo.



Ecco,come possiamo vedere l'exploit è avvenuto con successo,infatti abbiamo ottenuto le credenziali di accesso alla macchina target