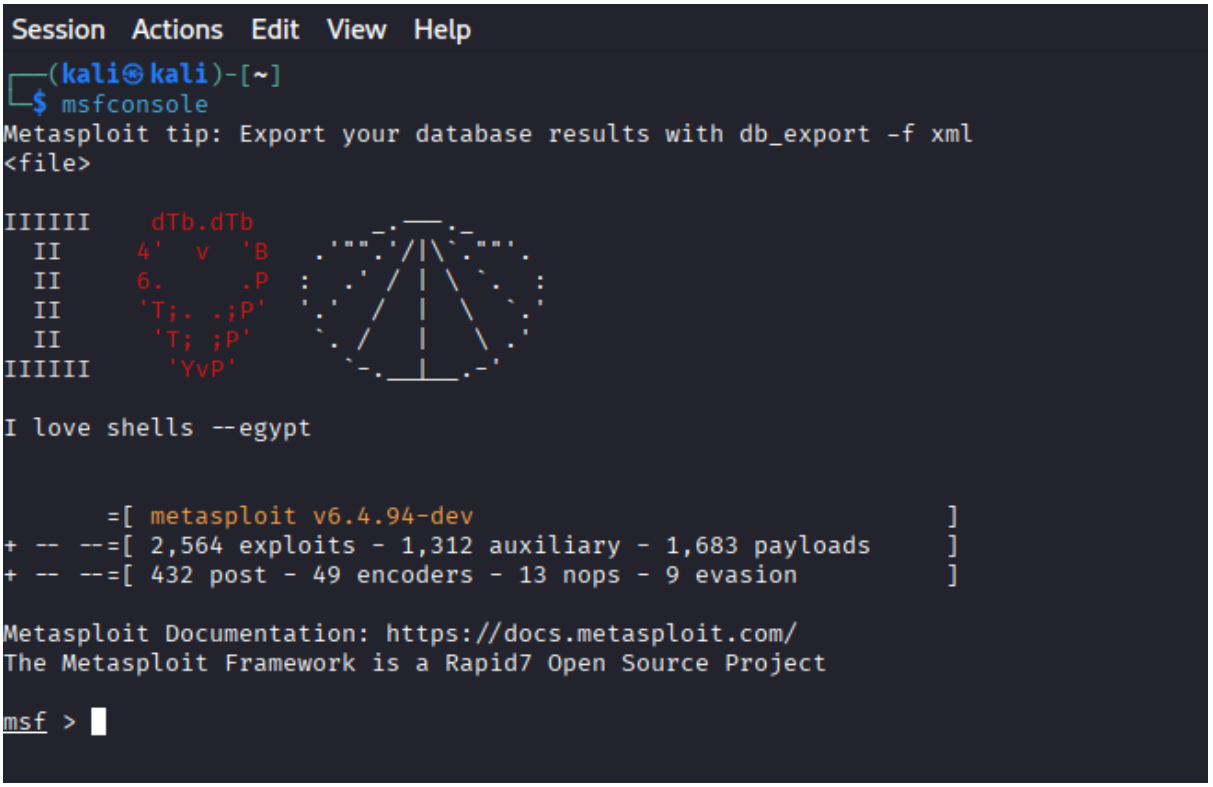
Traccia:

Sulla base di quanto visto, utilizzare Kali per sfruttare la vulnerabilità relativa a Telnet con il modulo auxiliary telnet_version sulla macchina Metasploitable.

Requisito: Seguire gli step già visti. Prima, configurate l'IP della vostra Kali con 192.168.1.25 e l'IP della vostra Metasploitable con 192.168.1.40

SVOLGIMENTO:



ho avviato msfconsole

```
msf > use auxiliary/scanner/telnet/telnet_version
msf 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.

msf auxiliary(scanner/telnet/telnet_version) >
```

ho sfruttato il modulo auxiliary scanner/telnet/telnet_version con il comando use

ho configurato Rhost con l'indirizzo della macchina meta e ho fatto partire l'exploit

```
PORT   STATE SERVICE VERSION
23/tcp open  telnet  Linux telnetd
MAC Address: 08:00:27:9A:8B:1E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: 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 0.34 seconds

┌──(kali㉿kali)-[~]
└─$ telnet 192.168.50.101
Trying 192.168.50.101 ...
Connected to 192.168.50.101.
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:
```

ho verificato la correttezza delle informazioni trovate dell'exploit provando l'accesso al servizio telnet con il comando telnet eseguito dalla kali.